TIC

Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de contenido

Tabla de contenido 3
Listado de tablas 4
1. Listado de Ilustraciones 4
Introducción 5
2. Audiencia 7
3. Definiciones 7
4. Propósitos 19
5. Marco jurídico 19
6. Diagnóstico 22
7. Fase 1: Planificación 23
7.1. Contexto 24
7.1.1. Comprensión de la organización y de su contexto 24
7.1.2. Necesidades y expectativas de los interesados 24
7.1.3. Definición del alcance del MSPI 25
7.2. Liderazgo 27
7.2.1. Liderazgo y Compromiso 27
7.2.2. Política de seguridad y privacidad de la información 28
7.2.3. Roles y responsabilidades 29
7.3. Planeacion 30
7.3.1. Identificación de activos de información e infraestructura critica cibernética 30
7.3.2. Valoración de los riesgos de seguridad de la información 31
7.3.3. Plan de tratamiento de los riesgos de seguridad de la información 33
7.4. Soporte 34
7.4.1. Recursos 34
7.4.2. Competencia, toma de conciencia y comunicación 35
7.4.3. Información documentada 36
8. Fase 2: Operación 37
8.1. Control y planeación operacional 37
8.2. Plan de tratamiento de riesgos 38
8.3. Definición de indicadores de gestión 39
9. Fase 3: Evaluación de desempeño 39
9.1. Seguimiento, medición, análisis y evaluación 40

9.2. Auditoría Interna 41
9.3. Revisión por la dirección 42
10. Fase 4: Mejoramiento continuo 42
10.1. Mejora continua 42
10.2. Acciones Correctivas y no conformidades 43
11. Anexo 44
11.1. Controles y objetivos de control 44

Listado de tablas

Tabla 1 Estructura de los controles 44
Tabla 2: Controles del Anexo A del estándar ISO/IEC 27001:2022 y dominios a los que pertenece 52

1. Listado de Ilustraciones

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información 6
Ilustración 2 Equipo de Gestión de Seguridad de la Información en las entidades 65

Introducción

El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, es consecuente con la realidad de que las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, por lo que puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Por la cual, el ministerio como entidad se encarga de diseñar, adoptar y promover políticas, planes, programas y proyectos para el uso y apropiación de las TIC, y establece lineamientos para generar confianza en el uso del entorno digital, garantizando el aprovechamiento de las tecnologías de la información y las comunicaciones. El Ministerio busca fortalecer la implementación y mejora continua de controles de seguridad de la información en las Entidades del Estado con el objetivo de: mejorar la ciberseguridad y resiliencia organizacional, promoviendo la aplicación de controles de seguridad digital para garantizar la continuidad de los servicios críticos para el Estado colombiano.

La política de gobierno digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además, establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen la implementación de controles físicos, lógicos y administrativos para asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las entidades públicas de orden nacional y territorial, gestionando los activos de información, infraestructura critica cibernética nacional, los riesgos e incidentes de seguridad y privacidad de la información, evitando la interrupción de la prestación de los servicios de la entidad enmarcados en su modelo de operación y minimizando el impacto en caso de presentarse

Teniendo en cuenta lo anterior, el MinTIC define el Modelo de Seguridad y Privacidad de la Información – MSPI y establece los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un Sistema de Gestión de Seguridad y privacidad de la Información – SGSPI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), integrando consideraciones y controles específicos de ciberseguridad en cada una de sus etapas:

Planear: Se definen objetivos de seguridad y privacidad de la información y de seguridad digital, según el contexto y la valoración de riesgos.

Hacer: Se implementan controles de seguridad digital para proteger activos digitales e infraestructura tecnológica al mitigar riesgos.

Verificar: Se evalúa la efectividad de controles de seguridad de la información y seguridad digital mediante auditorías e indicadores.

Actuar: Se identifican desviaciones y se toman acciones correctivas y preventivas para fortalecer la seguridad y privacidad de la información y la seguridad digital.

Así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento.

El Modelo de Seguridad y Privacidad de la Información (MSPI) está estructurado en cinco (5) fases que permiten a las entidades gestionar y mantener de forma adecuada la seguridad y privacidad de sus activos de información. Estas fases se desarrollan de la siguiente manera:

1. **Diagnóstico**: La entidad debe iniciar con un diagnóstico o análisis de brechas (GAP), cuyo propósito es identificar su estado actual frente a los requisitos del MSPI. Este insumo es clave tanto para la fase de planificación como para medir avances al finalizar la fase de mejoramiento continuo.

2. **Planificación**: Se establecen las necesidades, objetivos y estrategias de seguridad y privacidad de la información, considerando el mapa de procesos, el tamaño institucional y el contexto interno y externo. Esta fase incluye la identificación, valoración y tratamiento de riesgos, siendo el pilar del ciclo de gestión.

3. **Operación**: En esta fase, la entidad implementa los controles definidos en la planificación para reducir la probabilidad y el impacto de los riesgos identificados.

4. **Evaluación del desempeño**: Se mide la efectividad del modelo a través de auditorías, revisiones y análisis de indicadores definidos previamente, permitiendo identificar avances, desviaciones o áreas de mejora.

5. **Mejoramiento continuo**: Se establecen mecanismos para detectar y corregir desviaciones, implementar acciones correctivas y prevenir su repetición, fortaleciendo así el sistema de manera progresiva.

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

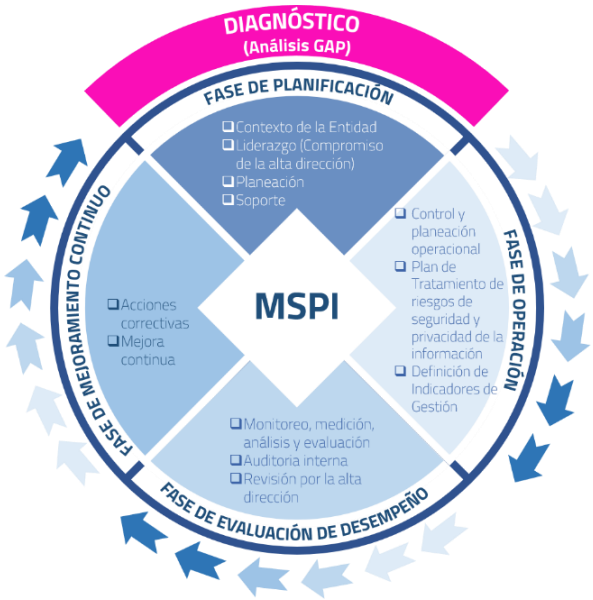


Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información

La seguridad de la información debe verse como la interacción de múltiples componentes que trabajan conjuntamente para proteger no solo los sistemas tecnológicos, sino también los activos humanos, la infraestructura física, el desarrollo de software, la gestión del talento humano, la calidad, la gestión con proveedores y otros elementos clave. Esto implica la implementación de estrategias que salvaguarden la confidencialidad, integridad y disponibilidad de la información en todos los niveles de la organización, abarcando tanto aspectos técnicos como organizativos y administrativos.

Ilustración 2. Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032)

2. Audiencia

El presente documento está dirigido a entidades públicas de orden nacional y territorial, así como proveedores de servicios de la Política de Gobierno Digital y estrategia de seguridad digital, terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información, entre otros, de acuerdo con la Política de Seguridad Digital y el Artículo 2. Ámbito de aplicación de la Resolución 500 de 2021, proferida por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la política de Gobierno Digital.”

3. Definiciones

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- **Activo crítico:** Son aquellos elementos o componentes que hacen parte de la infraestructura crítica.

- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022).

- **Alcance del MSPI**: Es el número del total de los procesos que serán incluidos en la implementación del MSPI.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).

- **Amenaza cibernética:** aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

- **Agente de Mesa de Servicio**: Recibe la información de los Colaboradores del Ministerio, registra los casos en la herramienta de mesa de servicio y es el

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27001:2022).

- **Ataque informático:** Conjunto de actividades realizadas por atacantes para vulnerar la seguridad informática de un sistema.

- **Ataque cibernético:** acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. Este concepto se desarrolla de manera más profunda como ciberataque.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27001:2022).

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- **BCP (Business Continuity Planning / Plan de Continuidad de Negocios):** Es un plan logístico detallado de cómo una entidad debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

- **CERT:** (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas, por su sigla en inglés. Es el equipo que dispone de la capacidad centralizada para la coordinación de gestión de incidentes de seguridad digital.

- **Ciberespacio:** Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias. (Decreto 338 de 2022).

- **Ciberdefensa:** capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. La ciberdefensa implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética. (Conpes 3995 de 2020).

- **Ciberespionaje:** Ciberespionaje - «El Ciberespionaje se utiliza principalmente como un medio para recopilar datos sensibles o clasificados, secretos comerciales u otras formas de propiedad intelectual que pueden ser utilizados por el agresor para crear una ventaja competitiva o vendidos para obtener beneficios financieros. En algunos casos, la violación simplemente pretende causar un daño reputacional a la víctima exponiendo información privada o prácticas empresariales cuestionables.» - Crowdstrike.

- **Ciberincidente:** Cualquier acto malicioso o evento sospechoso que comprometa, o intente comprometer la Seguridad del perímetro electrónico, la Seguridad del primero físico o un activo crítico.

- **Ciberseguridad:** Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

- **Ciberamenaza** - Cualquier circunstancia o evento con el potencial de impactar negativamente en las operaciones de la organización (incluyendo misión, funciones, imagen o reputación), activos de la organización o individuos a través de un sistema de información mediante acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicio. También, el potencial de una amenaza-fuente para explotar con éxito una vulnerabilidad particular del sistema de información. NIST SP 1800-15B

- **Ciberataque** - Un ataque, a través del ciberespacio, dirigido al uso del ciberespacio por parte de una empresa con el propósito de interrumpir, inutilizar, destruir o controlar maliciosamente un entorno/infraestructura informática; o destruir la integridad de los datos o robar información controlada. NIST SP 1800-10B de NIST SP 800-30 Rev.1

- **Ciberterrorismo:** es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo como consecuencia una violación a la voluntad de las personas.

- **CSIRT:** (Computer Security lncident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.

- **CSIRT Gobierno:** Equipo de Respuesta a Incidentes de Seguridad en sus siglas en inglés (Computer Security Incident & Response Team), integrado por un grupo de personas técnicas especializadas, que implementan y desarrollan medidas tendientes a prevenir y gestionar incidentes de ciberseguridad de las entidades del estado.

- **CSIRT sectorial:** Son los equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales, a partir del uso de las tecnologías de la información y las comunicaciones.

- **CSIRT sectorial crítico:** Son los equipos de respuesta a incidentes sectoriales de cada uno de los sectores identificados como críticos.

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Código malicioso:** Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.
-
- **COLCERT:** Por sus siglas en inglés Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual se encuentra enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica cibernética del Estado Colombiano frente a emergencias de Ciberseguridad que atenten y comprometan la seguridad y defensa nacional.

- **Contención de un incidente:** Son todas aquellas actividades encaminadas a reducir el impacto inmediato de un incidente de seguridad.

- **Criterios horizontales de criticidad:** Criterios únicos a nivel país para determinar si una infraestructura estratégica es considerada crítica. Adaptación Ley 8/2011-Gobierno de España.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art. 6)

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3, numeral 3)

- **Denegación del servicio:** Conjunto de actividades desarrolladas por atacantes informáticos para degradar o interrumpir el normal funcionamiento de un sistema servicio informático.

- **Derecho a la Intimidad:** Protege el ámbito privado del individuo y de su familia como el núcleo humano más próximo. Uno y otra están en posición de reclamar una mínima consideración particular y pública a su interioridad, actitud que se traduce en abstención de conocimiento e injerencia en la esfera reservada que les corresponde y que está compuesta por asuntos, problemas, situaciones y circunstancias de su exclusivo interés. Esta no hace parte del dominio público y, por tanto, no debe ser materia de información suministrada a terceros, ni de la intervención o análisis de grupos humanos ajenos, ni de divulgaciones o publicaciones (Sentencia C-640/10).

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

- **Entorno digital:** Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo

desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

- **Entorno digital abierto:** Entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

- **Evento:** Un evento es cualquier suceso observable en un sistema o red, como un usuario que se conecta a un recurso compartido de archivos, un usuario que envía un archivo electrónico o un firewall que bloquea un intento de conexión, entre otros.

- **Eventos adversos:** son aquellos que tienen consecuencias negativas, como fallos en un sistema, usos no autorizados de privilegios en un sistema, acceso no autorizados y ejecución de malware.

- **Evento de Seguridad de la Información:** Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles, o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 27000:2009].

- **Defacement:** Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia.

- **DoS / DDoS (Denial of Service / Distributed Denial of Service):** Se entiende como denegación de servicio, en términos de seguridad digital, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

- **DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres):** es un documento formal creado por una organización que contiene instrucciones detalladas con la definición de los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27001:2022).

- **Gobernanza de la seguridad digital para Colombia:** Corresponde al conjunto de interacciones y enfoques entre las múltiples partes interesadas para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes e información que en conjunto constituyen el entorno digital.

- **Incidente:** Un incidente es una violación o amenaza inminente a las políticas de seguridad digital, políticas de uso aceptable y/o prácticas de seguridad básicas.

- **Incidente de seguridad digital:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338 de 2022)

- **Infraestructura Cibernética (Ic):** Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO).

- **Infraestructuras Críticas**: incluyen la vasta red de carreteras, puentes y túneles de conexión, ferrocarriles, servicios públicos y edificios necesarios para mantener la normalidad en la vida cotidiana de los ciudadanos. El transporte, el comercio, el agua potable y la electricidad dependen de estos sistemas críticos. Infraestructura crítica puede ser cualquier sistema, ya sea físico o virtual, que sea tan vital que si se interrumpe puede tener un impacto debilitador en la seguridad, la economía, la salud pública o la seguridad, el medio ambiente. También puede definirse como los sistemas y activos que sustentan industrias o servicios urbanos y rurales subnacionales esenciales.

    - Las infraestructuras críticas son vulnerables a innumerables amenazas o peligros, además, de manejar una relación de interdependencia entre estas mismas. Lo que significa que sus operaciones confiables son tan críticas que una interrupción o pérdida de una de estas funciones afectará directamente la seguridad y la resiliencia de la infraestructura crítica dentro y entre numerosos sectores. Lo que con el tiempo puede provocar una pérdida adicional de otras funciones.

    - Aunque parte de esta infraestructura física y cibernética esta operada por empresas estatales, normalmente el sector privado tiene un gran margen de operatividad y propiedad sobre estas mismas, especialmente en la cibernética. Por lo que se debe trabajar en sociedad con el sector público y privado para aumentar la resiliencia, reducir el riesgo y mantener la confianza en la infraestructura crítica de la nación.

- **Infraestructura Crítica Cibernética (ICC):** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía. (Decreto 338 de 2022). Esta se alinea a la definición de NIST Sistema y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud pública nacional o la seguridad, o cualquier combinación de estos asuntos. NIST SP 800-30 Rev.1

- **Infraestructura Estratégica (IE):** Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España.

- **Infraestructura Estratégica Cibernética (IEC):** Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) y Tecnologías de Operación (TO), sobre las que se soporta el funcionamiento de los servicios esenciales. Fuente: Guía de IC Ministerio de Defensa.

- **Incidente de seguridad informática:** Una violación o inminente amenaza de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas estándar seguridad. En el contexto de este procedimiento, una inminente amenaza es definida como una situación en la cual la organización tiene evidencias para creer que un incidente de seguridad va a ocurrir.

- **Incidente de privacidad de la información:** Evento o serie de eventos no deseados e inesperados producto del tratamiento de los datos personales.

- **Incidentes de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000 2009].

- **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

- **Información pública**. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Literal b, artículo. 6 de la Ley 1712 de 2014)

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley. (Literal c, artículo. 6 de la Ley 1712 de 2014)

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Ingeniería social:** Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social.

- **Inyección de ficheros remota:** Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada, que permite a los atacantes transferir código malicioso al sistema subyacente a través de una aplicación web.

- **Inyección SQL:** Tipo de ataque a sitios web basados en bases de datos. Una persona malintencionada ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización mediante la computadora que funciona como servidor de la base de datos.

- **Incidente de seguridad digital - Ciberincidente:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

- **Infraestructura crítica cibernética:** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008, o aquella que la modifique, adicione o sustituya

- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014, o aquella que la modifique, adicione o sustituya.

- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado y pseudominización

- **Modelo de Gobernanza de Seguridad digital:** Es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información que, en conjunto, constituyen el entorno digital en el país. (Decreto 338-2022)..

- **Múltiples partes interesadas:** Corresponde al conjunto de actores que dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales. Comprende a las autoridades, las organizaciones privadas, los operadores o propietarios de las infraestructuras críticas cibernéticas nacionales, los prestadores de servicios esenciales, la academia y la sociedad civil.

- **NIST:** Es el Instituto Nacional de Estándares y Tecnología y busca promover la innovación y la competencia industrial mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada, por una decisión o actividad.

- **Pharming:** Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP (Internet Protocol) donde se aloja una web (página) falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27001:2022).

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Plan de Respuesta a Ciberincidentes:** Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, analizar, contener, erradicar y recuperar para minimizar las consecuencias de un ciberincidente.

- **Phishing:** Es un método que los ciberdelincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito, de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

- **Plan de Continuidad de la operación:** Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

- **Ransomware:** Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado, se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos, secuestrando computadores y servidores (imposibilidad de usarlo) o cifrando los archivos, con la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.

- **RAT- Remote Access Tool:** Pieza de software que permite a un “operador” controlar a distancia un sistema como si se tuviera acceso físico al mismo. Aunque tiene usos necesarios para la administración de sistemas a distancia, el software RAT se asocia habitualmente con ciberataques o actividades criminales o dañinas. En estos casos, el malware suele instalarse sin el conocimiento de la víctima, ocultando frecuentemente un troyano.

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27001:2022).

- **Riesgo de seguridad digital:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

- **Rootkit:** Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo.

- **Scanner (Scanning) Escáner de vulnerabilidades:** Programa que analiza un sistema buscando vulnerabilidades. Utiliza una base de datos de defectos conocidos y determina si el sistema bajo examen es vulnerable o no.

- **Spam (correo basura):** Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de los usuarios que están expuestos a este correo basura que se confirma en encuestas que muestran que más del 50% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.

- **Spear Phising:** Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo (suelen basarse en un trabajo previo de ingeniera social sobre la victima).

- **Spyware “spy software”:** Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.

- **Suplantación (Spoofing):** Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la

identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del anfitrión suplantado.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27001:2022).

- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y mediante: (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades; que demanda la voluntad social y política de las múltiples partes interesadas. (Decreto 338 de 2022). Para el caso de estandarización de lenguaje este concepto se asocia al aceptado internacionalmente como ciberseguridad.

- **Servicio esencial:** En el marco de la gestión de riesgos de la seguridad digital es aquel servicio necesario para el mantenimiento de las actividades sociales y económicas del país, que dependen del uso de tecnologías de la información y las comunicaciones, y un incidente en su infraestructura o servicio puede generar un daño significativo que afecte la prestación de dicho servicio y la consecuente parálisis de las actividades. (Decreto 338 de 2022).

- **Servicio crítico:** Conjunto de actividades que la organización realiza, al generar un producto o en la prestación de un servicio fundamental para la organización o sector del país, que al interrumpirse afectaría su operación.
- **Suplantación de identidad:** Todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.

- **Tecnologías de la Información:** Las tecnologías de la información se centra en el tratamiento y la gestión de datos. [1]

- **Tecnologías de Operación:** La tecnología de operación se define como el conjunto de sistemas, procesos y herramientas que permiten a las empresas gestionar y controlar sus operaciones diarias de manera eficiente.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

[1] https://www.eccouncil.org/cybersecurity-exchange/whitepaper/understanding-the-difference-between-it-and-ot-security/#:~:text=While%20IT%20focuses%20on%20data,controlling%20physical%20processes%20and%20machinery.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

- **Vulnerabilidad de seguridad digital:** Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización. (Decreto 338 de 2022).

- **Troyano:** Programa que aparentemente, o realmente, ejecuta una función útil, pero oculta un subprograma dañino que abusa de los privilegios concedidos para la ejecución del citado programa.

- **Virus informático / malware / software malicioso:** Programa informático que está diseñado para realizar acciones maliciosas sobre un activo informático como copiarse a sí mismo, cifrar información, recolectar y filtrar información, entre otros, sin el consentimiento del propietario

4. Propósitos

- Facilitar la adopción e implementación del MSPI con mecanismos y lineamientos claros.

- Desarrollar e implementar la estrategia de seguridad digital de las entidades.

- Integrar la seguridad como habilitador en la política de Gobierno Digital mediante procedimientos definidos.

- Institucionalizar la seguridad y privacidad de la información y seguridad digital en los procesos de la entidad.

- Contribuir a la transparencia en la gestión pública a través de la implementación efectiva del MSPI.

- Apoyar la implementación del plan estratégico institucional mediante el plan de seguridad y privacidad de la información.

- Asistir a las entidades en la identificación y tratamiento de riesgos de seguridad de la información y seguridad digital

5. Marco jurídico

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la entidad:

- Constitución Política de Colombia, artículos 15, 209 y 269.

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del Estado.

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Decreto 1074 de 2015. Por el que se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.

- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

- Decreto 1083 de 2015 establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.

- Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad digital.

- CONPES 4144 de 2025. Política Nacional de Inteligencia Artificial

- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional

del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.

- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 338 de 2022 Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Conpes 3975 del 2019 política nacional para la transformación digital e inteligencia artificial

- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.

- Decreto 767 de 2022. "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

- Norma ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.

- Decreto 1083 de 2015 y sus modificaciones y actualizaciones.

- Decreto 767 de 2022. “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”

- Decreto 1263 de 2022. “Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías

de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública”

Otras normas internacionales a tener en cuenta:

GDPR (Reglamento General de Protección de Datos): Se recomienda adoptar prácticas inspiradas en este reglamento, especialmente en lo relacionado con derechos del titular, principios de minimización, portabilidad, notificación de brechas de seguridad y consentimiento explícito, como complemento a la Ley 1581 de 2012.

NIST SP 800-53: Puede ser utilizado como guía técnica para complementar los controles de seguridad del MSPI, especialmente en sistemas críticos o servicios de procesamiento masivo de datos. Su adopción es flexible, gradual y adaptada al contexto local.

Este enfoque permitirá que las entidades públicas no solo cumplan con los requerimientos normativos nacionales, sino que también avancen hacia la adopción de estándares globales que refuercen la confianza digital, la interoperabilidad y la preparación ante riesgos emergentes.

6. Diagnóstico

La fase de diagnóstico permite a las entidades establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un “Diagnóstico” utilizando el “instrumento de evaluación MSPI” con el que se identifica de forma específica los controles implementados, se mide el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información y se obtienen insumos fundamentales para la fase de planificación.

Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación y actualizar la información tras terminar la fase de evaluación de desempeño, para identificar los cambios en el nivel de madurez de la implementación del Modelo en la entidad, el resultado que se obtenga después de la fase de evaluación de desempeño se incluirá como un insumo, en la fase de mejoramiento continuo.

Lineamiento:	Identificar a través de la herramienta de autodiagnóstico (instrumento de evaluación MSPI) el estado actual de la entidad respecto a la Seguridad y Privacidad de la Información.
Propósito:	Identificar el nivel de madurez de Seguridad y Privacidad de la información en el que se encuentra la entidad, como punto de partida para la implementación del MSPI.

Entradas recomendadas	Salidas
• Para la identificación del estado de implementación del MSPI, se debe utilizar la herramienta de autodiagnóstico del MSPI.	• Documento de la herramienta de autodiagnóstico diligenciada, identificando las brechas en la implementación

• Revisar aspectos internos tales como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros.	del MSPI en toda la entidad, y sus acciones de mejora.

7. Fase 1: Planificación

Para el desarrollo de esta fase se deben utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información, con el objetivo de que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI. Los documentos que se deben generar en esta fase son:

- Alcance MSPI.
- Acto administrativo con las funciones de seguridad y privacidad de la información.
- Adoptar la Política de seguridad y privacidad de la información mediante acto administrativo con el cual la entidad lo adopto colocar el número de resolución o acto administrativo.
- Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información.
- Procedimiento de inventario y Clasificación de la Información e infraestructura crítica.
- Metodología de inventario y clasificación de la información e infraestructura crítica.
- Política de Gestión de Riesgos de la entidad con los lineamientos para la gestión de riesgos de seguridad y privacidad de la información y demás documentación asociada que determinan dichos lineamientos para la administración y gestión del riesgo.
- Plan de tratamiento de riesgos de seguridad de la información.
- Declaración de aplicabilidad.
- Manual de políticas de Seguridad de la Información.
- Plan de Cambio, Cultura y Apropiación.

7.1. Contexto

7.1.1. Comprensión de la organización y de su contexto

Lineamiento:	Determinar los elementos externos e internos que son relevantes con las actividades que realiza la entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la entidad, teniendo en cuenta procesos necesarios y sus interacciones.
Propósito:	Conocer en detalle las características de la entidad y su entorno con el fin de implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas de cada entidad.

Entradas recomendadas	Salidas
• Para establecer el contexto de las entidades, deben tener en cuenta los aspectos relacionados en el Manual Operativo MIPG. • Modelo estratégico, modelo de procesos, modelo de servicios y modelo organizacional siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Plan estratégico de la entidad • Procedimientos e informes de auditoria al MSPI	Documentos obligatorios: Contexto de la entidad (Política de Planeación Institucional).

7.1.2.Necesidades y expectativas de los interesados

Lineamiento:	Se deben identificar las partes interesadas internas y externas que puedan influir o verse afectadas por la seguridad y privacidad de la información, así como sus necesidades y expectativas. Esta identificación debe incluir los requisitos legales, reglamentarios y contractuales, e integrarse adecuadamente al SGSI.

Propósito:	Conocer las necesidades y expectativas que se tiene respecto a la implementación del modelo de seguridad y privacidad de la información para identificar las acciones y actividades necesarias para satisfacerlas.

Entradas recomendadas	Salidas
• 7.1.1. Comprensión de la organización y de su contexto. • Política de Planeación institucional: 7.1.1. Comprensión de la organización y de su contexto. • Plan Nacional de Desarrollo. • Política de Gobierno Digital. • Política de seguridad digital • Entrevistas con los líderes de procesos de la entidad. • Listado de entidades de orden nacional o territorial que se relacionan directamente el cumplimiento misional de la entidad. • Listado de proveedores de la entidad. • Listado de operadores de la entidad. • Normatividad que le aplique a la entidad de acuerdo con funcionalidad respectivamente.	Documentos obligatorios: Compendio de necesidades y expectativas de las partes interesada. (Política de Planeación Institucional). Análisis de partes interesadas en seguridad de la información.

7.1.3. Definición del alcance del MSPI

Lineamiento:	Determinar con claridad los límites, el alcance y la aplicabilidad del MSPI en el marco del modelo de operación por procesos de la entidad. Esta definición debe especificar a qué procesos, recursos humanos, financieros, técnicos y tecnológicos se aplicará la implementación del modelo. Se recomienda iniciar con los procesos misionales, dado su

	impacto estratégico y su nivel de exposición a riesgos de seguridad y privacidad de la información.
Propósito:	Identificar qué activos de información, software, hardware, roles, sistemas de información, áreas seguras (generada o utilizada en los procesos de la entidad) será protegida mediante la adopción del MSPI.

Entradas recomendadas	**Salidas**
• 7.1.1 Comprensión de la organización y de su contexto. • 7.1.2 Necesidades y expectativas de los interesados • Modelo de procesos, modelo organizacional, modelo de servicios y catálogo de servicios tecnológicos; siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Presupuesto disponible para implementar el MSPI. • Listado de las sedes físicas donde opera la entidad.	• Alcance del MSPI, (Este alcance puede estar integrado al Manual del Sistema Integrado de Gestión, o en el documento del Modelo de Planeación y Gestión).

7.2. Liderazgo

7.2.1.Liderazgo y Compromiso

Lineamiento: Las entidades deben asignar, mediante acto administrativo, al comité institucional de gestión y desempeño (o su equivalente) las funciones relacionadas con la seguridad y privacidad de la información, asegurando la adopción, implementación y mejora continua del MSPI. En este comité debe incluirse como miembro permanente al responsable de seguridad de la información, con el fin de garantizar su implementación efectiva y el cumplimiento de acciones claves como:

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad.
- Comunicar en la entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año y en las que el Nominador deberá estar presente).

Propósito: Garantizar el liderazgo y el compromiso del comité institucional de gestión y desempeño o quien haga sus veces para conseguir los objetivos definidos para la implementación del MSPI.

Entradas recomendadas	Salidas
• 7.1.3 Definición del alcance del MSPI según lo que arroje el autodiagnóstico de cada entidad. • Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • 7.1.2 Necesidades y expectativas de los interesados	• Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.

7.2.2. Política de seguridad y privacidad de la información

Lineamiento: Se debe establecer en la política de seguridad y privacidad de la información los lineamientos y compromisos que se adoptaran para asegurar la confidencialidad, integridad y disponibilidad de la información, para ello debe tener en cuenta:

- Misión de la entidad.
- Normatividad vigente la cual se debe contar para el funcionamiento de la entidad.
- Establecer compromiso del cumplimiento de los requisitos relacionados con la seguridad y privacidad de la información, así como también el de la mejora continua que permita la reevaluación y actualización periódica de las medidas de seguridad para adaptarlas a la constante evolución de los riesgos y sistemas de protección. El personal calificado de la entidad supervisará, revisará y auditará la seguridad de la información. una vez el MSPI sea adoptado.
- Estar alineada con el contexto de la entidad, así como la identificación de las áreas que hacen parte de la implementación de seguridad de la información.
- Se deben asignar los roles y responsabilidades que se identifiquen.
- Ser incluidos y aprobados los temas de seguridad de la información y seguridad digital en el comité gestión y desempeño institucional.
- Ser comunicada al interior de la entidad y a los interesados que aplique.

Propósito: La política establece la base respecto al comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad.
Orientar y apoyar por parte de la alta dirección de la entidad a través del comité de gestión institucional, la gestión de la seguridad de la información de acuerdo con la misión de la entidad, normatividad y reglamentación pertinente

Entradas recomendadas	Salidas
• Comprensión de la organización y de su contexto. • Necesidades y expectativas de los interesados. • Definición del alcance del MSPI. • Requerimientos normativos y buenas prácticas de seguridad y privacidad de la información.	• Acto administrativo o acta de aprobación del Comité Institucional de Gestión y Desempeño con la adopción de la Política de seguridad y privacidad de la información

7.2.3. Roles y responsabilidades

Lineamientos:	Articular roles y responsabilidades con las áreas de la entidad para la adopción del MSPI, asegurando el monitoreo, reporte y aprobación ante el comité institucional. Los líderes de proceso deberán gestionar los riesgos de seguridad y privacidad de la información. Designar un responsable del MSPI con un equipo de apoyo, dependiente de un área estratégica distinta a la de Tecnología. Si no existe el cargo, deberá delegarse por acto administrativo e integrarse con voz y voto al comité de gestión institucional de gestión y desempeño y con voz al comité de control interno. Si no hay personal de planta, varias entidades podrán compartir un responsable de seguridad mediante contrato de servicios, justificando la falta de recursos, conforme al artículo 5 de la Resolución 500 sobre Estrategia de Seguridad Digital.
Propósito:	Es fundamental que los funcionarios y contratistas conozcan sus responsabilidades, comprendan el impacto de sus acciones en la seguridad de la información y entiendan cómo contribuyen a la implementación efectiva del MSPI.

Entradas recomendadas	Salidas
• 7.1.3 Definición del alcance del MSPI • Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	• Roles y responsabilidades en seguridad de la información de las diferentes áreas o procesos de la entidad. • Definición del rol de: responsable de seguridad de la información, indicando sus funciones y responsabilidades

7.3. Planeacion

7.3.1.Identificación de activos de información e infraestructura critica cibernética

Lineamiento:	Las entidades deben definir y aplicar un proceso de identificación y clasificación de los activos de información, que permita: • Identificar los activos de información que agregan valor al proceso y requieren protección, según el alcance y los procesos cubiertos por el MSPI. • Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información: Integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados. • Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso. • Identificar los activos de información con información personal en el inventario de activos de información. • Realizar la identificación y el inventario de infraestructura crítica y servicios esenciales de la entidad**.**
Propósito:	Estructurar una metodología que permita identificar y clasificar los activos de información

Entradas recomendadas	Salidas
• 7.1.3 Definición del alcance del MSPI • Modelo de procesos, y modelo organizacional, desarrollados para	• Procedimiento de inventario y clasificación de activos de información [2], del Modelo de

[2] Anexo 1. Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional

	la Arquitectura Misional de la entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional	Seguridad y Privacidad de la Información. • Documento metodológico de inventario y clasificación de la información. • Inventario de activos de información de cada proceso incluido en el alcance debidamente identificados, clasificados y valorados.

7.3.2. Valoración de los riesgos de seguridad de la información

Lineamiento	Las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita: • Identificar los riesgos que causen la pérdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la entidad dentro del alcance del MSPI. • Identificar los propietarios de los riesgos. • Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia. • Determinar el apetito de riesgos definido por la entidad. • Establecer criterios de aceptación de los riesgos. • Valorar los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información dentro del alcance del MSPI. • Determinar los niveles de riesgo. • Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral. • Priorización de los riesgos analizados para su tratamiento. • Se debe asegurar que las valoraciones repetidas de los riesgos de seguridad y privacidad de la información produzcan resultados consistentes, válidos y comparables.

	• Se recomienda realizar una evaluación de riesgos específica frente a amenazas avanzadas persistentes (APT) y vulnerabilidades emergentes, con el fin de ajustar las estrategias de seguridad a los ataques de alta sofisticación. • Se deben considerar los nuevos riesgos asociados a los dominios incluidos en la ISO/IEC 27001:2022, tales como amenazas avanzadas, entornos de nube, y riesgos en la cadena de suministro digital.
Propósito	Estructurar una metodología que permita identificar y clasificar los activos de información

Entradas recomendadas	**Salidas**

• 7.1.3 Definición del alcance del MSPI.
 	
• 7.2.2 Política de seguridad y privacidad de la información.
 	
• Directorio de servicios de componentes de información, de acuerdo con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.
 	
• Inventario de activos de información de la entidad usando:
 	
  ○ Proceso de valoración de riesgos de la seguridad de la información de acuerdo con lo definido en la Guía del DAPF
  ○ b) Reportes de debilidades o vulnerabilidades en los activos de información realizados por los colaboradores de la entidad o del resultado de auditorias
	• Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité institucional de gestión y desempeño.
	• Instrumento para la identificación y valoración de los riesgos de seguridad y privacidad de la información.

7.3.3. Plan de tratamiento de los riesgos de seguridad de la información

Lineamiento: Las entidades deben definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:

- Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.
- Elaborar una declaración de aplicabilidad que contenga: los controles adoptados por la entidad, su estado de implementación y la justificación de posible exclusión de acuerdo con los riesgos identificados y las capacidades técnicas y humanas con las que cuenta.
- Definir un plan de tratamiento de riesgos que contenga, fechas, acciones de tratamientos de riesgos a tratar y responsables con el objetivo de realizar trazabilidad.
- Los dueños de los riesgos que deben ser los dueños de los procesos afectados por estos riesgos, o las personas designadas por ellos. Deben realizar la aprobación formal del plan de tratamiento de riesgos y la aprobación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.

Propósito:

- Estructurar una metodología que permita definir las acciones que debe seguir la entidad para poder gestionar los riesgos de seguridad y privacidad de la información

Entradas recomendadas	Salidas
• Inventario de activos de información de la entidad. • 7.3.2 Valoración de los riesgos de seguridad de la información.	• Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia). • La aceptación de los riesgos residuales e indicación en que parte se deben aceptar. • Declaración de aplicabilidad, aceptada y aprobadas en el

	comité institucional de gestión y desempeño

7.4. Soporte

7.4.1. Recursos

Lineamiento:	Las entidades deben asegurar los recursos financieros, humanos y técnicos necesarios para adoptar, implementar y mantener el MSPI como un proceso transversal conforme al alcance definido.
Propósito:	Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI.

Entradas recomendadas	Salidas
• 7.1 Contexto • 7.1.3 Definición del alcance del MSPI. • 7.2.2 Política de seguridad y privacidad de la información. • 7.2.3 Roles y responsabilidades • 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información. • Plan de Seguridad y Privacidad de la Información. • Matriz de riesgos de seguridad y privacidad de la información. • Declaración de aplicabilidad. • Inventarios de activos de información, sistemas de información, infraestructura de TI y de sus administradores	• Incluir dentro de los proyectos de inversión de la entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido (esto involucra también al personal de seguridad de la información a contratar para el desarrollo de las actividades del SGSI). • Actualización del PETI de acuerdo con los recursos necesarios para realizar la gestión adecuada de los riesgos de seguridad de la información identificados y el plan de seguridad y privacidad de la información.

7.4.2. Competencia, toma de conciencia y comunicación

Lineamientos

Las entidades deben definir un plan de comunicación, capacitación, sensibilización y concientización para:

- Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.
- Involucrar al 100% de los colaboradores de la entidad en la implementación y gestión del MSPI.
- Concientizar a los colaboradores y partes interesadas en la importancia de la protección de la información.
- Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo.
- Tener un enfoque práctico en la respuesta a incidentes, especialmente en técnicas de phishing, ingeniería social y ciberhigiene, para fortalecer la capacidad de respuesta ante ataques dirigidos.
- Cuando proceda, tomar las acciones para adquirir y/o fortalecer la competencia de los responsables del MSPI.
- Evaluar la eficacia de las acciones de concientización y sensibilización realizadas.

Propósito

Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos los funcionarios conozcan la política, su rol en el MSPI y las implicaciones de no aplicar las reglas de seguridad y privacidad.

Entradas recomendadas

- 7.1.3 Definición del alcance del MSPI.
- 7.2.3 Roles y responsabilidades
- Manual de funciones de la entidad.

Salidas

- Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones - PIC.

• Plan de capacitación Institucional.	Plan de comunicaciones del modelo de seguridad y privacidad de la información

7.4.3. Información documentada

Lineamiento:	El modelo de seguridad y privacidad de la información de la entidad debe incluir: • Información documentada de los lineamientos establecidos. • Documentos que la entidad considere necesarios para la eficacia del SGSI. • Reglas claras para crear y actualizar documentos: identificación, formato, soporte, y control de versiones. • La información documentada debe estar disponible y ser adecuada para su uso, donde y cuando se necesite además de estar adecuadamente protegida
Propósito:	Mantener una documentación adecuada para que pueda ser consultada en cualquier momento por las partes interesadas y le permita conocer los detalles del sistema de gestión de seguridad de la información.

Entradas recomendadas	Salidas
• Lineamientos de las diferentes Fases del MSPI	• Políticas, manuales, procesos procedimientos guías, entre otros. • Inventario de activos, matriz de riesgos, planes de tratamiento, declaración de aplicabilidad, proceso de gestión de eventos, vulnerabilidades.

8. Fase 2: Operación

Tras finalizar la fase 7 de planeación del MSPI, se iniciará la implementación de los procesos de seguridad de la información: gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles. Se fomentará la cultura de seguridad y se definirán criterios de cumplimiento y mecanismos de control para procesos y servicios externos relevantes, asegurando su alineación con el SGSI. Los documentos que se deben generar en esta fase son:

- Actualización del inventario de información.
- Actualización de la matriz de riesgos de seguridad de la información.
- Plan de implementación de controles de seguridad.
- Actualización de la gestión de eventos e incidentes de seguridad de la información.
  Actualización de la gestión de vulnerabilidades.
  Evidencia de la implementación de los controles de seguridad de la información.

8.1. Control y planeación operacional

Lineamiento:	Las entidades deben realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos y el plan de Seguridad y Privacidad de la Información, esta información debe estar documentada para cada proceso según lo planificado, los planes de tratamiento deben ser definidos y aprobados por los lideres de proceso, Los proyectos o controles de seguridad que no pueden implementarse en el corto plazo o mediano plazo se deben escalar al comité institucional de gestión y desempeño para toma de decisiones y asignación de recursos. Las acciones que la entidad considere relevantes deben ser aprobadas por el comité institucional de gestión y desempeño. De igual manera, deben reforzar los mecanismos de monitoreo continuo, incluyendo la implementación de sistemas de alerta temprana que permitan a las entidades detectar y responder a incidentes en tiempo real, garantizando la resiliencia frente a ciberataques.
Propósito:	Implementar los planes y controles para lograr los objetivos del MSPI

Entradas recomendadas	***Salidas***
• 7.3.2 Valoración de los riesgos de seguridad de la información. • Anexo A 27001:2022	• Plan de seguridad y privacidad de la información que defina la implementación de controles de seguridad y privacidad de la información y contenga como mínimo: controles, actividades,

• Plan de 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información. • Plan de Seguridad y Privacidad de la Información	fechas, responsable de implementación y presupuesto. • Evidencia de la implementación de los controles de seguridad y privacidad de la información.

8.2. Plan de tratamiento de riesgos

Lineamiento:

- La entidad debe realizar evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos.
- La entidad debe conservar información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.
- La entidad debe implementar el plan de tratamiento de riesgos de seguridad de la información.
- La entidad debe conservar información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

Propósito: Establecer un proceso formal de identificación, evaluación y tratamiento de los riesgos de seguridad de la información

Entradas recomendadas	Salidas
• Inventario de activos de información • Incidentes de seguridad de la información • Eventos y reportes de amenazas y vulnerabilidades de seguridad e la información	• Matriz de riesgos de seguridad de la información. • Planes de tratamiento de los riesgos de seguridad e la información.

8.3. Definición de indicadores de gestión

Lineamiento:	La entidad debe definir indicadores que le permitan medir la evolución y avance en el nivel de madurez de la seguridad de la información.
Propósito:	Establecer indicadores para medir la gestión y madurez de la entidad en la implementación del modelo de seguridad y privacidad de la información

Entradas recomendadas	Salidas
• Política de seguridad de la información	• Indicadores de gestión de seguridad de la información

9. Fase 3: Evaluación de desempeño

Una vez culminada las actividades de la fase de operación del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de datos personales”, Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”, Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.

9.1. Seguimiento, medición, análisis y evaluación

Lineamiento:	Las entidades deben conocer sus avances en la implementación del modelo de Gobierno Digital, estableciendo tiempos y recursos para su monitoreo y reporte ante el Comité de Gestión y Desempeño, conforme al MIPG Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG. Los mecanismos utilizados para medir, analizar, monitorizar, evaluar y realizar seguimiento a la eficacia del Sistema deben ser comparables y reproducibles. Deberán incluir retroalimentación periódica que recoja la percepción de seguridad y las vulnerabilidades encontradas por los usuarios en cada entidad.
Propósito:	Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.

Entradas recomendadas	Salidas
• Documento con los resultados de la valoración de los riesgos. • Documento con los resultados del tratamiento de riesgos de seguridad de la información. • Resultado de la implementación de controles • Diagnóstico del MSPI • Plan de seguridad y privacidad de la información • Plan de concientización y sensibilización. • Reporte de incidentes presentados	• Hoja de vida de indicadores[3], los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el Decreto 612 de 2018. • Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.

[3] Para la definición de los indicadores se puede utilizar como guía los lineamientos de Indicadores de Gestión de Seguridad de la Información

9.2. Auditoría Interna

Lineamiento:	Realizar mínimo una auditoría interna al año con el fin de obtener información sobre el cumplimiento del MSPI.
Propósito:	Identificar no conformidades, desviaciones y oportunidades de mejora del MSPI

Entradas recomendadas	Salidas
• Todos los documentos producto de las salidas de las fases anteriores del MSPI. • El informe de los resultados de las evaluaciones independientes, seguimientos y auditorías. • Informes y compromisos adquiridos en los comités institucional de gestión y desempeño. • El informe de los incidentes de seguridad y privacidad de la información reportados y la solución de estos. • Informe sobre los cambios PESTEL[4] (legales, procesos, reglamentarios, regulatorios, tecnológicos, ambientales, o aquellos en el marco del contexto de la organización) en la entidad. • Indicadores definidos y aprobados para la evaluación del MSPI.	• Resultados de las auditorías internas. • No conformidades, hallazgos u oportunidades de mejora de las auditorías internas. • Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité de Coordinación de Control Interno.

[4] Factores análisis PESTEL (Factores políticos, factores económicos, factores sociales, factores tecnológicos, factores legales)

9.3. Revisión por la dirección

Lineamiento:	La Política y el Manual de Seguridad y Privacidad deben ser revisados y aprobados por el Comité de Gestión y Desempeño o por decisión del nominador, considerando los cambios en las necesidades de las partes interesadas.
Propósito:	Revisar el MSPI de la entidad, por parte de la alta dirección (comité Institucional de Gestión y Desempeño), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.

Entradas recomendadas	Salidas
• Los documentos de alto nivel del MSPI deberán ser aprobados, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la entidad.	• Revisión a la implementación. • Acta y documento de Revisión por la Dirección. • Compromisos de la Revisión por la Dirección.

10. Fase 4: Mejoramiento continuo

Una vez culminadas las actividades del MSPI de la fase evaluación y desempeño, se deben consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

10.1. Mejora continua

Lineamiento:	Las entidades deben contar con un plan de mejoramiento continuo que integre oportunidades de mejora, no conformidades y desviaciones, con acciones correctivas claras, responsables, tiempos y recursos definidos para fortalecer el MSPI.
Propósito:	Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

Entradas recomendadas	Salidas
• Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.	• Plan anual de mejora del MSPI que incluya los controles de seguridad a implementar, oportunidades de mejora, no conformidades y demás desviaciones identificadas en la

• Resultados de auditorías y revisiones independientes al MSPI.	gestión de los diferentes procesos de seguridad y privacidad de la información que componen el SGSI. • Plan estratégico de seguridad y privacidad de la información actualizado.

10.2. Acciones Correctivas y no conformidades

Lineamiento:	Ante una no conformidad, la entidad debe corregirla, mitigar sus efectos y evaluar acciones para evitar su repetición.
Propósito:	Identificar las no conformidades asociadas a la evaluación del MSPI y de los procesos.

Entradas recomendadas	Salidas
• Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.	• Plan anual de mejora del MSPI que incluya los controles de seguridad a implementar
• Resultados de auditorías y revisiones independientes al MSPI.	• Plan estratégico de seguridad y privacidad de la información actualizado.
• Incidentes de seguridad de la información	• Planes de acción para la remediación de las no conformidades

11. Anexo

11.1. Controles y objetivos de control

La siguiente tabla muestra los controles de seguridad detallando cada uno de los dominios establecidos en el anexo **A** de la norma NTC: ISO/IEC 27001:2022, los cuales tratan los 4 temas en los que se agrupan los 93 controles de seguridad de la información y se estructurarán tal como lo muestra la Tabla 1:

	Políticas especificas			
Núm.	**Nombre**	**Seleccionado / Excepción**	**Tema**	**Descripción / Justificación**
	Nombre	Control	#Proteccion	
	...			

Tabla 1 Estructura de los controles

Cada uno de los campos de la tabla anterior se definen de la siguiente manera:

- Núm.: Este campo identifica cada uno de los controles correspondientes al Anexo A |de la norma NTC: ISO/IEC 27001:2022.

- Nombre: Este campo hace referencia al nombre del control que se debe aplicar para dar cumplimiento a la política definida.

- Control: Este campo describe el control que se debe implementar con el fin de dar cumplimiento a la política definida.

- Tema: Este campo describe a que tipo de control pertenece (Dominios).

- Seleccionado / Excepción: El listado de controles además debe incluir un campo que permita ser utilizado para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado, lo cual ayuda a que la entidad tenga documentado y de fácil acceso el inventario de controles.

- Descripción / Justificación: El listado de controles cuenta con la descripción de cada control en la tabla. Adicionalmente, es posible utilizarlo para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado.

Núm.	Nombre	Descripción / Justificación
A.5	Controles organizacionales	
A.5.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes, que integren controles de ciberseguridad específicos para detectar y responder a incidentes, para garantizar un enfoque coordinado en la protección del ciberespacio
A.5.2	Roles y responsabilidades en la seguridad de la información	Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.5.3	Segregación de tareas	Control: Deben segregarse los deberes conflictivos y las áreas conflictivas de responsabilidad.
A.5.4	Responsabilidades de gestión	Control: La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.
A.5.5	Contacto con las autoridades	Control: Se deben mantener los contactos apropiados con las autoridades pertinentes.
A.5.6	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.5.7	Inteligencia de amenazas	Control: La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para generar información sobre amenazas. Se sugiere establecer un procedimiento formal de Inteligencia de amenazas de la seguridad de la información.
A.5.8	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.5.9	Inventario de activos de información y otros asociados a la misma	Control: Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios
A.5.10	Uso aceptable de activos de información y otros asociados a la misma	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.5.11	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.5.12	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Núm.	Nombre	Descripción / Justificación
A.5.13	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.5.14	Intercambio de la información	Control: Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
A.5.15	Control de Acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.5.16	Gestión de la identidad	Control: Debe gestionarse el ciclo de vida completo de las identidades.
A.5.17	Información de autenticación	Control: La asignación de la información secreta se debe controlar por medio de un proceso de gestión formal, además se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.5.18	Derechos de acceso	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.5.19	Seguridad de la información en la relación con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deberían documentar.
A.5.20	Requisitos de seguridad de la información en contratos con terceros	Control: Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo relación con el proveedor.
A.5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación)	Control: Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC
A.5.22	Gestión del cambio, revisión y monitoreo de los servicios del proveedor o suministrador	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.5.23	Seguridad de la información para el uso de servicios en la nube (cloud)	Control: Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.

Núm.	Nombre	Descripción / Justificación
A.5.24	Planeamiento y preparación de la gestión de incidentes de seguridad de la información	Control: Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.
A.5.25	Evaluación y decisión en los eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.5.26	Respuesta a los incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.5.27	Aprendizaje sobre los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
A.5.28	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.5.29	Seguridad de la información durante interrupciones	Control: La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.
A.5.30	Preparación de las TIC para la continuidad de negocio	Control: La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
A.5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Control: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.5.32	Derechos de propiedad intelectual	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.5.33	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.5.34	Privacidad y protección de la PII (Información Identificable Personal)	Control: La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales. Se recomienda incluir dentro del procedimiento de gestión de incidentes las actividades pertinentes para atender de manera diligente los

Núm.	Nombre	Descripción / Justificación
		incidentes relacionados con información personal de acuerdo a lo establecido en la ley 1581 del 2012.
A.5.35	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.5.36	Cumplimiento con las políticas, reglas y normas de la seguridad de la información	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.5.37	Procedimientos operacionales documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.
A.6	Controles de personas	
A.6.1	Revisión de antecedentes	Control: Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accede y los riesgos percibidos.
A.6.2	Términos y condiciones de empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.6.3	Concientización, educación y entrenamiento en seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberán recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.6.4	Proceso disciplinario	Control: Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra colaboradores que hayan cometido una violación a la seguridad de la información.
A.6.5	Responsabilidades luego de la finalización o cambio de empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.6.6	Acuerdos de confidencialidad o no revelación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Núm.	Nombre	Descripción / Justificación
A.6.7	Trabajo remoto	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza trabajo remoto.
A.6.8	Reportes de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.7	Controles físicos	
A.7.1	Perímetros de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.7.2	Entrada física	Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.7.3	Seguridad de oficinas, despachos e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.7.4	Supervisión de la seguridad física	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.7.5	Protección contra amenazas físicas y ambientales	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.7.6	Trabajo en áreas seguras	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.7.7	Escritorio y pantalla limpios	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.7.8	Emplazamiento y protección de equipos	Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.7.9	Seguridad de activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.7.10	Medios de almacenamiento	Control: Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
A.7.11	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.7.12	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta

Núm.	Nombre	Descripción / Justificación
		servicios de información debe estar protegido contra interceptación, interferencia o daño.
A.7.13	Mantenimiento de equipos	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.7.14	Eliminación o reutilización segura de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.8	Controles tecnológicos	
A.8.1	Dispositivos terminales de usuario	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.8.2	Derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.8.3	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A.8.4	Acceso al código fuente	Control: Se debe restringir el acceso a los códigos fuente de los programas.
A.8.5	Autenticación segura	Control: Las tecnologías y los procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
A.8.6	Gestión de la capacidad	Control: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.8.7	Protección contra código malicioso (malware)	Control: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.8.8	Gestión de vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.8.9	Gestión de la configuración	Control: Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.
A.8.10	Borrado de información	Control: La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.
A.8.11	Enmascarado de datos	Control: Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos

Núm.	Nombre	Descripción / Justificación
		personales, como se exige en la legislación y la reglamentación pertinentes. Se deben aplicar medidas como el cifrado, el control de acceso y el monitoreo del acceso y uso de estos datos, en alineación con legislaciones de privacidad relevantes ej: GDPR en Europa. Además, se deben aplicar técnicas de anonimización de datos cuando sea posible, siguiendo los lineamientos de la guía de anonimización de datos estructurados del archivo general de la nación u otras guías aplicables al respecto, reduciendo la cantidad de información personal que se almacena o se transmite innecesariamente.
A.8.12	Prevención de filtración de datos	Control: Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.
A.8.13	Respaldo de información	Control: Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.8.14	Redundancia de las instalaciones de procesamiento de información	Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.8.15	Registro	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.8.16	Actividades de supervisión	Control: Se deben producir, almacenar, proteger y analizar registros que registren actividades, excepciones, fallas y otros eventos relevantes.
A.8.17	Sincronización de reloj (clock)	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.8.18	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.8.19	Instalación de software en sistemas operacionales	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.8.20	Seguridad en redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.8.21	Seguridad de servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los

Núm.	Nombre	Descripción / Justificación
		servicios se presten internamente o se contraten externamente.
A.8.22	Segregación de redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.8.23	Filtrado web	Control: El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso.
A.8.24	Uso de criptografía	Control: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.8.25	Ciclo de vida de desarrollo seguro	Control: Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.
A.8.26	Requerimientos de seguridad en aplicaciones	Control: Los requerimientos relacionados con seguridad de la información se deben incluir en los requerimientos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.8.27	Principios de arquitectura de sistemas e ingeniería seguras	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.8.28	Generación de código seguro	Control: Los principios de codificación segura deben aplicarse al desarrollo de software.
A.8.29	Prueba segura en el desarrollo y aceptación	Control: La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
A.8.30	Desarrollo tercerizado	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.8.31	Separación de entornos de desarrollo, prueba y producción	Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.8.32	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.8.33	Información de prueba	Control: Asegurar la protección de los datos usados para pruebas.
A.8.34	Protección de sistemas de información durante pruebas de auditoría	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

Tabla 2: Controles del Anexo A del estándar ISO/IEC 27001:2022 y dominios a los que pertenece

TIC

Lineamientos de Roles y Responsabilidades

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de contenido

Tabla de contenido 55
Lineamientos de Roles y Responsabilidades 56
1. Objetivo 56
2. Alcance 56
3. Definicion de roles y responsabilidades 56
4. Identificación de los responsables 57
5. Identificación de los responsables 57
6. Perfiles y responsabilidades 57
6.1. Responsable de Seguridad de la Información para la entidad 57
Oficial de Protección de Datos Personales (OPD) **58**
6.2. Comité Institucional de Gestión y Desempeño Institucional – Comité de Seguridad y privacidad de la información 60
6.3. Oficina asesora Jurídica 61
6.4. Gestión del Talento Humano 62
6.5. Control Interno 62
6.6. Oficina Infraestructura Tecnológica 63
6.7. Funcionarios y contratistas 63
7. Arquitectura de seguridad de la información 64
7.1. Responsabilidades Del Equipo De Proyecto de implementación y gestión del MSPI 65
7.2. Comité o Mesa técnica de seguridad y privacidad de la información 66
7.3. Otras responsabilidades de Proveedores y Terceros 67

Listado de tablas

Tabla 3 Lineamientos Dominio de Arquitectura de Seguridad y sus evidencias 64

Lineamientos de Roles y Responsabilidades

Este documento busca orientar a la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, en la estructuración y documentación de la Matriz del grupo de Arquitectura Empresarial, el cual es el instrumento base sobre el cual se inicia la documentación del RRHH del área de TI.

La Matriz del grupo de Arquitectura hace parte de la arquitectura de TI de una entidad u organización y a grandes rasgos describe cada una de las personas que hacen parte de estas.

A continuación, se presentan los objetivos y alcance del Instructivo.

1. Objetivo

Definir la estructura organizacional para la gestión y operación MSPI en las entidades mediante una adecuada distribución de roles y responsabilidades.

2. Alcance

El presente documento involucra a todo el personal que forma parte del alcance del MPSI

3. Definicion de roles y responsabilidades

Una de las primeras metas para implementar un modelo de seguridad y privacidad de la información es que en todas las entidades se deben definir internamente las responsabilidades para ejecutar las actividades específicas de seguridad de la información designando a las personas apropiadas, documentando las competencias y formación necesaria para el personal encargado de la seguridad de la información.

La definición de roles dentro del MSPI es fundamental, ya que permite establecer de manera precisa las tareas y responsabilidades de cada miembro del equipo. Esto minimiza las ambigüedades y reduce el riesgo de imprecisiones en la ejecución de sus funciones, garantizando una gestión eficiente y alineada con los principios establecidos en la norma.

Partiendo de este punto, las entidades tendrán asegurado que cada actividad establecida dentro de la etapa de planeación del MSPI, tenga un responsable claro y de igual forma que cada uno de los miembros del equipo responsable de la ejecución entiendan claramente sus roles y responsabilidades.

4. Identificación de los responsables

Es fundamental garantizar la participación efectiva del personal de alto nivel en el desarrollo e implementación del Modelo de Seguridad de la Información (MSPI) dentro de la entidad. Su vinculación temprana en la planeación del proyecto permite establecer una base sólida para el éxito del modelo, asegurando el liderazgo y respaldo necesarios desde el inicio del proceso.

Los representantes de alto nivel deben identificar, conformar y organizar un grupo de trabajo multidisciplinario, compuesto por integrantes de todas las áreas de la entidad, el cual será responsable de la implementación del MSPI en las entidades del Estado. Este grupo debe ser designado con base en perfiles y roles definidos en el documento de política de seguridad de la información, en concordancia con la normativa aplicable, sin perjuicio de lo establecido en la Ley 489 de 1998. Cada entidad deberá determinar los plazos y mecanismos adecuados para cumplir con esta obligación en el menor tiempo posible.

Al finalizar este proceso, el equipo directivo encargado de la implementación del MSPI deberá formalizar y comunicar los perfiles, funciones y responsabilidades de los integrantes designados, asegurando su correcta alineación con los objetivos estratégicos de seguridad de la información de la entidad.

5. Identificación de los responsables

El equipo de gestión del proyecto en cada entidad tomará las medidas necesarias para planear, implementar y hacer seguimiento a las actividades necesarias para adoptar el Modelo de Seguridad de la Información al interior de su entidad y las actividades necesarias para una adecuada administración y sostenibilidad de este.

6. Perfiles y responsabilidades

A continuación, se proponen los siguientes roles y responsabilidades asociados a seguridad y privacidad de la información:

6.1. Responsable de Seguridad de la Información para la entidad

El responsable de seguridad y privacidad de la información u oficial de seguridad de la información tendrá a su cargo liderar y gestionar la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad y tendrá entre otras las siguientes responsabilidades principales:

- Definir y gestionar la normativa de seguridad y privacidad de la información y seguridad digital.

- Participar y reportar la gestión de seguridad y privacidad de la información en los comités institucionales relevantes.

- Promover la concientización, capacitación y mejora continua en materia de seguridad y privacidad de la información para todo el personal de la entidad.

- Definir, socializar e implementar los procedimientos relacionados con la gestión de seguridad y privacidad de la información al interior de la entidad.

- Asesorar y acompañar a las diferentes áreas de la entidad en la gestión de activos de información, riesgos, implementación de controles y definición de actividades de planes de tratamiento para mejorar la postura de seguridad en la entidad.

Oficial de Protección de Datos Personales (OPD)

La función del OPD en la organización es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta para cumplir el Régimen de Protección de Datos Personales de Colombia. Adicionalmente, es la de velar por la implementación de buenas prácticas de gestión de datos personales dentro de la entidad.

De esta manera, el OPD tendrá a su cargo la función de estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente.

Como función esencial de un OPD en la organización se encuentra la de supervisar el cumplimiento del Régimen General de Protección de Datos Personales. Acatando y cumpliendo todos los lineamientos que establezca la Superintendencia de Industria y Comercio como Autoridad Nacional de Protección de Datos Personales, en específico se le pueden asignar las siguientes responsabilidades:

- Recabar información para determinar las actividades de Tratamiento.

- Analizar y comprobar la conformidad con la normativa de las actividades de Tratamiento.

- Informar, asesorar y emitir recomendaciones al Responsable o al Encargado del Tratamiento.

- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del Tratamiento de Datos personales.

- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.

- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.

- Impulsar una cultura de protección de Datos personales en poder de la organización y su debida clasificación según su naturaleza.

- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio.

- Obtener las declaraciones de conformidad de la Superintendencia de Industria y Comercio cuando sea requerido.

- Obtener la certificación de las Normas Corporativas Vinculantes por parte de la Superintendencia de Industria y Comercio cuando sea requerido.

- Revisar los contenidos de los contratos de transferencias internacionales de Datos personales que se suscriban con otros Responsables del Tratamiento, ubicados o no en territorio colombiano.

- Revisar los contenidos de los contratos de transmisión internacional de Datos personales que se suscriban con Encargados del Tratamiento, ubicados o no en territorio colombiano.

- Analizar la responsabilidad de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de Datos personales específico para cada uno de ellos.

- Realizar un entrenamiento general en protección de Datos personales para todos los empleados de la compañía.

- Proyectar la documentación relacionada con la recolección y tratamiento de los datos personales.

- Realizar el entrenamiento necesario a los nuevos colaboradores, que tengan acceso por las condiciones de sus contratos a Datos personales gestionados por la organización.

- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers, gestión de proveedores, etc.)

- Medir la participación y calificar el desempeño, en los entrenamientos de protección de datos Personales.

- Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre Datos personales.

- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de Tratamiento de información personal.

- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.

- Realizar seguimiento al Programa Integral de Gestión de Datos Personales.

Nota: Supervisar la observancia no significa que el OPD sea personalmente Responsable de cualquier caso de inobservancia al Régimen General de Protección de Datos Personales.

Las Leyes Estatutarias 1266 de 2008 y 1581 de 2012 establecen claramente los sujetos obligados ante la ley y quienes están obligados a “ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado las medias apropiadas y efectivas para cumplir con las obligaciones establecidas”.

Por eso, el cumplimiento de las normas en materia de protección de datos es responsabilidad del Responsable / Encargado del Tratamiento, no del OPD.

6.2. Comité Institucional de Gestión y Desempeño Institucional – Comité de Seguridad y privacidad de la información

El Comité Institucional de Gestión y Desempeño debe tratar los temas de seguridad y privacidad de la información asegurando la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:

- Aprobar y realizar seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información.

- Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.

- Aprobar acciones y mejores prácticas que contribuyan en la implementación del MSPI.
- Promover la gestión de seguridad de la información en los procesos y cultura organizacional.
- Vigilar el cumplimiento de la normatividad relacionada con la implementación de la seguridad de la información.
- Asegurar que se logren los resultados previstos del MPSI, con un enfoque de mejora continua del referido modelo.
- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.
- Gestión de crisis y continuidad del negocio con la finalidad asegurar la capacidad de recuperación ante incidentes graves
- Presentación de indicadores de desempeño para medir la efectividad en la gestión de la seguridad de la información y los resultados de monitoreo de la eficacia de las políticas y procedimientos establecidos

Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

6.3. Oficina Asesora Jurídica

Corresponde a la Oficina Asesora Jurídica:

- Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.
- Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.
- Realizar el seguimiento y la interpretación de las nuevas regulaciones y normativas que impacten el MSPI.
- Asesorar a las áreas de la entidad sobre las obligaciones legales y los requisitos de cumplimiento en materia de seguridad de la información y protección de datos.

- Apoyar los lineamientos de seguridad para la gestión con proveedores.
- Verificar que las políticas y procedimientos del MSPI se ajusten a la normativa vigente.

6.4. Gestión del Talento Humano

Controlar y salvaguardar la información personal de los funcionarios de planta de la entidad, asegurando su tratamiento conforme a la normatividad vigente.

- Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.
- Implementar procesos de selección que incluyan verificación de antecedentes y evaluaciones de confiabilidad con criterios de seguridad de la información.
- Garantizar la firma de acuerdos de confidencialidad y compromiso con la protección de datos desde la vinculación.
- Integrar el entrenamiento en seguridad de la información dentro del proceso de inducción y reinducción del personal
- Apoyar al responsable de Seguridad de la Información en la implementación del plan de concientización y sensibilización en seguridad y privacidad de la información.

6.5. Control Interno

- En el marco de su Plan Anual de Auditoría, la Oficina de Control Interno o quien haga sus veces debe incluir auditorías técnicas y de gestión de seguridad de la información.
- Se deben definir responsables de planificar, ejecutar y reportar las auditorías de seguridad de la información, asegurando que cuenten con la competencia y formación necesarias para evaluar la efectividad de los controles del MSPI.
- Se debe establecer la efectividad de los controles para asegurar el cumplimiento de la normativa vigente en materia de seguridad de la información y protección de datos personales, a través de sus procesos de seguimiento y evaluación.
- Las responsabilidades principales del encargado de realizar las auditorias técnicas y de gestión de seguridad de la información son:
    - Realizar auditorías internas de seguridad de la información
    - Evaluar la efectividad de los controles de seguridad de la información
    - Identificar no conformidades, desviaciones y oportunidades de mejora del MSPI
    - Informar sobre los resultados de las auditorías

- Coordinar actividades con otras áreas (ej. Oficina Asesora de Planeación)
- Realizar seguimiento al cumplimiento normativo

Su función primordial es la de proporcionar una evaluación independiente y objetiva sobre la eficacia del sistema de gestión de seguridad de la información, identificando áreas de riesgo y proponiendo mejoras para garantizar el cumplimiento de los objetivos y la normativa aplicable.

6.6. Oficina de Infraestructura Tecnológica

Será responsable de:

- Identificar los activos de información de los cuales es Responsable y Encargado.
- Gestionar los riesgos de seguridad de la información de los activos a su cargo.
- Asesorar a las otras dependencias en los procesos de identificación e implementación de controles.
- Implementar los controles de seguridad de la información de la infraestructura a su cargo.
- Apoyar al Responsable de Seguridad de la Información y del Oficial de Protección de Datos en los temas de su competencia.

6.7. Funcionarios y contratistas

A continuación, se detallan las responsabilidades principales de los funcionarios y contratistas de la entidad:

- Aplicar las políticas y procedimientos de seguridad de la información.
- Cumplir con los roles y responsabilidades asignados.
- Gestionar los riesgos de seguridad y privacidad de la información inherentes a los procesos
- Participar activamente en los programas de capacitación y sensibilización sobre seguridad de la información.
- Identificar y clasificar los activos de información bajo su responsabilidad.
- Actuar como propietarios o custodios de la información, garantizando la protección de los activos

7. Arquitectura de seguridad de la información

Dentro de la definición de lineamientos en cada uno de los Dominios entregados en el Marco de Arquitectura Empresarial, está contemplado el Dominio de Arquitectura de Seguridad el cual debe cumplir con lo siguiente:

LINEAMIENTO	NOMBRE	DESCRIPCIÓN	EVIDENCIAS
MAE.LI.AS.01	Catálogo de servicios de seguridad de la información y ciberseguridad	Las entidades de la administración pública deben contar con un catálogo de servicios de seguridad que comprende una lista de servicios que proporcionan e identifican funciones específicas de seguridad para los sistemas de información y una lista de servicios institucionales relacionados con seguridad de la información y ciberseguridad.	Catálogo de servicios de seguridad con base en los requerimientos identificados en los demás dominios.
MAE.LI.AS.02	Análisis de impacto del negocio	Las entidades de la administración pública deben realizar el análisis de impacto de negocio para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afecten las operaciones regulares de las organizaciones. Este análisis debe ser incorporado en el diseño de la o las arquitecturas de seguridad y formar parte del sistema de gestión de riesgos y ser utilizado como mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencias.	Informe de análisis de impacto de negocio de acuerdo con el alcance definido por la entidad.
MAE.LI.AS.03	Arquitectura de Seguridad	Las entidades de la administración pública deben definir, evolucionar y aplicar una arquitectura de seguridad sobre la infraestructura tecnológica, los sistemas de información y los datos durante la ejecución de los ejercicios de arquitectura empresarial	Arquitectura de seguridad que incluya todos los artefactos que faciliten su entendimiento e implementación.
MAE.LI.AS.04	Ciberseguridad	Las entidades de administración pública deben diseñar los controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la información identificados durante la ejecución de los ejercicios de arquitectura empresarial.	Controles de seguridad identificados en la entidad.

Tabla 3 Lineamientos Dominio de Arquitectura de Seguridad y sus evidencias

Según la naturaleza de la entidad, debe conformarse un equipo para desarrollar el proyecto de implementación del MSPI al que deben pertenecer miembros directivos y representantes de las áreas misionales, para asegurar que toda la información más relevante de la entidad esté disponible oportunamente. Así se busca asegurar que sea una iniciativa transversal a la entidad, y que no dependa de la oficina o área de TI.

|Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol. De esta forma, y de manera general se pone a consideración el siguiente

listado para que las entidades analicen de acuerdo con su composición orgánica cuales deben ser los miembros del equipo de seguridad y privacidad de la información, de acuerdo con los siguientes perfiles:

- Personal de seguridad de la información.
- Un representante del área de Tecnología.
- Un representante del área de Control Interno.
- Un representante del área de Planeación.
- Un representante de sistemas de Gestión de Calidad.
- Un representante del área Jurídica.
- Funcionarios, proveedores, y ciudadanos

La necesidad del compromiso de la Alta dirección de la entidad es necesario, así se presenta la figura No. 01, donde se presentan los perfiles de manera genérica el nivel al que pertenecerían según lo propuesto.

Ilustración 2 Equipo de Gestión de Seguridad de la Información en las entidades

7.1. Responsabilidades Del Equipo De Proyecto de implementación y gestión del MSPI

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.

- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.

- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.

- Las que considere el líder del proyecto o el comité institucional de Gestión y Desempeño.

De manera particular se resaltan dos perfiles que deben estar participando de manera activa durante el desarrollo del proyecto, a pesar de que el proyecto no es de responsabilidad exclusiva del área de TI su papel es fundamental, y de acuerdo con la Ley de Protección de Datos Personales se debe tener muy presente el rol del Oficial de Protección de Datos Personales y el Responsable de seguridad de la información u oficial de seguridad de la información.

Teniendo en cuenta que el responsable u Oficial de Protección de Datos Personales en la entidad, es quien tiene decisión sobre las bases de datos que contengan este tipo de datos y que el responsable es quien direcciona las actividades de los encargados de los datos personales (quien realiza el tratamiento directamente), adicional a las responsabilidades arriba citadas, se tendrá en cuenta que los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales de acuerdo a la Ley 1581 de 2012 " Protección de Datos Personales" son:

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.

- Tramitar las consultas, solicitudes y reclamos.

- Utilizar solo los datos personales obtenidos mediante autorización, salvo que no la requieran.

- Respetar las condiciones de seguridad y privacidad de información del titular.

- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

7.2. Comité o Mesa técnica de seguridad y privacidad de la información

En caso de considerarlo pertinente, la entidad podrá establecer un Comité o Mesa Técnica de Seguridad y Privacidad de la Información, como instancia de apoyo al Comité Institucional de Gestión y Desempeño. Esta instancia podrá abordar aspectos especializados relacionados con la arquitectura de seguridad de la información, análisis y correlación de logs, gestión de eventos e incidentes, tratamiento de vulnerabilidades, así como aspectos normativos y

técnicos asociados al tratamiento de información pública clasificada, reservada y datos personales. Las decisiones o recomendaciones técnicas de esta mesa deberán ser elevadas al Comité Institucional para su validación y seguimiento, asegurando su alineación con la política institucional, los requisitos legales vigentes y los lineamientos del MSPI y la norma ISO/IEC 27001.

7.3. Otras responsabilidades de Proveedores y Terceros

Teniendo en cuenta la importancia de la gestión de la seguridad de la información en las entidades, es primordial establecer responsabilidades de proveedores externos, especialmente aquellos que interactúan con activos de información críticos de la entidad, como proveedores de servicios en la nube o la cadena de suministro de las TIC. Dentro de las responsabilidades se detallan las siguientes:

- Implementar y mantener los controles de seguridad de la información acordados contractualmente.
- Cumplir con la política de seguridad de la información de la entidad y las políticas específicas del tema que les sean aplicables
- Proteger la confidencialidad, integridad y disponibilidad de la información de la entidad
- Garantizar el uso aceptable de la información y otros activos asociados
- Informar sobre el cumplimiento de los requisitos de seguridad de la información
- Permitir la realización de auditorías para verificar el cumplimiento de los requisitos de seguridad.
- Gestionar de manera segura el acceso a la información y otros activos asociados.
- Notificar de manera oportuna los incidentes de seguridad de la información.
- Cooperar en la gestión y resolución de incidentes de seguridad.
- Asegurar la devolución de todos los activos de la organización al finalizar el contrato o acuerdo.
- Cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales aplicables.
- Tener una gestión adecuada de la seguridad de la información, especialmente si manejan información clasificada o reservada.

- Colaborar en la gestión de incidentes de seguridad y notificar oportunamente cualquier evento adverso

- Para proveedores de servicios en la nube, garantizar la portabilidad de los datos y la interoperabilidad de los servicios-

Responsabilidades de los ciudadanos

- Uso responsable de los servicios digitales ofrecidos por las entidades.

TIC

Lineamientos de Indicadores de Gestión de Seguridad de la Información

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de contenido

Tabla de contenido 71
Listado de Tablas 71
Lineamientos de Indicadores De Gestión De Seguridad De La Información 72
1. Objetivo de la medición 72
2. Construcción de indicadores 72
2.1. Identificación Del Objeto De La Medición 73
2.2. Definición De Las Variables 73
2.3. Criterios de selección y calidad de los datos 73
2.4. Diseño Del Indicador 73
3. Relación con otros marcos de referencia 74
4. Indicadores Propuestos 75

Listado de Tablas

Tabla 4 Criterios para selección de indicadores 74
Tabla 5 Relación con otros marcos de referencia 74

Lineamientos de Indicadores De Gestión De Seguridad De La Información

1. Objetivo de la medición

La creación de indicadores de gestión está orientada principalmente a la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora.

Los objetivos de estos procesos de medición en seguridad de la información son:

- Evaluar la efectividad de la implementación de los controles de seguridad.
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumos al plan de análisis y tratamiento de riesgos.
- Permitir que se cuente con un proceso que demuestre si está siendo eficaz y está llegando a su punto de equilibrio dentro del sistema de gestión de seguridad de la información.

Nota: Los objetivos de seguridad deben ser monitoreados, y este monitoreo debe estar disponible como “información documentada”

2. Construcción de indicadores

Acorde con la “Guía para Diseño, Construcción e Interpretación de Indicadores del DANE” , para la construcción de indicadores se debe tener en cuenta un tratamiento adecuado de la información que será la base del proceso de revisión control y mejora, de esta forma, dentro de la elaboración de indicadores se tienen definidos cuatro etapas específicas, como se menciona a continuación:

2.1. Identificación Del Objeto De La Medición

En este primer paso los encargados de la implementación del MSPI, deben tener en cuenta el Plan de Seguridad de la Información que se ha definido y de esta manera se desarrolla el objeto de medición sobre los aspectos que consideren más relevantes para evaluar, determinar qué tan fácil es recolectar la información asociada y que herramientas estoy empleando para obtener dicha información.

2.2. Definición De Las Variables

Una vez determinado el objeto de la medición, se definirán los aspectos que precisarán los datos que se recolectarán al levantar la información, así se determinarán los insumos, puntos de control, herramientas usadas y la relación entre estos aspectos o variables de medición.

En este sentido, las variables, una vez identificadas, deben ser definidas con la mayor rigurosidad, asignándole un sentido claro, para evitar que se originen ambigüedades y discusiones sobre sus resultados. Así mismo, se debe tener claridad de quién y cómo produce dicha información para de esta forma mejorar el criterio de confiabilidad.[5]

2.3. Criterios de selección y calidad de los datos

El punto inicial es determinar si el indicador que se está eligiendo es de interés para la alta dirección, si va a permitir al líder de proyecto (el encargado de la seguridad de la información de la entidad) identificar la efectividad no solo del avance en la implementación, sino que, con esta recolección, medición y seguimiento del proyecto se logra demostrar cómo éste aporta al objetivo misional de la entidad.

Finalmente, es importante que el indicador sea sencillo de expresar, leer e interpretar, y como se menciona en la guía para la Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Nacional de Planeación, debe elaborarse metodológicamente de forma sencilla, automática, sistemática y continua.

2.4. Diseño Del Indicador

El diseño del indicador implica, además, la realización de ciertas actividades o etapas que deben contemplarse en el proceso definitivo de construcción de indicadores.

[5] GUÍA PARA LA CONSTRUCCIÓN Y ANÁLISIS DE INDICADORES, Departamento Nacional de Planeación.

Criterio de selección	Pregunta a tener en cuenta	Objetivo
Pertinencia	¿El indicador expresa qué se quiere medir de forma clara y precisa?	Busca que el indicador permita describir la situación o fenómeno determinado, objeto de la acción.
Funcionalidad	¿El indicador es monitoreable?	Verifica que el indicador sea medible, operable y sensible a los cambios registrados en la situación inicial
Disponibilidad	¿La información del indicador está disponible?	Los indicadores deben ser construidos a partir de variables sobre las cuales exista información estadística de tal manera que puedan ser consultados cuando sea necesario.
Confiabilidad	¿De donde provienen los datos?	Los datos deben ser medidos siempre bajo ciertos estándares y la información requerida debe poseer atributos de calidad estadística.
Utilidad	¿El indicador es relevante con lo que se quiere medir?	Que los resultados y análisis permitan tomar decisiones.

Tabla 4 Criterios para selección de indicadores

Fuente: Guía para Diseño, Construcción e Interpretación de Indicadores. Metodología línea base de indicadores, DANE 2009.

3. Relación con otros marcos de referencia

A continuación, se detalla una validación de la metodología utilizada con el marco de referencia ISO/IEC 27004:2016 (Gestión de métricas de seguridad de la información) y el marco de referencia de la NIST SP 800-55.

Aspecto	Guía del DANE	ISO/IEC 27004:2016	NIST SP 800-55 Rev.1
Propósito	Diseñar y construir indicadores de gestión institucional	Medir la eficacia del SGSI conforme a ISO/IEC 27001	Evaluar desempeño de controles de seguridad de la información
Enfoque	Evaluación de gestión pública y política basada en indicadores	Evaluación de controles y procesos dentro del SGSI	Evaluación de desempeño técnico, operacional y de impacto
Tipo de indicadores	Resultado, Producto, Eficiencia, Calidad, Impacto	Desempeño, Eficacia, Cumplimiento	Implementación, Eficacia, Eficiencia, Impacto
Ciclo de medición	Definir → Diseñar → Recolectar → Analizar → Interpretar	Planear → Medir → Analizar → Mejorar	Seleccionar → Desarrollar → Implementar → Analizar → Usar
Nivel de especificidad técnica	Media, orientada a procesos organizacionales y gestión institucional	Alta, con métricas alineadas a controles ISO/IEC 27001	Alta, orientada a sistemas de TI y operaciones de seguridad
Estructura del indicador	Nombre, definición, unidad, fórmula, frecuencia, fuente, interpretación	Objetivo, medida, fórmula, unidad, frecuencia, responsable, interpretación	Atributo, medida, fórmula, fuente, periodicidad, nivel de impacto
Marco normativo asociado	CONPES, Ley 87, Sistema de Gestión (MIPG)	ISO/IEC 27001 (SGSI)	NIST SP 800-53 (controles de seguridad)

Tabla 5 Relación con otros marcos de referencia

Nota. Tener presente que el marco de referencia a utilizar para la definición de indicadores es de acuerdo como lo tenga definido la entidad en su sistema de calidad.

4. Indicadores Propuestos

A continuación, se definen una serie de indicadores para medir la gestión y el cumplimiento en el avance de la implementación del Modelo de Seguridad y Privacidad de la Información.

Estos indicadores son ejemplos que pueden ser adoptados por las entidades o modificados de acuerdo con sus necesidades.

<table>
<tr><td colspan="6">INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.</td></tr>
<tr><td colspan="2">IDENTIFICADOR</td><td colspan="4">SGIN01</td></tr>
<tr><td colspan="6">DEFINICIÓN</td></tr>
<tr><td colspan="6">El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad</td></tr>
<tr><td colspan="6">OBJETIVO</td></tr>
<tr><td colspan="6">Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información por parte de la alta dirección.</td></tr>
<tr><td colspan="6">TIPO DE INDICADOR</td></tr>
<tr><td colspan="6">Indicador de Gestión</td></tr>
<tr><td colspan="2">DESCRIPCIÓN DE VARIABLES</td><td colspan="2">FORMULA</td><td colspan="2">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VSI01: Número de personas que conforman el equipo de seguridad de la información con su respectivo rol y responsabilidades asignadas.</td><td colspan="2" rowspan="2">(VSI01/VSI02) *100</td><td colspan="2">Lineamientos de roles y responsabilidades.</td></tr>
<tr><td colspan="2">VSI02: Número de personas que deberían conformar el equipo de seguridad de la información según la estructura definida por la entidad y que tengan responsabilidades de seguridad de la información definidas.</td><td colspan="2">Actas de asignación de personal.</td></tr>
<tr><td colspan="6">METAS</td></tr>
<tr><td>MÍNIMA</td><td>75-80%</td><td>SATISFACTORIA</td><td>80- 90%</td><td>SOBRESALIENTE</td><td>100%</td></tr>
<tr><td colspan="6">OBSERVACIONES</td></tr>
</table>

Según los lineamientos establecidos en la sección de Roles y responsabilidades, hay que crear nuevos cargos y asignar responsabilidades en los actuales, por lo que el indicador está enfocado, no solo a la contratación de nuevas personas, sino a la asignación de responsabilidades.

INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.					
IDENTIFICADOR	SGIN02				
DEFINICIÓN					
El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos **críticos** de información de una entidad y los controles aplicados.					
OBJETIVO					
Hacer un seguimiento a la inclusión de nuevos activos críticos de información y sus controles, dentro del marco de seguridad y privacidad de la información.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI03: Número de activos de información críticos incluidos en la gestión de riesgos de seguridad de la información con controles identificados.		(VSI03/VSI04) *100		Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos	
VSI04: Número de activos de información críticos identificados en el inventario de activos de información.				Inventario de Activos de información.	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80-90%	SOBRESALIENTE	100%
OBSERVACIONES					
Los indicadores de cada proceso deben recolectarse y promediarse para construir un indicador que refleje el estado general de la entidad. 'Incluir un activo' implica gestionar su ciclo completo: clasificarlo, evaluar sus riesgos, definir controles para mitigarlos y aplicar el tratamiento correspondiente.					

Este indicador mide la proporción de activos de información que han sido identificados como críticos (según el procedimiento de identificación, clasificación y valoración de activos de la entidad) y que están cubiertos por controles de seguridad.

INDICADOR 03 - TRATAMIENTO DE EVENTOS O INCIDENTES DE SEGURIDAD RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
IDENTIFICADOR	SGIN03				
DEFINICIÓN					
Mide la eficiencia en la resolución de eventos e incidentes de seguridad de la información, reportados o detectados, con base en su cierre dentro del tiempo objetivo establecido por la entidad.					
OBJETIVO					
Evaluar la capacidad de la entidad para gestionar y resolver oportunamente los eventos e incidentes de seguridad de la información.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI05: Número de eventos o incidentes cerrados dentro del tiempo objetivo.		(VSI05/VSI06) *100		Auditorías internas, herramientas de atención de servicios	
VSI06: Número total de eventos o incidentes reportados o detectados.				Auditorías internas, herramientas de atención de servicios	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80- 90%	SOBRESALIENTE	100%
OBSERVACIONES					
La clasificación y priorización de los eventos e incidentes de seguridad se realiza conforme a los criterios establecidos en el procedimiento de gestión de incidentes de seguridad de la información de la entidad.					

INDICADOR 04 – CUMPLIMIENTO DEL PLAN DE SENSIBILIZACIÓN					
IDENTIFICADOR	SGIN04				
DEFINICIÓN					
El indicador permite medir cuántos usuarios aplican correctamente lo aprendido en las actividades de sensibilización en seguridad de la información.					
OBJETIVO					
El indicador pretende establecer la efectividad del plan de sensibilización en seguridad de la información y determinar si los usuarios finales aplican correctamente los conocimientos adquiridos en las actividades de sensibilización, como evidencia de la efectividad del plan.					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI07: Número de usuarios evaluados que aplicaron correctamente los contenidos sensibilizados.		(VSI07/VSI08) *100		Oficial de Seguridad de la Información, auditorías internas, atención al usuario, listas de asistencia, resultados de evaluaciones realizadas.	
VSI08: Total de personal capacitado durante el periodo evaluado.				Total, de funcionarios de la entidad.	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80-90%	SOBRESALIENTE	100%
OBSERVACIONES					
La evaluación debe incluir actividades prácticas, simulaciones o pruebas que midan la apropiación y aplicación de los contenidos sensibilizados.					

INDICADOR 05 – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
IDENTIFICADOR SGIN05
DEFINICIÓN
Mide el grado de cumplimiento de las políticas de seguridad y privacidad de la información en la entidad, con base en criterios definidos relacionados con existencia de política, organización interna y cumplimiento normativo.

OBJETIVO			
Determinar si la entidad ha definido e implementado adecuadamente las políticas de seguridad de la información, y si cumple con los aspectos organizativos y normativos requeridos.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI09: ¿Existe una política general de seguridad de la información formalizada y vigente?		(VSI09 + VSI10 + VSI11) / 3 * 100	Usuarios Internos
VSI10: ¿Existe una estructura organizativa con roles y responsabilidades claras?			Usuarios Internos
VSI11: ¿Se da cumplimiento a requisitos legales, reglamentarios y contractuales en el tratamiento de la información?			Usuarios Internos
METAS CUMPLE SI / NO CUMPLE NO			
MÍNIMA 75-80%	**SATISFACTORIA** 80-90%	SOBRESALIENTE	100%
OBSERVACIONES			
La validación de este indicador debe hacerse mediante revisión documental y entrevistas con responsables del SGSI, conforme a los lineamientos del Modelo de Operación de la Entidad. Se recomienda su actualización anual o tras cambios normativos o estructurales.			

INDICADOR 06 - CUMPLIMIENTO DE LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
IDENTIFICADOR	SGIN06
DEFINICIÓN	
Mide el nivel de cumplimiento de los lineamientos establecidos por la entidad para la gestión de la seguridad y privacidad de la información, considerando tanto su definición formal como su aplicación efectiva.	
OBJETIVO	
Evaluar si la entidad cuenta con lineamientos definidos y aplicados en materia de seguridad y privacidad de la información, y si estos son conocidos y adoptados por los funcionarios y contratistas como parte de sus responsabilidades.	
TIPO INDICADOR	
Indicador de Cumplimiento	

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI12: Evidencia de lineamientos aplicados por funcionarios y contratistas que contribuyen a minimizar los riesgos sobre los activos de información.	(VSI12 / VSI13) * 100	lineamientos formales, encuestas a funcionarios
VSI13: Evidencia de lineamientos definidos para cumplir las políticas de seguridad de la información.		lineamientos formales, encuestas a funcionarios

METAS			
MÍNIMA 75-80%	**SATISFACTORIA** 80-90%	SOBRESALIENTE	100%

OBSERVACIONES
La verificación debe realizarse mediante revisión documental de los lineamientos institucionales, encuestas o entrevistas a funcionarios y contratistas, y observación directa de medidas implementadas para proteger la información. Se recomienda realizar esta evaluación al menos una vez al año o cuando se actualicen las políticas de seguridad y privacidad de la información de la entidad.

INDICADOR 07 – EFECTIVIDAD OPERATIVA DEL CONTROL DE ACCESO	
IDENTIFICADOR	SGIN07
DEFINICIÓN	
Mide la efectividad de los controles de acceso implementados, con base en la detección y gestión de accesos no autorizados o intentos de acceso fallidos.	
OBJETIVO	
Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad.	
TIPO INDICADOR	
Indicador de Cumplimiento	

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI14: Número de accesos no autorizados detectados	VSI14/VSI15 * 100	Revisión documental de políticas y procedimientos, entrevistas con responsables de TI, y evidencia de difusión o implementación.

VSI15: Total de intentos de acceso			Revisión documental de políticas y procedimientos, entrevistas con responsables de TI, y evidencia de difusión o implementación.
METAS			
MÍNIMA 75-80%	SATISFACTORIA 80-90%	SOBRESALIENTE	100%
OBSERVACIONES			
La verificación debe realizarse mediante revisión documental de políticas y procedimientos, entrevistas con responsables de TI, y evidencia de difusión o implementación. Se recomienda su evaluación anual.			

INDICADOR 08– CUMPLIMIENTO DE LINEAMIENTOS PARA EL ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE			
IDENTIFICADOR	SGIN08		
DEFINICIÓN			
Mide el nivel de cumplimiento de la entidad en cuanto a la existencia de lineamientos, normas o estándares que aseguren la incorporación de criterios de seguridad de la información en el desarrollo, adquisición y mantenimiento de software y servicios tecnológicos.			
OBJETIVO			
Verificar si la entidad ha definido e implementado lineamientos formales que aseguren la protección de los servicios tecnológicos en las fases de adquisición, desarrollo y mantenimiento de software, incluyendo la gestión de incidentes asociados.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI17: ¿La entidad ha definido y documentado lineamientos, normas o estándares para el desarrollo o adquisición segura de software, sistemas y aplicaciones?		(VSI17 + VSI18) / 2 * 100	Usuarios Internos / Documentación técnica

¿La entidad ha establecido lineamientos para la gestión de incidentes relacionados con fallas o vulnerabilidades en los servicios de software?		Usuarios Internos / Procedimientos

METAS			
CUMPLIMIENTO TOTAL	100%	CUMPLIMIENTO PARCIAL 50%	NO CUMPLE 0%

OBSERVACIONES

La verificación debe realizarse mediante revisión documental de lineamientos sobre desarrollo/adquisición de software, análisis de contratos o convenios, entrevistas con responsables de TI y revisión de reportes de incidentes relacionados con software. La evaluación debe actualizarse al menos anualmente o cuando se implementen nuevos servicios.

INDICADOR 09 – CUMPLIMIENTO DE LINEAMIENTOS DE REGISTRO Y AUDITORÍA EN SEGURIDAD DE LA INFORMACIÓN		
IDENTIFICADOR	SGIN09	
DEFINICIÓN		
Mide el cumplimiento de la entidad en cuanto a la definición e implementación de lineamientos, normas y/o estándares relacionados con el registro de eventos y auditorías de seguridad de la información.		
OBJETIVO		
Verificar si la entidad cuenta con directrices formalizadas para registrar eventos de seguridad y auditar periódicamente sus sistemas, con el fin de garantizar trazabilidad y mejora continua del modelo de seguridad.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI19: ¿La entidad ha definido y aplica lineamientos o estándares para el registro y control de eventos en sus sistemas, redes y servicios?	(VSI19 + VSI20) / 2 * 100	Documentación institucional, revisión de logs, entrevistas

VSI20: ¿La entidad realiza auditorías internas o externas periódicas sobre sus procesos y controles de seguridad de la información?			Informes de auditoría, cronogramas de verificación
METAS			
CUMPLIMIENTO TOTAL	100%	CUMPLIMIENTO PARCIAL 50%	NO CUMPLE 0%
OBSERVACIONES			
La verificación debe realizarse mediante revisión de lineamientos internos, políticas, bitácoras o registros de eventos, y evidencia de auditorías internas o de terceros. Es recomendable evaluar al menos una vez al año y cada vez que se actualicen los sistemas críticos.			

|

INDICADOR 10 – IMPLEMENTACIÓN DE MECANISMOS PARA LA DETECCIÓN DE ANOMALÍAS EN LA INFRAESTRUCTURA Y SERVICIOS DE INFORMACIÓN			
IDENTIFICADOR			
DEFINICIÓN	SGIN10		
Mide el nivel de implementación de mecanismos y herramientas en la entidad para detectar de manera proactiva vulnerabilidades, fallas o comportamientos anómalos que puedan afectar la seguridad en su infraestructura tecnológica, redes, sistemas, aplicaciones y servicios.			
OBJETIVO			
Verificar si la entidad ha adoptado e implementado mecanismos de monitoreo y análisis que permitan identificar oportunamente anomalías o vulnerabilidades en la prestación de sus servicios de información.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI21: VAPRSG005: ¿La entidad ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de: a) su infraestructura, b) redes, c) sistemas de información, d) aplicaciones y/o		VSI0X = 1 (SÍ se evidencia)	Informes técnicos, reportes de monitoreo, hallazgos de no conformidades

e) uso de los servicios?		VSIOX = 0 (NO se evidencia)	
METAS			
CUMPLE	1	NO CUMPLE	0
OBSERVACIONES			
Se puede descomponer la variable en subcomponentes (VSI21a–e) si se desea medir de forma más granular cada ámbito, en este caso la fórmula sería ((VSI21a + VSI21b + VSI21c + VSI21d + VSI21e) / 5) * 100 La verificación debe realizarse mediante revisión de evidencias técnicas (reportes de escaneo de vulnerabilidades, alertas de monitoreo, sistemas SIEM, logs de eventos), entrevistas al equipo de TI, y validación de hallazgos registrados en auditorías o no conformidades. Se recomienda evaluación semestral o posterior a cambios significativos en infraestructura.			

INDICADOR 11 – IMPLEMENTACIÓN DE POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN			
IDENTIFICADOR	SGIN11		
DEFINICIÓN			
Mide el nivel de implementación de políticas, lineamientos y controles relacionados con la privacidad de los datos personales y la confidencialidad de la información procesada por la entidad.			
OBJETIVO			
Verificar si la entidad ha establecido e implementado mecanismos que garanticen la protección de la información personal de los ciudadanos y la confidencialidad de los datos que gestionan o transfieren otras entidades a través de sus servicios.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN	
VSI22: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios, en cumplimiento de la Ley 1581 de 2012 y demás normas aplicables?		Políticas institucionales, registros de cumplimiento, entrevistas	

VSI23: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información confidencial compartida por otras entidades?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Documentación técnica, acuerdos de confidencialidad, revisión de procesos

METAS			
CUMPLE	1	NO CUMPLE	0

OBSERVACIONES

La validación debe realizarse mediante revisión de políticas de privacidad y confidencialidad definidas en la entidad, verificación de medidas técnicas y administrativas de protección de datos personales, entrevistas con responsables de tratamiento de la información y análisis de cumplimiento con el régimen legal aplicable en Colombia. Se recomienda evaluación anual o posterior a cambios normativos.

INDICADOR 12 – IMPLEMENTACIÓN DE POLÍTICAS Y MECANISMOS PARA LA INTEGRIDAD DE LA INFORMACIÓN	
IDENTIFICADOR	SGIN12

DEFINICIÓN

Mide el nivel de implementación de políticas, lineamientos y controles orientados a garantizar la integridad de la información de la entidad, previniendo su alteración, pérdida o destrucción accidental o maliciosa.

OBJETIVO

Verificar si la entidad ha implementado mecanismos para prevenir, detectar y recuperar información ante eventos que comprometan su integridad, ya sean accidentales o intencionales.

TIPO INDICADOR

Indicador de Cumplimiento

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI24: ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Políticas institucionales, evidencias técnicas, entrevistas
VSI25: ¿La entidad ha definido mecanismos de recuperación ante eventos que afecten la integridad de la información, tanto intencionales como accidentales?		Planes de contingencia, pruebas de restauración, revisión de procesos

METAS			
CUMPLE	1	NO CUMPLE	0
OBSERVACIONES			
La verificación debe realizarse a través de revisión documental de políticas de integridad, planes de respaldo, registros de restauración de datos, entrevistas a responsables de TI y pruebas de los mecanismos de control y recuperación. La evaluación debe realizarse al menos una vez al año.			

INDICADOR 13 – IMPLEMENTACIÓN DE POLÍTICAS Y MECANISMOS PARA LA DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN			
IDENTIFICADOR	SGIN13		
DEFINICIÓN			
Mide el nivel de implementación de políticas, normas y mecanismos orientados a garantizar la disponibilidad continua de los servicios de la entidad y el acceso oportuno a la información, especialmente en el contexto de servicios digitales.			
OBJETIVO			
Verificar si la entidad cuenta con lineamientos y controles implementados para garantizar la continuidad operativa y la alta disponibilidad de sus servicios de información, incluyendo servicios digitales esenciales.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI26: ¿La entidad verifica el cumplimiento de lineamientos y estándares orientados a la continuidad del servicio y recuperación ante interrupciones?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Procedimientos, políticas de continuidad, evidencias de pruebas
VSI27: ¿La entidad ha implementado mecanismos para que los servicios de Gobierno Digital tengan altos índices de disponibilidad?			Reportes de disponibilidad, herramientas de monitoreo, sistemas de respaldo
METAS			
CUMPLE	1	NO CUMPLE	0
OBSERVACIONES			
La verificación debe incluir revisión de políticas de continuidad, registros de pruebas de recuperación, reportes de monitoreo de disponibilidad, y entrevistas con responsables de			

TI. La evaluación se recomienda de forma semestral o posterior a incidentes que afecten la operación.

INDICADOR 14 – PROPORCIÓN DE ATAQUES INFORMÁTICOS CON IMPACTO EN LA CONTINUIDAD DEL SERVICIO			
IDENTIFICADOR	SGIN14		
DEFINICIÓN			
Mide el porcentaje de ataques informáticos que, durante un periodo determinado, generaron interrupciones o afectaciones en la prestación de los servicios institucionales ofrecidos a ciudadanos o terceros.			
OBJETIVO			
Identificar el impacto real de los ataques informáticos en la operación de la entidad, evaluando la capacidad de los controles de seguridad para mitigar o contener amenazas que puedan comprometer la continuidad de los servicios.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI28: Número total de ataques informáticos recibidos por la entidad en el último año		(VSI29 / VSI28) * 100	Herramientas de monitoreo, reportes técnicos
VSI29: Número de ataques informáticos que causaron interrupción o afectación en la prestación de servicios			Herramientas de Monitoreo/Usuarios Internos.
METAS			
CUMPLE	1	NO CUMPLE	0
OBSERVACIONES			
La fórmula indica el porcentaje de ataques exitosos o con impacto, que es una métrica de desempeño operativo.			

INDICADOR 15 – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIOS EN LÍNEA DE LA ENTIDAD	
IDENTIFICADOR	SGIN15
DEFINICIÓN	

Mide el porcentaje de tiempo durante el cual los servicios en línea de la entidad estuvieron disponibles para los usuarios en un periodo determinado, en relación con el tiempo total esperado de funcionamiento.			
OBJETIVO			
Evaluar el desempeño operativo de los servicios en línea ofrecidos por la entidad, identificando su nivel de disponibilidad efectiva y permitiendo la mejora de la continuidad del servicio.			
TIPO INDICADOR			
Indicador de Desempeño			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI30: Tiempo total que el servicio en línea estuvo disponible durante el periodo evaluado		(VSI30/VSI31)*100	Logs del sistema, herramientas de monitoreo
VSI31: Tiempo total esperado de disponibilidad del servicio en ese mismo periodo			SLA, planificación técnica
METAS			
MÍNIMA 75-80%	**SATISFACTORIA** 80-90%	SOBRESALIENTE	100%
OBSERVACIONES			
Este indicador debe ser calculado con base en datos registrados por herramientas de monitoreo de infraestructura o reportes automáticos de uptime. Se recomienda una evaluación mensual o trimestral. Puede incluirse un umbral mínimo de disponibilidad definido por los SLA (acuerdos de nivel de servicio).			

INDICADOR 16 – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	
IDENTIFICADOR	SGIN16
DEFINICIÓN	
Mide el grado de avance en la implementación de los controles de seguridad establecidos en el plan de tratamiento de riesgos de la entidad, en el marco del Sistema de Gestión de Seguridad de la Información de la entidad.	
OBJETIVO	
Determinar el nivel de cumplimiento del plan de tratamiento de riesgos a través de la ejecución efectiva de los controles de seguridad definidos, permitiendo hacer seguimiento a la madurez de la gestión de riesgos de la entidad.	

TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI32: Número de controles implementados efectivamente, según evidencia técnica y documental		(VSI032/VSI33) *100		Plan de tratamiento de riesgos, informes de auditoría.	
VSI33: Número total de controles definidos para ser implementados en el periodo evaluado				Plan de Tratamiento de riesgos.	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80-90%	SOBRESALIENTE	100%
OBSERVACIONES					
La validación debe hacerse con base en el seguimiento al plan de tratamiento de riesgos, revisión de evidencia documental de implementación, informes técnicos o auditorías internas. La medición debe realizarse trimestral o semestralmente según el ciclo de implementación definido por la entidad.					

INDICADOR 17 – PROPORCIÓN DE INVERSIÓN EN SEGURIDAD DE LA INFORMACIÓN RESPECTO AL PRESUPUESTO GENERAL DE LA ENTIDAD		
IDENTIFICADOR	SGIN17	
DEFINICIÓN		
Mide la proporción del presupuesto institucional que es destinada específicamente a actividades, servicios, soluciones y proyectos relacionados con la seguridad de la información, en comparación con el presupuesto total ejecutado por la entidad durante un periodo determinado.		
OBJETIVO		
Evaluar el nivel de inversión financiera orientada a la protección de los activos de información, permitiendo analizar la prioridad institucional otorgada a la seguridad de la información frente a otras áreas.		
TIPO INDICADOR		
Indicador Financiero / Estratégico		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI34: Monto total invertido por la entidad en iniciativas de seguridad de la información (proyectos, servicios,	(VSI34 / VSI35) * 100	Plan de adquisiciones

personal, infraestructura, consultorías, etc.)					
VSI35: Total del presupuesto ejecutado por la entidad en el mismo periodo				Plan de adquisiciones	
METAS					
MÍNIMA	< 2%	SATISFACTORIA	2–4.9%	SOBRESALIENTE	≥ 5%
OBSERVACIONES					
La inversión debe incluir gastos directos en seguridad de la información (infraestructura, capacitación, auditorías, herramientas tecnológicas, personal especializado) y excluir los gastos generales de TI no relacionados directamente con seguridad. Se recomienda evaluar este indicador anualmente, alineado con el ciclo presupuestal.					

INDICADOR 18 - IMPLEMENTACIÓN DE MECANISMOS DE INTELIGENCIA DE AMENAZAS		
IDENTIFICADOR	SGIN18	
DEFINICIÓN		
Mide el grado de implementación de fuentes y mecanismos que permitan anticiparse a posibles amenazas mediante el análisis proactivo de datos internos y externos.		
OBJETIVO		
Evaluar la adopción de fuentes, procesos y herramientas que permitan anticiparse a posibles amenazas de seguridad mediante el análisis proactivo de información técnica y contextual.		
TIPO INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI36: Número de fuentes activas de inteligencia de amenazas utilizadas	(VSI032/VSI33) *100	Plan de ciber inteligencia, boletines de CERT, CSIRT, SIEM, informes del área de seguridad.
VSI37: Número total de fuentes planeadas		Plan de ciber inteligencia, boletines de CERT, CSIRT, SIEM,

				informes del área de seguridad.	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80- 90%	SOBRESALIENTE	100%
OBSERVACIONES					
Se deben considerar tanto amenazas técnicas como de ingeniería social. Evaluar semestralmente.					

INDICADOR 19 - PORCENTAJE DE SERVICIOS EN LA NUBE CON CONTROLES DE SEGURIDAD EVALUADOS Y DOCUMENTADOS					
IDENTIFICADOR SGIN19					
DEFINICIÓN					
Mide el porcentaje de servicios en la nube que han sido revisados formalmente en cuanto a cumplimiento de requisitos de seguridad de la información.					
OBJETIVO					
Verificar que los servicios en la nube utilizados por la entidad han sido formalmente evaluados en cuanto a riesgos de seguridad, cumplimiento normativo y controles asociados.					
TIPO DE INDICADOR					
Indicador de Cumplimiento					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI37 Servicios en la nube con evaluación de seguridad documentada		(VSI37 / VSI38) *100		Contratos con proveedores, informes técnicos de seguridad, matrices de riesgo, auditorías internas.	
VSI38 Total de servicios en la nube utilizados					
MINIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Considerar servicios SaaS, PaaS o IaaS. Verifica si los controles incluyen cifrado, acceso seguro, respaldo, trazabilidad, etc. Se recomienda actualización anual.					

<table>
<tr><td colspan="6">INDICADOR 20 – PORCENTAJE DE CANALES CRÍTICOS CON CONTROLES ACTIVOS DE PREVENCIÓN DE FUGA DE DATOS</td></tr>
<tr><td>IDENTIFICADOR</td><td colspan="5">SGIN20</td></tr>
<tr><td colspan="6">DEFINICIÓN</td></tr>
<tr><td colspan="6">Mide el nivel de protección aplicado a los canales de comunicación críticos mediante controles de prevención de fuga de datos (DLP).</td></tr>
<tr><td colspan="6">OBJETIVO</td></tr>
<tr><td colspan="6">Medir la cobertura de las soluciones y medidas de prevención de pérdida de datos (DLP) implementadas en los canales utilizados para la transmisión, almacenamiento o compartición de información crítica.</td></tr>
<tr><td colspan="6">TIPO INDICADOR</td></tr>
<tr><td colspan="6">Indicador de Gestión</td></tr>
<tr><td colspan="2">DESCRIPCIÓN DE VARIABLES</td><td>FORMULA</td><td colspan="3">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VSI39: Número de canales críticos protegidos por controles DLP</td><td rowspan="2">(VSI039/VSI40) *100</td><td colspan="3">Informes técnicos de herramientas DLP, matrices de canales críticos, configuraciones de seguridad, políticas de uso.</td></tr>
<tr><td colspan="2">VSI40: Total de canales identificados como críticos</td><td colspan="3">Informes técnicos de herramientas DLP, matrices de canales críticos, configuraciones de seguridad, políticas de uso.</td></tr>
<tr><td colspan="6">METAS</td></tr>
<tr><td>MÍNIMA</td><td>75-80%</td><td>SATISFACTORIA</td><td>80-90%</td><td>SOBRESALIENTE</td><td>100%</td></tr>
<tr><td colspan="6">OBSERVACIONES</td></tr>
<tr><td colspan="6">Los canales incluyen correo, almacenamiento externo, nube, impresoras, etc. La revisión debe hacerse al menos cada seis meses o tras un incidente relevante.</td></tr>
</table>

TIC

Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de contenido

Tabla de contenido 95
Listado de Tablas 95
Gestión inventario clasificación de activos e infraestructura critica Cibernética 96
1. Identificación y tipificación de los activos de información 97
2. Clasificación de Activos de Información 100
2.1. Clasificación de acuerdo con la confidencialidad 101
2.2. Clasificación de acuerdo con la Integridad 104
3. Identificación de Infraestructura critica Cibernética Nacional 105
4. Revisión y aprobación de los activos de información 106
5. Publicación de los activos de información 107
6. Etiquetado de los Activos de Información 107
7. Otros lineamientos relacionados 108

Listado de Tablas

Tabla 1: Tipificación de Activos 100
Tabla 2: Criterios de Clasificación 101
Tabla 3: Niveles de Clasificación de acuerdo con la confidencialidad 101
Tabla 4: Esquema de clasificación por confidencialidad 102
Tabla 5: Esquema de clasificación por Integridad 104
Tabla 6: Esquema de clasificación por Disponibilidad 105

Gestión inventario clasificación de activos e infraestructura critica Cibernética

El presente documento detalla los lineamientos básicos que se deben tener en cuenta para realizar una adecuada identificación, gestión y clasificación de activos de información e infraestructura critica cibernética de cada entidad.

- Establecer las responsabilidades de los funcionarios y contratistas de la entidad con los activos de información.
- Garantizar que los activos de información de la entidad reciban un adecuado nivel de protección de acuerdo con su valoración.
- Proporcionar una herramienta que visualice de manera fácil los activos de información de la entidad.
- Sensibilizar y promover la importancia de los activos de información de la entidad.
- Proveer las pautas requeridas y necesarias para la adecuada identificación, clasificación y valoración de los activos de información de la entidad.
- Cumplir con la organización y publicación de los activos de información, respetando tanto las normas como los procedimientos que se deben cumplir.

El inventario y clasificación de activos hace parte de las actividades más relevantes e importantes del Modelo de Seguridad y Privacidad de la Información y está compuesta por las fases:

- **Identificación y Tipificación de los Activos de Información**: Corresponde a la etapa en donde la dependencia como propietario y custodio de la información, identifica y clasifica la información producida, de acuerdo con: Activos de información puros, de Tecnologías de la Información, de Talento humano y Servicios.
- **Clasificación de los activos de Información**: Corresponde a la etapa en donde la dependencia como propietario y custodio de la información califica los activos de información teniendo en cuenta los criterios de confidencialidad, integridad y disponibilidad, conforme a los principios de seguridad de la información. Adicionalmente, los debe alinear con la Ley 1712 de 2014 sobre acceso a la información pública y la Ley 1581 de 2012 sobre protección de datos personales, garantizando un tratamiento diferencial según el tipo de activo clasificado.
- **Revisión y Aprobación**: Corresponde a la etapa en donde se valida la clasificación y valoración dada a los activos de información, para la presentación y aprobación por parte del dueño o responsable de los activos.

- **Publicación de los Activos de Información**: Corresponde a la etapa de publicación de la información en la página web de la entidad, Link de transparencia y acceso a la Información Pública, Portal de Datos Abiertos del estado colombiano o el sitio que lo modifique o sustituya.

1. Identificación y tipificación de los activos de información

De acuerdo con las directrices del Archivo General de la Nación, que implementan la metodología apropiada sobre el tratamiento de los "tipos de información y documentos físicos y electrónicos, así como los sistemas, medios y controles asociados a la gestión", la identificación y tipificación de los activos de información se deben articular de igual forma.

Los propietarios y custodios de la información producida en el área deben identificar, clasificar y valorar los activos de información de acuerdo con la siguiente compilación de Activos de Información teniendo en cuenta lo establecido en la norma técnica ISO/IEC 27001:2022 (Información; Software como programa informático; Hardware como computadora; servicios; personas, y sus calificaciones, habilidades y experiencia; intangibles como reputación e imagen).

De igual forma, se deben tomar como fuente de información, las Tablas de Retención Documental actualizadas de la entidad, que contemplan las series, subseries y tipos documentales de la información producida, su medio de conservación y preservación. Las fuentes de información de valor que no están contemplados en las TDR, deben ser complementadas e identificadas por los Gestores, con los jefes de las áreas, Oficina TI (sistemas de información y tecnologías) y servidores (funcionarios y/o contratistas).

Información básica: hace referencia a aquellas características mínimas del activo que deben identificarse durante esta fase:

- **Macroproceso**: Macroproceso de la Entidad al que pertenece el activo de información (En caso de que existan).
- **Proceso**: Proceso de la Entidad al que pertenece el activo de información.
- **Identificador**: Se sugiere que el identificador sea una concatenación del código de la dependencia según la Tabla de Retención Documental (TRD) + número consecutivo.
- **Tipo**: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

TIPIFICACIÓN DEL ACTIVO	DESCRIPCIÓN	COMPONENTES
Información	Corresponden a este tipo datos e información almacenada o procesada electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema,	

TIPIFICACIÓN DEL ACTIVO	DESCRIPCIÓN	COMPONENTES
	investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.	
Hardware	Se consideran los medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la entidad.	Servidores, routers, módems Computadores (portátiles, escritorio), impresoras, Celulares Tablet, Teléfonos IP
Software	Se refiere a los programas, aplicativos, sistemas de información que soportan las actividades de la entidad y la prestación de los servicios.	Software de aplicación, correo electrónico, sistema operativo, etc.
Servicios	Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.	
Recurso Humano	Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información	Contratistas, funcionarios, proveedores.
Instalaciones	Los lugares donde se almacenan o resguardan los sistemas de información y comunicaciones.	Centros de cómputo, centros de cableado, Datacenter.
Infraestructura crítica cibernética nacional	se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el	

TIPIFICACIÓN DEL ACTIVO	DESCRIPCIÓN	COMPONENTES
	eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.	

Tabla 1: Tipificación de Activos

- **Serie documental**: Serie documental del área, dependencia o proceso que se encuentra identificando el Activo.

- **Subserie documental**: Subserie documental del área, dependencia o proceso que se encuentra identificando el Activo.

- **Nombre**: Nombre completo del activo de información.

- **Descripción**: Descripción resumida de manera clara para identificar el activo de información.

- **Nombre del responsable de la producción de la información (Propietario del activo)**: Nombre del área, dependencia, proceso responsable de producir el activo de información

- **Fecha de generación de la información**: Fecha en la que el activo de información fue incluido en el inventario de activos de información.

- **Custodio del activo de la información**: Corresponde al nombre del área, proceso o dependencia encargada en la Entidad de la custodia o control de la información o implementación de controles de protección.

- **Fecha de ingreso del activo al archivo**: Fecha en la que el activo ingresa al archivo de gestión. (Aplica para los activos tipo información)

- **Soporte de registro**: De acuerdo con el Decreto 2609 de 2012:

    - **Físico** (análogo): ; Este campo se diligencia si el Tipo de activo es "Información"
    - **Digital** o Electrónico; Este campo se diligencia si el Tipo de activo es "Información"
    - **N/A:** Para el resto de los tipos de activos se debe seleccionar N/A.

- **Medio de conservación**: De acuerdo con el Decreto 2609 de 2012 Archivo Institucional Es la instancia administrativa de custodiar, organizar y proteger.

- **Formato**: Identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: Hoja de cálculo, imagen, audio, video, documento de texto, etc.

- **Idioma**: Establece el idioma, lengua o dialecto en que se encuentra la información.

Es importante partir de la identificación de la información de la entidad como activo primario y determinar los activos secundarios que participan en el tratamiento de esta información,

por ejemplo: La información de los beneficiarios de un programa de la entidad, se almacena en una base de datos, esta base de datos se encuentra en un servidor que esta alojada en un centro de datos y es accedida por los ciudadanos a través de una aplicación web. Para este caso se deben identificar como activos: la información, el sistema gestor de base de datos, el servidor, el datacenter, la aplicación y las redes por donde fluye la información, ya que los controles de seguridad para cada activo de información son diferentes y en cualquiera de estos activos podría generarse perdida de confidencialidad, integridad o disponibilidad.

Las entidades deberán identificar dentro de su inventario de activos las aplicaciones de terceros que traten información de la entidad o bajo su custodia y asegurar el cumplimiento de las políticas de seguridad de la información para estas aplicaciones.

Las razones por las cuales debería realizarse una actualización del inventario de activos son:

- Actualizaciones al proceso al que pertenece el activo.
- Adición de actividades al proceso.
- Inclusión de nuevos registros de calidad, nuevos registros de referencia o procesos y procedimientos.
- Inclusión de un nuevo activo.
- Desaparición de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio (Cambios Organizacionales).
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

2. Clasificación de Activos de Información

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, de acuerdo con sus características particulares.

El sistema de clasificación definido se basa en la Confidencialidad, la Integridad y la Disponibilidad de cada activo. Asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades.

Para cada propiedad se establecieron criterios específicos y lineamientos para el tratamiento adecuado del activo. Así mismo se definieron tres (3) niveles que permiten determinar el valor general o criticidad del activo en la entidad (es importante aclarar que los niveles pueden ser definidos a criterio de la entidad): Alta, Media y Baja, con el fin identificar qué activos deben ser tratados de manera prioritaria (ver Tabla: Niveles de evaluación).

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 2: Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 3: Niveles de Clasificación de acuerdo con la confidencialidad

2.1. Clasificación de acuerdo con la confidencialidad

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, Esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad. Como ejemplo se definieron los siguientes niveles, los 3 primeros alineados con los tipos de información declarados en la Ley 1712 del 2014:

INFORMACION PUBLICA RESERVADA	Es la información que no debe ser divulgada debido a que esto puede causar daño a intereses públicos. Solamente la Constitución o la ley pueden definir qué información es de carácter reservado.

INFORMACION PÚBLICA CLASIFICADA	Es la información que no debe ser divulgada debido a que se pueden vulnerar los derechos de las personas naturales o jurídicas, tales como: derecho de las personas a la intimidad, derecho a la vida, salud o seguridad y los secretos comerciales, industriales y profesionales.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA. como: Hardware, Colaboradores de Planta o Contratistas

Tabla 4: Esquema de clasificación por confidencialidad

2.1.1 Clasificación Ley de protección de datos personales

La información clasificada incluye los datos personales, los cuales se dividen en las siguientes categorías:

Según la Ley 1581 de 2012

2.1.1.1 **Información Semiprivada** El dato personal semiprivado es aquel que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general. Puede accederse a ellos por orden de autoridad judicial o administrativa y para los fines propios de sus funciones, o a través del cumplimiento de los principios de administración de datos personales. Ejemplos de ello son el comportamiento financiero y crediticio de actividad comercial o de servicios [6] y los datos sobre la seguridad social distintos a aquellos que tienen que ver con las condiciones médicas de los usuarios.[7]

La información semiprivada tiene tres características relevantes para el presente caso: Su divulgación debe estar conforme con el principio de finalidad que rige el derecho fundamental al hábeas data. Los particulares que no son titulares de tal información solo pueden acceder a ella a través de una orden judicial o administrativa de la autoridad competente en el ejercicio de sus funciones. No se rige por las reglas del artículo 74 Superior sobre la reserva de información pública.

2.1.1.2. **Información Privada** La información privada es aquella que por versar sobre información personal o no, y que, por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones.

[6] Ley 1266 de 2008, Art. 3°, Lit. “g)”.

[7] Corte Constitucional, Sentencia C-1011 de 2008 (revisión de constitucionalidad de la Ley Estatutaria 1266 de 2008), punto “2.5

2.1.1.3 **Información Sensible** La información sensible es aquel dato personal que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos5

Respecto al tratamiento de datos sensibles, este se prohíbe, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;

b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; [8]

e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

Según la Ley 1712 de 2024

2.1.2 **Información pública clasificada**. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley;

Se sugiere que estos campos estén descritos en la matriz de inventario y clasificación de activos de Información como lo relacionado con la finalidad de la recolección de estos datos y la existencia de la autorización expresa para su tratamiento.

Nota: Para los activos de información que contengan información pública clasificada, pública reservada y datos personales se debe identificar qué criterios del índice de información clasificada y reservada (Decreto 103 de 2015 compilado en el Decreto 1080 de 2015) y de la ley de protección datos personales (Ley 1581 de 2012) les aplica además de hacer el

[8] Ley 1581 de 2012 Articulo 6

correspondiente reporte de dichas bases de datos ante la Superintendencia de industria y comercio a través del Registro Nacional de Bases de Datos (Decreto Único 1074 de 2015)

2.2. Clasificación de acuerdo con la Integridad

La integridad se refiere a la exactitud y completitud de la información (ISO 27000:2022) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. En este documento se recomienda el siguiente esquema de clasificación:

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Tabla 5: Esquema de clasificación por Integridad

2.3. Clasificación de acuerdo con la Disponibilidad

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

Se recomienda el siguiente esquema de clasificación:

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Tabla 6: Esquema de clasificación por Disponibilidad

3. Identificación de Infraestructura critica Cibernética Nacional

Una vez se ejecute la identificación de los activos, la entidad pública debe definir si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto, esto debe estar debidamente documentando y aprobado por la Línea Estratégica – Alta dirección.

Identificar si existen Infraestructuras Críticas Cibernéticas Nacionales -ICCN-

Se invita a que las entidades públicas a que identifiquen y reporten a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICCN. Un activo es considerado infraestructura crítica si su impacto o afectación podría cumplir con alguno de los criterios establecidos por el Colcert en su metodología para la identificación de infraestructuras criticas cibernéticas nacionales.

Si la entidad pública determina que tiene ICC, es importante que se identifiquen los componentes que conforman dicha infraestructura. Por ejemplo, dicha ICC puede tener componentes de TI (como servidores) o de TO (como sistemas de control industrial o sensores).

Las entidades deberán consultar y aplicar los criterios y la metodología de identificación de infraestructura critica cibernética que esté vigente, cada vez que realicen el inventario de activos de información o una actualización a este.

Los criterios y la metodología de identificación de infraestructura critica cibernética serán actualizados por el ColCERT.

4. Revisión y aprobación de los activos de información

Posterior a la identificación, clasificación y valoración de los activos de información compilados en la Matriz de Activos de Información por los lideres de los procesos o sus delegados y que esta haya sido validada y aprobada por los jefes de cada dependencia, se debe enviar la matriz para su consolidación y validación por parte de la Oficina Asesora Jurídica o al área correspondiente para finalmente ser presentada ante el Comité Institucional de Gestión y Desempeño de ser necesario y proceder con la publicación correspondiente.

En general, el inventario de activos puede ser revisado o validado en cualquier momento en que el líder del proceso (o quien haga sus veces) así lo solicite, o si el equipo de gestión de activos lo solicita o algún líder de proceso o el oficial de seguridad de la información si así lo requiere.

La aprobación por parte del Comité Institucional de Gestión y Desempeño de los activos de información de la entidad se encuentra establecida en el Decreto 1083 de 2015, modificado por el Decreto 1499 de 2017 siendo este el encargado de “orientar la implementación y operación del Modelo Integrado de Planeación y Gestión - MIPG” según el **ARTÍCULO 2.2.22.3.8**. Comités Institucionales de Gestión y Desempeño del mencionado Decreto.

Nota: De conformidad con la implementación del presente lineamiento es importante tener en cuenta que, una vez se publique la metodología para la identificación de infraestructuras criticas cibernéticas establecida en el Decreto 1078 de 2015, adicionado por el Decreto 338 de 2022, se actualizarán los lineamientos generados en el presente documento para realizar la identificación de activos vinculados a las infraestructuras criticas cibernéticas, la cual será de obligatorio cumplimiento para entidades del sector público.

5. Publicación de los activos de información

El área, proceso, grupo interno, funcionario o rol responsable de la custodia del inventario de activos de información debe enviar a la Oficina Asesora de Prensa o quien haga sus veces en la entidad, el consolidado del inventario de Activos de Información para la respectiva publicación de la información en la página web de la entidad, Link de transparencia y acceso a la Información Pública, Portal de Datos Abiertos del estado colombiano o el sitio que lo modifique o sustituya: Intranet institucional (si cuentan con esta) y deberá ser divulgado con todos los colaboradores de la entidad, teniendo en cuenta si se debe anonimizar o restringir el acceso algunos datos de acuerdo con su clasificación según lo establecido en la Ley 1581 de 2012

6. Etiquetado de los Activos de Información

Para realizar el etiquetado de los Activos de Información se proponen los siguientes lineamientos:

- Se deben etiquetar todos los Activos de Información que estén clasificados según el esquema clasificación de Confidencialidad de la entidad.

- Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado como si tuviera la clasificación de confidencialidad más alta establecido por la entidad.

- Para los activos clasificados en confidencialidad como INFORMACION PUBLICA RESERVADA se podría utilizar la etiqueta IPR, INFORMACION PUBLICA CLASIFICADA IPC e INFORMACION PUBLICA, IPB.

- Para los activos clasificados en integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA, B.

- Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta A, MEDIA M, y BAJA B.

De esta manera se realizarían las combinaciones de acuerdo con los criterios de clasificación de la información.

7. Otros lineamientos relacionados

A continuación, se sugieren lineamientos a tener en cuenta:

- La entidad debe establecer directrices para identificar, clasificar y proteger los activos de información que son almacenados, procesados o transmitidos mediante servicios en la nube.

- Los activos gestionados en la nube deben ser gestionados bajo los mismos principios de seguridad de los activos locales, incorporando además consideraciones específicas de soberanía, cifrado, control de accesos y cumplimiento contractual con proveedores de nube.

- Se deberán documentar los servicios utilizados (SaaS, PaaS, IaaS), sus responsables, niveles de disponibilidad esperados, mecanismos de respaldo, y condiciones para su monitoreo continuo.

- La entidad debe definir e implementar procedimientos para la eliminación segura de información contenida en activos físicos y digitales, asegurando que los datos no puedan ser recuperados una vez descartados.

Estos procedimientos deben considerar el tipo de activo (papel, disco duro, dispositivos USB, nube), su nivel de clasificación, y el medio de eliminación (desmagnetización, destrucción física, borrado certificado, etc.). La eliminación debe estar documentada y respaldada por registros auditables.

- La entidad debe establecer mecanismos automatizados para la clasificación y etiquetado de la información, especialmente en entornos digitales, de acuerdo con su nivel de sensibilidad y criticidad.

- La entidad debe identificar, clasificar y controlar los activos digitales no estructurados, tales como archivos ofimáticos, correos electrónicos, presentaciones, grabaciones y otros documentos generados en la operación diaria que no están formalizados en un sistema de gestión documental. Estos activos deben estar incorporados en el inventario de activos y estar sujetos a revisión periódica.

TIC

Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de Contenido

Tabla de Contenido 111

Listado de Tablas 112

Tabla de Ilustraciones 112

Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas 113

1. Generalidades 113

1.1. Derechos de autor 113

1.2. Objetivos 113

1.2.1. Objetivo general 113

1.2.2. Objetivos especificos 114

1.3. Alcence del documento 114

2. Integración del modelo de seguridad y privacidad de la Información (MSPI) 115

3. Gestión De riesgos De Seguirdad De La Información Para Entidades Publicas 116

3.1. Fase 1. Planificación de la GRSD 116

3.1.1. Contexto interno y externo de la entidad pública 117

3.1.2. Alcance para aplicar la gestión de riesgos de seguridad de la información 119

3.1.3. Alineación o creación de la política de gestión de riesgo de seguridad de la información 120

3.1.4. Definición de roles y responsabilidades 120

3.1.5. Responsable de seguridad de la información 120

3.1.6. Definición de recursos para la Gestión de riesgos de seguridad de la información 121

3.1.7. Identificación de activos de información 122

3.1.8. Identificar los riesgos inherentes de seguridad de la información 128

3.1.9. Identificación del nivel de confianza para la autenticación digital 140

3.1.10. Valoración del riesgo 142

3.1.11. Identificación y evaluación de los controles existentes 142

3.1.12. Tratamiento de los riesgos de seguridad de la información 142

3.1.13. Planes de Tratamiento de Riesgos de Seguridad de la información e Indicadores para la Gestión del Riesgo 143

3.2. Fase 2. Ejecución 143

3.3. Fase 3. Monitoreo y revisión 144

3.3.1. Reporte de la gestión del riesgo de seguridad de la información al interior de la entidad pública.....145
3.3.2. Reporte de la gestión del riesgo de seguridad de la información a autoridades o entidades especiales.....146
3.3.3. Auditorías internas y externas.....147
3.3.4. Medición del desempeño.....147
3.4. Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad de la información 148
4. Controles de De Referencia Para La Mitigación De Los Riesgos De Seguirdad 149

Listado de Tablas

Tabla 1 Factores del entorno digital..... 119
Tabla 2 Tabla de amenazas.....130
Tabla 3 Tabla de amenazas dirigida por el hombre 132
Tabla 4 Tabla de Vulnerabilidades Comunes.....134
Tabla 5 Tabla de Amenazas y Vulnerabilidades.....139

Tabla de Ilustraciones

Ilustración 1 Interacción MSPI - Modelo Gestión de Riesgo de seguridad de la información 116
Ilustración 2 Reportes de información por parte de la entidad.....146

Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

1. Generalidades

1.1. Derechos de autor

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información -MSPI, son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC.

De igual forma, son derechos reservados por parte del MinTIC, todas las referencias a las políticas, definiciones o contenido relacionados con los documentos del MSPI publicadas en el compendio de las normas técnicas colombianas vigentes.

Las reproducciones, referencias o enunciaciones de estos documentos deberán ir siempre acompañadas por el nombre o seudónimo del titular de los derechos de autor (Ministerio de Tecnologías de la Información y las Comunicaciones).

Lo anterior, sin perjuicio de los derechos reservados por parte de entidades tales como la International Standard Organización (ISO), ICONTEC, entre otras, respecto de referencias, definiciones, documentos o contenido relacionado en el MGRSD y sus documentos o anexos que son de su autoría o propiedad.

1.2. Objetivos

1.2.1. Objetivo general

El objetivo principal de este documento es orientar a todas las entidades públicas del orden nacional y del sector público en general, en la implementación de la Gestión de Riesgos de Seguridad de la información, que permita incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en las entidades.

1.2.2. Objetivos especificos

a. Otorgar una herramienta de orientación para la ejecución de la Gestión de Riesgos de Seguridad de la información, en las entidades de Gobierno nacional, territorial y del sector público en general.

b. Estandarizar el proceso de Gestión de Riesgos de Seguridad de la información, en las entidades del Gobierno nacional, territorial y del sector público en general.

c. Generar mecanismos para que las entidades del Gobierno nacional, territorial y del sector público en general puedan establecer los elementos para identificar, analizar, valorar y tratar los riesgos, amenazas y vulnerabilidades del entorno digital.

d. Proponer estrategias para la ejecución de planes de acción para mitigar los riesgos generados en el entorno digital.

1.3. Alcance del documento

Este documento tiene como objetivo ampliar y profundizar en los contenidos presentados en la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas" del Departamento Administrativo de la Función Pública. En particular, se enfoca en las secciones relacionadas con el análisis del contexto, con un énfasis especial en el entorno digital.

Además, aborda temas como la identificación de activos, la elaboración de catálogos de amenazas y vulnerabilidades para llevar a cabo un análisis exhaustivo de los riesgos de seguridad de la información, la implementación de controles diseñados para mitigar estos riesgos y el proceso de reporte de estos. También se abordan otros aspectos adicionales que desempeñan un papel fundamental en la gestión efectiva del riesgo de seguridad de la información en el ámbito de las entidades públicas.

Este material ha sido desarrollado en colaboración entre el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República9 con el propósito de proporcionar una orientación detallada y práctica sobre estos aspectos clave.

[9] Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Departamento Administrativo de la función pública, Dirección de Gestión y Desempeño Institucional Noviembre 2022

2. Integración del modelo de seguridad y privacidad de la Información (MSPI)

Conforme al ámbito de aplicación del Decreto 1078 de 2015, en lo relacionado con la Estrategia de Gobierno Digital, y a la Resolución 500 del 10 de marzo de 2021, mediante la cual el MinTIC establece los lineamientos y estándares para la estrategia de seguridad digital y adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de dicha política, las entidades públicas deben implementar el MSPI con el fin de establecer un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de su organización.

El MSPI incorpora, en cada una de sus fases, actividades orientadas a la gestión de riesgos de seguridad de la información, ya que esta constituye su eje central. Para ello, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, junto con este Anexo, proporcionan las directrices necesarias para cumplir con los requerimientos de gestión del riesgo establecidos en el modelo.

En esencia, la interacción entre el modelo de seguridad y privacidad de la información y el modelo nacional de gestión de riesgos de seguridad de la información puede resumirse de la siguiente manera:

1. Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.

2. Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del MSPI.

3. Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de EVALUACIÓN DEL DESEMPEÑO del MSPI.

4. Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del desempeño para identificar aspectos a mejorar en la aplicación de ambos modelos.

A continuación, se ilustra en que acciones del MSPI tendrán interacción directa con el Modelo de Gestión de Riesgos de Seguridad de la información.

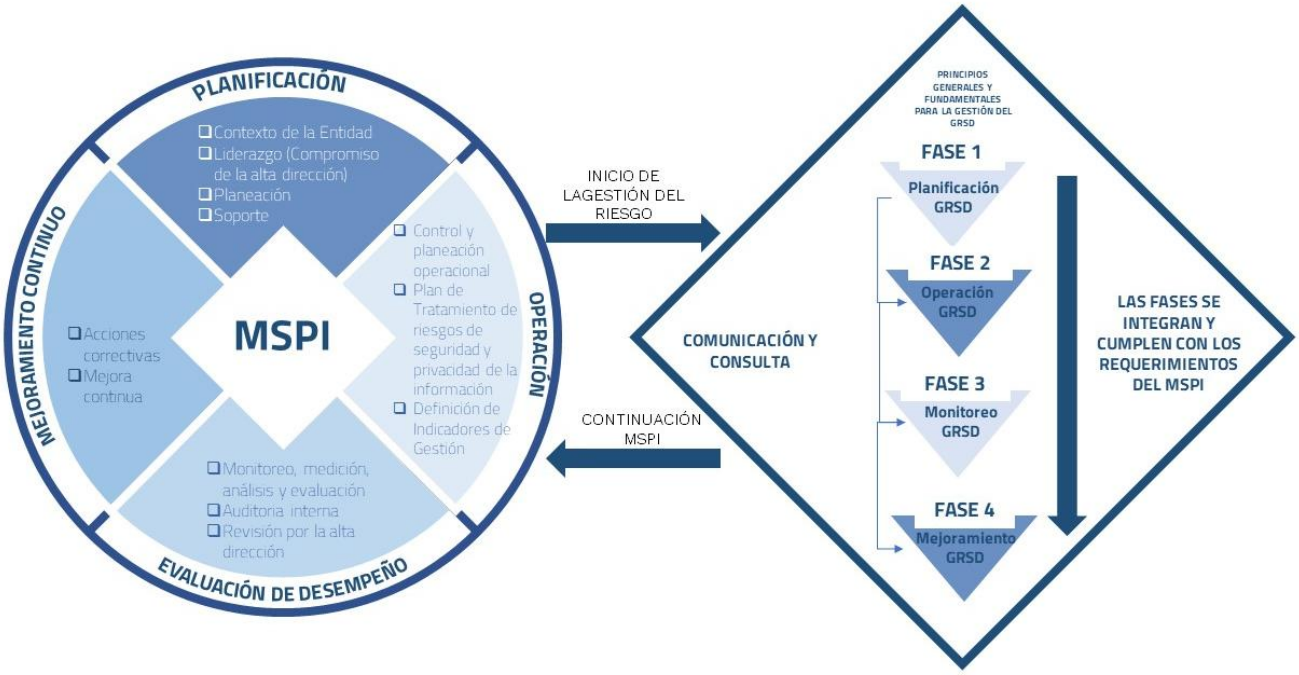


Ilustración 1 Interacción MSPI - Modelo Gestión de Riesgo de seguridad de la información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

3. Gestión De riesgos De Seguridad De La Información Para Entidades Publicas

En los siguientes numerales se indican los aspectos complementarios a lo expuesto en el documento "Guía para la administración del riesgo y el diseño de controles en entidades públicas" [10], donde se incluyen los riesgos de seguridad de la información.

3.1. Fase 1. Planificación de la GRSD

La fase de planificación comprende todo lo expuesto en los Pasos 1, 2 y 3 de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas", emitida por el Departamento Administrativo de la Función Pública, es decir, comprende todo lo relacionado con las siguientes actividades:

[10]La guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas, la encuentra en el portal del Departamento Administrativo de la Función Pública - DAFP.

- Definición del contexto interno, externo y de los procesos de la entidad pública.
- Definición de la política de administración de riesgo.
- Designación de roles y responsabilidades.}
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos de información.
- Identificación de riesgos.
- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

Respecto a estas actividades, el presente documento busca profundizar en lo concerniente a riesgos de seguridad de la información, en cada una de ellas, siendo el documento del Departamento Administrativo de la Función Pública -DAFP-, el documento metodológico principal.

3.1.1. Contexto interno y externo de la entidad pública

Conforme lo indica el DAFP, las entidades públicas deben realizar la identificación del contexto interno y externo de la entidad, sin embargo, es necesario profundizar en este análisis relacionado con seguridad de la información, por lo tanto, a continuación, se dan unas directrices adicionales para realizar la actividad adecuadamente.

Las entidades deben revisar los ecosistemas digitales desde la óptica de los daños colaterales que pueden presentarse dentro de la organización, y que pueden impactar en la afectación del principio de disponibilidad, sin que necesariamente el evento inicial sea considerado como de orden digital.

Establecimiento del contexto externo: Para determinar el contexto externo, la entidad pública debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

CONTEXTO EXTERNO

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.
- Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la Ley 1581 de 2012 o la Ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el Decreto 1078 de 2015 o el Decreto número 1083 de 2015, modificado por el Decreto 1499 de 2017.
- Dependencias económicas y financieras por parte de otras empresas.
- Entorno cultural.
- Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local.
- Cantidad de ciudadanos a los cuales la entidad pública brinda u ofrece servicios a través del entorno digital como trámites a través de páginas web.
- Aspectos externos que pueden verse afectados con los riesgos de seguridad

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

Establecimiento del contexto interno: Para esto se considera factores que impactan directamente a:

- La entidad pública, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.

- Cada uno de los procesos sobre los cuales están soportadas sus operaciones.

Para determinar los factores de la entidad pública y los procesos se debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

PARA LA ENTIDAD PÚBLICA	PARA LOS PROCESOS
• Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros • Flujos de información y los procesos de toma de decisiones • Empleados, contratistas • Objetivos estratégicos y la forma de alcanzarlos • La misión, visión, valores y cultura de la organización • Sus políticas, procesos y procedimientos • Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros) • Toda la estructura organizacional • Roles y responsabilidades • Sistemas de información o servicios. • Infraestructuras físicas, servicios y sistemas de información de apoyo y servicios logísticos transversales.	• Identificación de los procesos y su respectiva caracterización • Detalle de las actividades que se llevan a cabo en el proceso • Flujos de información • Identificación y actualización de los activos en la cadena de valor de la entidad pública • Recursos • Alcance del proceso • Relaciones con otros procesos de la entidad pública • Cantidad de ciudadanos afectados por el proceso • Procesos de gestión de riesgos que se tienen actualmente implementados • Personal involucrado en la toma de decisiones

Tabla 1 Factores del entorno digital

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

Para llevar a cabo esta actividad se sugiere hacer una lista en la que estén enumeradas las partes interesadas externas e internas que tengan relación con la entidad pública y con sus objetivos, misión o visión.

3.1.2. Alcance para aplicar la gestión de riesgos de seguridad de la información

El alcance de la administración del riesgo de seguridad de la información debe ser extensible y aplicable a los procesos de la entidad pública, así como a los grupos de valor que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información[11], habilitador de la Estrategia de Gobierno Digital expedida por el MINTIC.

[11] http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

3.1.3.Alineación o creación de la política de gestión de riesgo de seguridad de la información

Es necesario que la entidad pública establezca una política de gestión de riesgo integral, donde se incluya el compromiso en la gestión de los riesgos de seguridad de la información en todos sus niveles. Esta debe crearse como lo indica la guía para la Administración del Riesgo y el diseño de controles en entidades públicas del DAFP en el Paso 1, incluyendo la gestión de riesgos de seguridad de la información. Esta actividad es responsabilidad de la Línea estratégica dispuesta por el MIPG.

3.1.4. Definición de roles y responsabilidades

Además de las líneas de defensa y las responsabilidades designadas en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas" del DAFP, es necesario indicar o profundizar en las responsabilidades que deberá tener designadas el responsable de Seguridad digital:

3.1.5. Responsable de seguridad de la información

Cada entidad pública debe designar una persona o grupo responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica, como lo establece el Manual Operativo del MIPG en el numeral 3.2.1.4 Política de Seguridad de la información, se recomienda que este responsable pertenezca a un área diferente a la de tecnología con el fin de evitar conflicto de intereses. Las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad de la información serán las siguientes:

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

- Actualizar el procedimiento para la Identificación y Valoración de Activos de la Entidad, de acuerdo a los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad).
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Nota: Como complemento de esta actividad, la entidad pública debe tomar como referencia lo definido en el documento de Lineamientos de Roles y responsabilidades del MSPI de la Estrategia de Gobierno Digital del MINTIC, en complemento a lo anterior.

3.1.6. Definición de recursos para la Gestión de riesgos de seguridad de la información

La entidad pública debe disponer los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad de la información, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad de la información.

La línea estratégica o alta dirección debe asignar entre otros, recursos tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad de la información.

- Recursos económicos para la implementación de controles para la mitigación de riesgos (con base al análisis de riesgo realizado, teniendo en cuenta el alcance de la política de riesgos de la entidad en cuanto a seguridad de la información), que permita ser incluido dentro de la gestión presupuestal y eficiencia del gasto público de la entidad.

- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

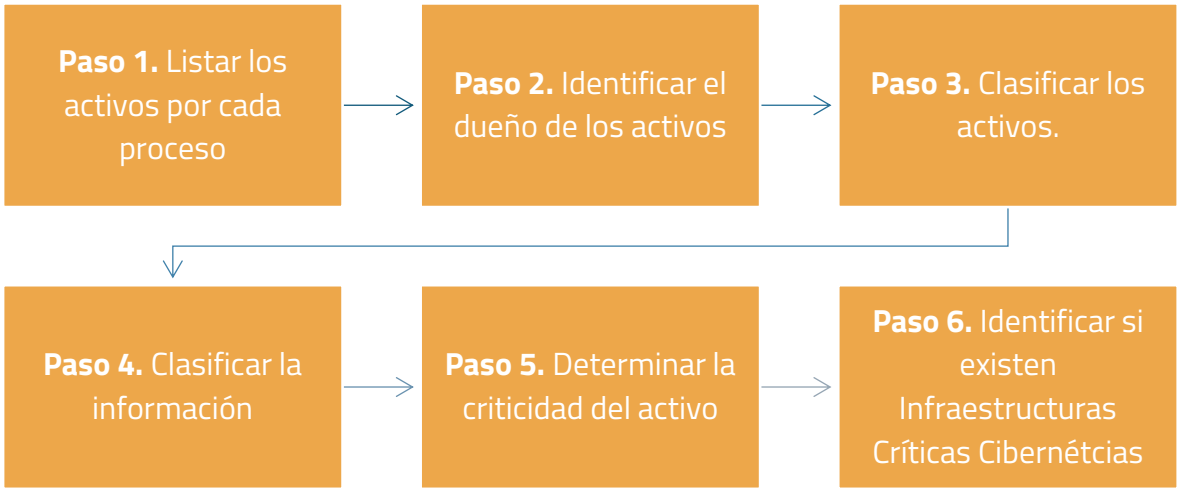
3.1.7. Identificación de activos de información

Un activo de información es cualquier elemento que participe en el tratamiento de información que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la entidad pública, servicios Web, redes, información digital, personal, ubicación, organización, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento y que por afectación operativa, se afecte el principio de disponibilidad.

Es necesario que la entidad pública identifique los activos de información y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (Front Office), aumentando así su confianza en el uso del entorno digital para interactuar con las partes interesadas.

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa - Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.

Para la generación de este inventario, la entidad pública debe tener en cuenta los siguientes pasos:



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

A continuación, se especifica lo que deberá tenerse en cuenta para la realización de cada uno de los pasos mencionados para la identificación y valoración de activos.

Paso 1. Listar los activos por cada proceso:

En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

Ejemplo:

PROCESO	ACTIVO	DESCRIPCION
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad
Gestión Financiera	Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Las entidades públicas pueden adicionar identificadores o nemónicos para complementar la identificación de los activos.

Paso 2. Identificar el dueño de los activos:

Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

Ejemplo:

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO
Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe Oficina de Nómina
Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos	Jefe Oficina de Nómina
Cuentas de Cobro	Formatos de cobro diligenciados	Jefe Oficina de Nómina

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Generalmente el dueño del activo es el líder del proceso o el jefe de una de las áreas pertenecientes al proceso.

Paso 3. Clasificar los activos:

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros.

La siguiente tabla presenta una propuesta de tipología de activos con el fin de hacer la clasificación mencionada.

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el *'good will'*, entre otros
Infraestructura crítica cibernética nacional	Se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

Tipo de activo	Descripción
	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Recursos Humanos	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones y Otros Servicios	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Ejemplo:

ACTIVO	TIPO DE ACTIVO
Base de datos de nómina	Información
Aplicativo de Nómina	Software
Cuentas de Cobro	Información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Paso 4. Clasificar la información:

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, los controles de la norma ISO27001:2022 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

Ejemplo:

ACTIVO	*TIPO DE ACTIVO*	*Ley 1712 de 2014*	*Ley 1581 de 2012*
Base de datos de nómina	Información	Información Reservada	Contiene datos personales
Aplicativo de Nómina	Software	N/A	N/A
Factura de venta	Información	Información Pública	No contiene datos personales

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Al realizar la identificación del contexto externo, la entidad pública debería tener plenamente identificados los aspectos regulatorios y normativos con los que deberá cumplir, las leyes enunciadas (1712 de 2014 y 1581 de 2012) pueden ser de cumplimiento para la mayoría de las entidades públicas sin embargo es tarea de la entidad pública determinar si hay más o menos aspectos regulatorios para tener en

cuenta respecto a la información. El **área jurídica** de Las entidades debe colaborar en esta tarea específica.

En este paso la entidad pública debe definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso. Para definir estas escalas puede tomar como referencia el documento de Lineamentos para el Inventario de Activos de Información del Modelo de Seguridad y Privacidad de la Información (MSPI)12, estas escalas deberán ser definidas y documentadas en un procedimiento de gestión de activos que debe ser aprobado por parte de la línea estratégica de la entidad pública.

ACTIVO	TIPO DE ACTIVO	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de Criticidad
Base de datos de nómina	Información	ALTA	ALTA	ALTA	ALTA
Aplicativo de Nómina	software	BAJA	MEDIA	BAJA	MEDIA
Listas de asistencia	Información	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Una vez se ejecute la identificación de los activos, la entidad pública debe definir si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto o altos y medios, esto debe estar debidamente documentando y aprobado por la **Línea Estratégica – Alta dirección**.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas Nacionales -ICCN-

Se invita a que las entidades públicas identifiquen si poseen ICC. Un activo se caracteriza y es considerado infraestructura crítica si su impacto o afectación podría cumplir alguno de los criterios establecidos por el COLCERT en sus LINEAMIENTOS EN CIBERSEGURIDAD

Si la entidad pública determina que tiene ICC, es importante que se identifiquen los componentes que conforman dicha infraestructura. Por ejemplo, dicha ICC puede tener componentes de TI (como servidores) o de TO (como sistemas de control industrial o sensores).

[12] http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html - Guía Gestión Clasificación de Activos

Las entidades deberán consultar y aplicar los criterios y la metodología de identificación de infraestructura critica cibernética que esté vigente, cada vez que realicen el inventario de activos de información o una actualización a este, estos criterios y metodología serán actualizados por el ColCERT.

Con base a los seis (6) pasos vistos previamente, la entidad pública podría generar un formato como el siguiente (ejemplo de referencia) para generar tanto su procedimiento de identificación e inventario de activos como el formato para hacer su levantamiento. El formato puede variar en cada entidad según la necesidad y normatividad aplicable o si desea integrar otra información.

Proceso	Activo	Descripción	Dueño del Activo	Tipo de Activo	Clasificación de información (Ley 1581 de 2012 / Ley 1712 de 2014)	Criticidad del Activo (De acuerdo con su confidencialidad, integridad y disponibilidad)
Ver Paso 1	Ver Paso 1	Ver Paso 1	Ver Paso 2	Ver Paso 3	Ver Paso 4	Ver Paso 5
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe oficina de nómina	Información	Ley 1712 Información reservada Ley 1581 Contiene datos personales Otras normas que apliquen	ALTA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Recomendaciones adicionales para la identificación de activos:

Para identificar los activos, realizar su inventario y clasificación, las entidades públicas pueden emplear los siguientes métodos:

- Revisión de los flujos o diagramas del proceso.
- Revisión de inventarios de activos previos o de otras áreas.
- Entrevistas o lluvia de ideas dentro de cada proceso.

Nota: adicional a lo anterior, el documento de **Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional del Modelo de Seguridad y Privacidad de la Información** de la Estrategia Gobierno

Digital de MINTIC, también brinda una orientación para clasificar los activos de información.

> Importante:
>
> La entidad pública puede decidir si realiza la gestión de riesgos en todos los activos identificados en este punto o si desea hacerlo a los activos más críticos. Esta decisión debe estar debidamente formalizada en el procedimiento de gestión de activos que solicita el **Modelo de Seguridad y Privacidad de la Información**. Adicionalmente, debe quedar explícita en la Política de Administración de Riesgos de la entidad pública, debidamente aprobada por el Comité Institucional de Coordinación de Control Interno.

3.1.8. Identificar los riesgos inherentes de seguridad de la información

Como lo indica el Paso 2 de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas" emitida por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad.
- Pérdida de la integridad.
- Pérdida de la disponibilidad.

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso o su ecosistema digital operativo, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

a) Identificación de Amenazas:

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

Ejemplos de amenazas clásicas

Categoría	Nº	Descripción de la amenaza	Tipo de fuente de riesgo *
Amenazas físicas	TP01	Fuego	A, D, E
	TP02	Agua	A, D, E
	TP03	Contaminación, radiación nociva	A, D, E
	TP04	Accidente grave	A, D, E
	TP05	Explosión	A, D, E
	TP06	Polvo, corrosión, heladas	A, D, E
Amenazas naturales	TN01	Fenómeno climático	E
	TN02	Fenómeno sísmico	E
	TN03	Fenómeno volcánico	E
	TN04	Fenómeno meteorológico	E
	TN05	Inundación	E
	TN06	Fenómeno de pandemia/epidemia	E
Fallas en las infraestructuras	TI01	Fallas en un sistema de suministro	A, D
	TI02	Falla del sistema de refrigeración o ventilación	A, D
	TI03	Pérdida del suministro eléctrico	A, D, E
	TI04	Falla de una red de telecomunicaciones	A, D, E
	TI05	Falla del equipo de telecomunicaciones	A, D
	TI06	Radiación electromagnética	A, D, E
	TI07	Radiación térmica	A, D, E
	TI08	Impulsos electromagnéticos	A, D, E
Fallas técnicas	TT01	Falla de dispositivos o sistemas	A
	TT02	Saturación del sistema de información	A, D
	TT03	Vulneración del mantenimiento del sistema de información	A, D
Acciones humanas	TH01	Atentado terrorista, sabotaje	D
	TH02	Ingeniería social	D
	TH03	Interceptación de la radiación de un dispositivo	D
	TH04	Espionaje remoto	D
	TH05	Escucha clandestina	D
	TH06	Robo de medios o documentos	D
	TH07	Robo de equipos	D
	TH08	Robo de identidad digital o de credenciales	D
	TH09	Recuperación de medios reciclados o descartados	D
	TH10	Divulgación de información	A, D
	TH11	Entrada de datos de fuentes no fiables	A, D
	TH12	Manipulación con hardware	D
	TH13	Manipulación con software	A, D
	TH14	Ataque de descarga oculta a través de internet	D
	TH15	Ataque de repetición, ataque de intermediario	D

	TH16	Tratamiento no autorizado de datos personales	A, D
	TH17	Entrada no autorizada en instalaciones	D
	TH18	Uso no autorizado de dispositivos	D
	TH19	Uso incorrecto de dispositivos	A, D
	TH20	Daño de dispositivos o medios	A, D
	TH21	Copia ilícita de software	D
	TH22	Uso de software falsificado o copiado	A, D
	TH23	Corrupción de datos	D
	TH24	Tratamiento ilegal de datos	D
	TH25	Envío o distribución de malware	A, D, E
	TH26	Detección de posición	D
Compromiso de funciones o servicios	TC01	Error en el uso	A
	TC02	Abuso de derechos o permisos	A, D
	TC03	Falsificación de derechos o permisos	D
	TC04	Denegación de acciones	D
Amenazas a la organización	TO01	Falta de personal	A, E
	TO02	Falta de recursos	A, E
	TO03	Falla de los proveedores de servicios	A, E
	TO04	Violación de la legislación o la normativa	A, D
* D : deliberado; A : accidental; E : medioambiental			

Tabla 2 Tabla de amenazas

Fuente: ISO/IEC 27005:202209

- Deliberadas (D), fortuitas (F) o ambientales (A).

    - Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	• Reto • Ego • Rebelión • Estatus • Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	• Destrucción de la información • Divulgación ilegal de la información • Ganancia monetaria • Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema

Fuente de amenaza	Motivación	Acciones amenazantes
Terrorismo	• Chantaje • Destrucción • Explotación • Venganza • Ganancia política • Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	• Ventaja competitiva • Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	• Curiosidad • Ego • Inteligencia • Ganancia monetaria • Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema

Fuente de amenaza	Motivación	Acciones amenazantes
		• Acceso no autorizado al sistema.

Tabla 3 Tabla de amenazas dirigida por el hombre

Fuente: ISO/IEC 27005:2022

b) Identificación de vulnerabilidades:

la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Ejemplos de vulnerabilidades clásicas

Categoría	Nº	Ejemplos de vulnerabilidades
Hardware	VH01	Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento
	VH02	Programas insuficientes para el reemplazo periódico de equipos
	VH03	Susceptibilidad a la humedad, al polvo y a la suciedad
	VH04	Sensibilidad a la radiación electromagnética
	VH05	Control insuficiente de los cambios de configuración
	VH06	Susceptibilidad a las variaciones de tensión
	VH07	Susceptibilidad a las variaciones de temperatura
	VH08	Almacenamiento sin protección
	VH09	Falta de protección a la disposición final
	VH10	Copia no controlada
Software	VS01	Pruebas de software inexistentes o insuficientes
	VS02	Defectos conocidos en el software
	VS03	No se cierra la sesión al abandonar el puesto de trabajo
	VS04	Disposición o reutilización de medios de almacenamiento sin un borrado adecuado
	VS05	Configuración insuficiente de los registros para fines de auditoría
	VS06	Asignación errónea de derechos de acceso
	VS07	Software ampliamente distribuido
	VS08	Aplicación de programas de aplicación a datos erróneos desde el punto de vista cronológico
	VS09	Interfaz de usuario complicada
	VS10	Documentación insuficiente o inexistente
	VS11	Configuración incorrecta de los parámetros
	VS12	Fechas incorrectas
	VS13	Mecanismos insuficientes de identificación y autenticación (por ejemplo, para la autenticación de usuarios)
	VS14	Tablas de contraseñas desprotegidas
	VS15	Gestión deficiente de contraseñas
	VS16	Activación de servicios innecesarios
	VS17	Programas informáticos nuevos o inmaduros
	VS18	Especificaciones poco claras o incompletas para los desarrolladores
	VS19	Control ineficiente de los cambios

	VS20	Descarga y uso de programas informáticos incontrolados
	VS21	Copias de seguridad inexistentes o incompletas
	VS22	Incumplimiento de la elaboración de informes de gestión
Red	VN01	Mecanismos insuficientes para la prueba de envío o recepción de un mensaje
	VN02	líneas de comunicación sin protección
	VN03	Tráfico sensible sin protección
	VN04	Cableado de empalme deficiente
	VN04	Un solo punto de falla
	VN06	Ineficacia o falta de mecanismos para la identificación y autenticación del remitente y el destinatario
	VN07	Arquitectura de red insegura
	VN08	Transferencia de contraseñas en claro
	VN09	Gestión inadecuada de la red (resiliencia del enrutamiento)
	VN10	Conexiones a redes públicas sin protección
Personal	VP01	Ausencia de personal
	VP02	Procedimientos inadecuados de contratación
	VP03	Formación insuficiente sobre seguridad
	VP04	Uso incorrecto de software y hardware
	VP05	Escasa concienciación en materia de seguridad
	VP06	Mecanismos de monitoreo insuficientes o inexistentes
	VP07	Trabajo de personal externo o de limpieza sin supervisión
	VP08	Ineficacia o falta de políticas para el uso correcto de los medios de telecomunicación y mensajería
Instalaciones	VS01	Uso inadecuado o descuidado del control de acceso físico a edificios y salas
	VS02	Ubicación en una zona susceptible de inundación
	VS03	Red de energía inestable
	VS04	Protección física insuficiente del edificio, puertas y ventanas
Organización	VO01	No se ha creado un procedimiento formal para el registro y la cancelación de usuarios, o su aplicación es ineficaz
	VO02	No se ha creado un proceso formal de revisión (supervisión) de los derechos de acceso, o su aplicación es ineficaz
	VO03	Disposiciones insuficientes (en materia de seguridad) en los contratos con clientes y/o con terceros
	VO04	No se ha creado un procedimiento de monitoreo de las instalaciones de tratamiento de la información, o su aplicación es ineficaz
	VO05	Las auditorías (supervisión) no se realizan con regularidad
	VO06	No se han creado procedimientos de identificación y evaluación de riesgos, o su aplicación es ineficaz
	VO07	Insuficiencia o falta de informes de averías grabados en los registros del administrador y del operador
	VO08	Respuesta inadecuada del servicio de mantenimiento
	VO09	Acuerdo de nivel de servicio insuficiente o inexistente
	VO10	No se ha creado un procedimiento de control de cambios, o su aplicación es ineficaz
	VO11	No se ha creado un procedimiento formal para el control de la documentación del SGSI, o su implementación es ineficaz
	VO12	No se ha creado un procedimiento formal para la supervisión de los registros del SGSI, o su implementación es ineficaz
	VO13	No se ha creado un procedimiento formal para la autorización de información pública, o su implementación es ineficaz
	VO14	Asignación inadecuada de responsabilidades en materia de seguridad de la información

	VO15	Los planes de continuidad no existen, están incompletos o son obsoletos
	VO16	No se ha creado una política de uso del correo electrónico, o su aplicación es ineficaz
	VO17	No se han creado procedimientos para introducir software en los sistemas operativos, o su aplicación es ineficaz
	VO18	No se han creado procedimientos para el tratamiento de información clasificada, o su aplicación es ineficaz
	VO19	Las responsabilidades con respecto a la seguridad de la información no están presentes en las descripciones de los cargos
	VO20	Insuficiencia o falta de disposiciones (respecto a la seguridad de la información) en los contratos con los empleados
	VO21	No se ha definido el proceso disciplinario en caso de incidentes de seguridad de la información, o no funciona correctamente
	VO22	No se ha creado una política formal sobre el uso de computadores móviles, o su aplicación es ineficaz
	VO23	Control insuficiente de los activos fuera de las instalaciones
	VO24	Insuficiencia o falta de una política de “escritorio y pantalla limpios”
	VO25	Autorización de instalaciones de tratamiento de la información no implementada o que no funciona correctamente
	VO26	Los mecanismos de monitoreo de las infracciones de seguridad no se implementan correctamente
	VO27	No se han creado procedimientos para notificar las deficiencias de seguridad, o su aplicación es ineficaz
	VO28	No se han creado procedimientos de conformidad con las disposiciones en materia de derechos intelectuales, o su aplicación es ineficaz

Tabla 4 Tabla de Vulnerabilidades Comunes

Fuente: ISO/IEC 27005:2022

NOTA: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
HARDWARE	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de Información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Susceptibilidad a las variaciones de voltaje	Perdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección física	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
SOFTWARE	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
INFRAESTRUCTURA CRITICA CIBERNETICA	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
RECURSO HUMANOS	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
INSTALACIONES	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Hurto de medios o documentos
	Ubicación en área susceptible de inundación	Destrucción de equipos o medios
	Red energética inestable	Falla en equipo de telecomunicaciones
	Ausencia de protección física de la edificación (Puertas y ventanas)	Hurto de medios o documentos
SERVICIOS	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de estos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al publico	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

Tabla 5 Tabla de Amenazas y Vulnerabilidades

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

c) Descripción de los riesgos de seguridad de la información:

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Adicionalmente, se debe identificar el dueño del riesgo, es decir, "quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo" [13].

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

- **Lluvia de ideas:** mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la entidad pública o en el sector. Deben existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias.

- **Juicio de expertos:** a través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad de la información se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración.

- **Análisis de escenarios**: en este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse: explosión de un pozo, sobrecarga de un nodo, pérdida de control de una unidad operada remotamente; y con base en estas posibilidades, se determina qué puede llegar a suceder, desde la perspectiva digital, a los activos de información y las consecuencias de la afectación.

- **Otras técnicas que pueden ser empleadas** son: entrevistas estructuradas, encuestas o listas de chequeo.

Posterior a la identificación de los riesgos de seguridad de la información con sus respectivas amenazas y vulnerabilidades enunciadas en este documento, se deberá continuar con el Paso de Valoración del Riesgo, de la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas" del DAFP.

3.1.9. Identificación del nivel de confianza para la autenticación digital

Se deben identificar aquellos tramites y servicios ciudadanos digitales que deben contar con autenticación digital de acuerdo con lo señalado en la guía de lineamientos para los Servicios Ciudadanos Digitales, en la que se establece que inicialmente, para

[13] GTC 137 Gestión del Riesgo. Vocabulario

el acceso al servicio de Autenticación Digital, las entidades deben identificar y determinar el grado de confianza requerido para los procesos relacionados con el trámite acorde con la siguiente clasificación:

- Bajo: Ofrece un nivel de confianza mínimo en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es mínimo.

- Medio: Ofrece cierto nivel de confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es moderado.

- Alto: Ofrece una gran confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo alto.

- Muy alto: Ofrece más confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo extremo.

Para la definición del nivel de confianza y establecer el nivel de garantía requerido para el sistema de información asociado al trámite que usará el servicio de Autenticación Digital, se debe realizar el proceso para la valoración de riesgos de Seguridad de la información, señalado en la Guía para la administración de riesgos y diseño de controles de la Función Pública, en el capítulo 5. Lineamientos riesgos de seguridad de la información y lo establecido en el catálogo y metodología de Infraestructuras Criticas Cibernéticas del Ministerio de Tecnologías de la Información y las Comunicaciones.

En este sentido, es necesario identificar dentro del inventario de activos de información aquellos activos de tipo software que requieren autenticación digital, especialmente si los trámites o servicios digitales asociados solo pueden ser realizados por el titular de la información. En estos casos, debe establecerse un control de autenticación digital adecuado, cuyo nivel se determinará a partir del análisis del impacto por pérdida de confidencialidad, integridad y disponibilidad. Este análisis debe considerar la vulnerabilidad asociada a la ausencia de mecanismos de identificación y autenticación (como el inicio de sesión de usuario), así como la amenaza de falsificación de derechos sobre dichos activos de software.

Posteriormente, se debe realizar el análisis de probabilidad e impacto de materialización de los riesgos identificados, con el fin de determinar su nivel conforme a la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (niveles: extremo, alto, moderado o bajo). A partir de este resultado, se establecerá el grado de confianza requerido para la autenticación digital (muy alto, alto, medio o bajo). Una vez definido el nivel de confianza, se deben aplicar los lineamientos de la Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales, con el fin de adelantar el proceso de vinculación al servicio de autenticación digital.

3.1.10. Valoración del riesgo

Para realizar la valoración de los riesgos de seguridad de la información se debe llevar a cabo: el análisis de riesgo, la evaluación del riesgo, las estrategias para combatir el riesgo, las herramientas para la gestión del riesgo y finalmente el monitoreo y revisión tal como se establece en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del Departamento Administrativo de la función Pública (DAFP).

3.1.11. Identificación y evaluación de los controles existentes

Como lo indica la Guía de DAFP, arriba mencionada, una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios.

Nota: Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se puede consultar la sección **4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA** (*Tomados del Anexo A de la Norma ISO/IEC 27001:2022* como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad de la información que están enunciados en dicho anexo.

3.1.12. Tratamiento de los riesgos de seguridad de la información

Una vez se han identificado los riesgos, la entidad pública debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional.

El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la entidad pública puede tener en cuenta las opciones planteadas en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del DAFP: **aceptar, reducir, evitar, compartir el riesgo.**

Importante:

Si la entidad pública decide **mitigar o tratar el riesgo** mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, deberá tener en cuenta la **Sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA**, basados en la norma ISO/IEC 27001:2022 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad de la información, sin embargo, la entidad pública puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

3.1.13. Planes de Tratamiento de Riesgos de Seguridad de la información e Indicadores para la Gestión del Riesgo

Los planes de tratamiento de riesgos y los indicadores para medir la eficacia o la efectividad se deberán generar como lo indica el **Esquema 9. Consolidación de los Planes de Tratamiento de Riesgos,** de la *"Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas Versión 4 - 2018 "* emitida por el DAFP.

Nota: Tenga en cuenta para el diseño de controles, los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes, por lo tanto, se sugiere remitirse a dicho documento.

3.2. Fase 2. Ejecución

Esta fase se centra en la implementación de los planes de tratamiento de riesgos definidos en la fase anterior, en esencia es seguir la ruta crítica definida y llevar a cabo todo lo planeado en la Fase 1.

Aquí la Línea Estratégica debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes (Primer Línea de Defensa y la Oficina de Tecnologías de la Información -TI- generalmente) ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

3.3. Fase 3. Monitoreo y revisión

La entidad pública a través de las Tres Líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, Componente Actividades de control, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.

- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.

- Realizar monitoreo de los riesgos y controles tecnológicos que contemple alertas y vulnerabilidades genéricas que puedan generar eventos o incidentes que posteriormente implique una materialización de riesgo.

- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad de la información para verificar su efectividad.

- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.

- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Nota 1: Una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad pública debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el ultimo nivel de riesgo residual.

En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad pública. Así mismo, también deberán tenerse en cuenta los incidentes de seguridad de la información que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y las partes interesadas.

Nota 2: De conformidad con la implementación del presente lineamiento es importante tener en cuenta que, una vez se publique la metodología para la identificación de infraestructuras criticas cibernéticas establecida en el Decreto 338 de 2022, se actualizarán los lineamientos generados en el presente documento para realizar la identificación y evaluación mediante una nueva metodología de riesgos, la cual será de obligatorio cumplimiento para entidades del sector público.

a) Registro y reporte de incidentes de seguridad de la información

Es importante que la entidad pública cuente con el registro de los incidentes de seguridad de la información que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

Nota: El reporte de incidentes de seguridad de la información a terceros (entes de control, reguladores, superintendencias, instancias o autoridades en la materia, entre otros), no es la misionalidad del presente documento, sin embargo, se recomienda realizar dichos reportes conforme lo estipulan los entes o las buenas prácticas en seguridad de la información.

3.3.1. Reporte de la gestión del riesgo de seguridad de la información al interior de la entidad pública

El responsable de seguridad digital debería reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

REPORTE

1. Matriz de los riesgos identificados de seguridad de la información.
2. Listado de activos críticos TI/TO y listado de ICC.
3. Reporte de criticidad/impacto de la organización.
4. Plan de tratamiento de riesgos.
5. Reporte de evolución de riesgos y modificación del riesgo.
6. Cantidad de riesgos por fuera de la tolerancia del riesgo identificados de acuerdo con la periodicidad de evaluación realizada.
7. Impacto económico que podría presentarse frente a la materialización de los riesgos.

PERIODICIDAD

> Periódicamente por parte de todas las Entidades u organizaciones que han adoptado el modelo respectivo.
> Cuando ocurra un cambio organizacional o de procesos de la organización que genere un impacto en las operaciones o que pueda afectar los riesgos ya identificados anteriormente. En este caso debe realizarse una nueva evaluación de los riesgos y reportar los resultados a la Entidad de control.
> Cuando se incluya un nuevo proceso dentro del alcance de la gestión de riesgos de seguridad de la información de la Entidad. En este caso se debe realizar una nueva evaluación de riesgos y reportar los resultados a la Entidad de control.

Ilustración 2 Reportes de información por parte de la entidad.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

3.3.2. Reporte de la gestión del riesgo de seguridad de la información a autoridades o entidades especiales

Una vez la entidad pública obtenga los resultados de la gestión de riesgos de seguridad de la información, se debería consolidar información (previamente obtenida con la aplicación del modelo) con el fin de reportarla a futuro a las autoridades o instancias encargadas del tema y que el Gobierno defina.

La finalidad del reporte de esta información es que el Gobierno Nacional pueda identificar posibles oportunidades para la generación de política pública, generación de capacidades o asignación de recursos que permita ayudar a la mejora de la seguridad de la información.

Información por consolidar para generar el reporte de información:

Se propone que las entidades públicas consoliden la siguiente información puntual para poder llevar a cabo el reporte respectivo:

- Riesgos con nivel crítico.

- Amenazas críticas.
- Vulnerabilidades críticas.
- Tipos de Activos afectados por los riesgos críticos (incluyendo servicios digitales o que delimitan con internet).
- Planes de tratamiento propuestos para la mitigación y si han sido ejecutados.
- Servicios digitales críticos en la entidad pública (Servicios o trámites para los ciudadanos o sistemas de información críticos para la entidad).

Esta información tiene por objetivo permitir la construcción de un panorama de riesgos de seguridad de la información de todo el país, para poder tomar decisiones estratégicas para la construcción de política pública, generación de capacidades o planes de acción con base a la información que pueda analizarse.

Reportes relacionados con Infraestructuras Críticas Cibernéticas, cuando aplique:

Las infraestructuras críticas cibernéticas -ICC- que hayan sido identificadas deberían reportarse a las autoridades o instancias encargadas del tema en el Gobierno nacional.

Nota: Es importante indicar que los reportes de riesgos de seguridad de la información a las entidades de gobierno no implicarían o significarían el traslado de la responsabilidad sobre los riesgos o su tratamiento.

3.3.3. Auditorías internas y externas

Le corresponde a las Unidades de Control Interno (tercera línea de defensa), realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad de la información en la entidad pública, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

3.3.4. Medición del desempeño

La entidad pública debe utilizar medidas de desempeño (indicadores[14]) para la gestión de los riesgos de seguridad de la información, las cuales deben reflejar el

[14] Consultar en la *Guía de Administración del Riesgo de Gestión, Corrupción y Seguridad de la información* del DAFP – Sección Indicadores - Gestión del Riesgo de Seguridad de la información, para definir indicadores de seguimiento para la gestión del riesgo de seguridad de la información.

cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente alineadas con la revisión por la línea estratégica.

3.4. Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad de la información

La entidad pública debe garantizar la mejora continua de la gestión de riesgos de seguridad de la información, por lo tanto, debe establecer que cuando existan

hallazgos, falencias o incidentes de seguridad de la información se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad de la información de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

4. Controles de De Referencia Para La Mitigación De Los Riesgos De Seguirdad

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando los controles, del numeral 11.1 Controles y objetivos de control, del documento maestro del Modelo de Seguridad y Privacidad de la Información - MSPI.

TIC

Lineamientos De Gestión de incidentes de seguridad de la información y seguridad digital

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de contenido

Tabla de contenido 152
Listado de Tablas 153
Tabla de ilustraciones 153
Lineamientos De Gestión de incidentes de seguridad de la información y seguridad digital 154
1. Derechos De Autor 154
2. Audiencia 154
3. Introducción 154
4. Justificación 154
5. Objetivos 155
6. Alcance 156
7. Adaptabilidad al ciclo de vida de la ciberseguridad NIST 156
8. Gestión De Incidentes 158
8.1. ¿Qué es la gestión De incidentes? 158
8.1.1. Evento 158
8.1.2. Incidente de seguridad digital 158
8.2. Objetivos 158
8.3. Despliegue de acciones adecuadas para la gestión de incidente. 159
9. Ciclo de vida de la gestión de incidentes 160
9.1. Preparación 161
9.1.1. Acciones de prevención: 162
9.2. Detección y Análisis 163
9.2.1. Identificación de incidentes 163
9.2.2. Análisis 164
9.2.3. Documentación del incidente. 165
9.2.4. Clasificación de Incidentes de seguridad de la información y seguridad digital 166
9.2.5. Priorización del incidente 170
9.2.6. Criterios de valoración del Nivel de Impacto 171
9.2.7. Criterios de valoración del nivel de recuperabilidad - urgencia del Incidente 172
9.2.8. Tiempos de Respuesta 173
9.3. Contención, Erradicación y Recuperación 174
9.3.1. Recopilación y preservación de evidencia 175
9.3.2. Erradicación y Recuperación 175

9.3.3. Recuperación 175
10. Actividades posteriores al Incidente. 176
10.1. Lecciones aprendidas. 176
10.2. Uso de datos e información recopilados del incidente. 177
10.2.1. Evaluación Objetiva: 178
10.2.2. Evaluación Subjetiva: 178
10.3. Retención de pruebas: 179
10.4. Lista de verificación para la gestión de incidentes. 179
11. Recomendaciones Generales 180
12. Coordinación e intercambio de información. 181
13. Lineamientos a considerar. 181
14. Referencias. 182

Listado de Tablas

Tabla 6 Taxonomía clasificación de incidentes 170
Tabla 7 Descripción categorías de impacto función y de compromisos de información 172
Tabla 8 Descripción de categorías de impacto de recuperabilidad de las operaciones 172
Tabla 9 Descripción de escalas de nivel de prioridad de atención de incidentes 173
Tabla 10 Descripción Tiempos Máximos de Atención de Incidentes por parte del IRT 174
Tabla 11 Pasos para seguir en la gestión del incidente 180
Tabla 12 Lineamientos a considerar 182

Tabla de ilustraciones

Ilustración 1 Figura adaptada al Modelo CSF NIST 2.0 – Funciones del CSF 157
Ilustración 2 Ciclo de vida de Gestión de incidentes- NIST.SP 800-61 r2 161

Lineamientos De Gestión de incidentes de seguridad de la información y seguridad digital

1. Derechos De Autor

Para el desarrollo de este lineamiento, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre por parte del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide Special Publication 800-61 Revisión 2) y el artículo 9 de la Resolución 500 de 2021 MinTIC.

2. Audiencia

Entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno Digital, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la estrategia de seguridad digital.

3. Introducción

Este anexo entrega los lineamientos básicos para poner en marcha un Sistema de Planificación y Preparación de la Gestión de Incidentes de Seguridad Digital y de la información física impresa, a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren.

4. Justificación

El lineamiento expuesto en este documento es un complemento del Modelo de Seguridad y Privacidad de la Información MSPI y se constituye en un referente de planificación y preparación de la gestión de incidentes de seguridad de la información y seguridad digital, para las entidades del Estado.

La gestión de incidentes de seguridad digital (ciberseguridad) se ha convertido en una actividad relevante e indispensable de las áreas de tecnologías y seguridad de la información por el volumen de ataques a las infraestructuras tecnológicas y los nuevos métodos cada vez más sofisticados que afectan a mayor escala, así las cosas, las entidades y organizaciones necesitan capacidades de respuesta que permita detectar de manera rápida y oportuna los incidentes que puedan presentarse, minimizando el impacto y permitiendo restaurar los servicios afectados en el menor tiempo posible .

Estos lineamientos proporcionan recomendaciones y pautas que deben ser adoptadas por las entidades y organizaciones sin importar el tipo de infraestructura con las que se cuente, de igual manera, es necesario realizar una identificación de activos y gestión de riesgos para asegurar la infraestructura, compartir información con las comunidades para alertar sobre amenazas y establecer estrategias de respuesta contra los ataques más comunes.

Es fundamental establecer un criterio para la priorización de atención de los incidentes (Resolución 500 del 2021 – MinTIC), un procedimiento de lecciones aprendidas para realizar los ajustes y mejoras al proceso de gestión de incidentes. Finalmente, se debe revisar la matriz de riesgo y diseñar controles que permitan ajustar la postura de seguridad digital de la entidad/Organización.

5. Objetivos

El objetivo principal del presente documento de planificación y preparación de la gestión de incidentes de seguridad digital es tener un enfoque estructurado, consensuado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información / seguridad digital (Ciberseguridad).

Los objetivos específicos del presente documento son:

Identificar y Gestionar los incidentes de seguridad de la información /seguridad digital (Ciberseguridad) para ser evaluados y dar respuesta de la manera más eficiente y adecuada.

Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.

Definir roles y responsabilidades dentro de los sujetos obligados, para mejorar la postura de seguridad de la infraestructura tecnológica, mediante la identificación de activos de información, la gestión de riesgos, la gestión de incidentes que permitan la continuidad de las operaciones en el tiempo.

Establecer e implementar el procedimiento de gestión de incidentes de seguridad de la información y de seguridad digital (Ciberseguridad), según lo establecido en el presente documento, la Resolución 500 del 2021 del MinTIC, la norma ISO/IEC 27001:2022.

Gestionar los incidentes de seguridad de la información/seguridad digital (Ciberseguridad), que se presenten en la infraestructura tecnológica, infraestructura crítica ICC y servicios esenciales de manera eficiente y adecuada por parte del Equipo de Respuesta a Incidentes de Seguridad de la Información – IRT.

Minimizar los impactos adversos de los incidentes, mediante la oportuna gestión por parte del Equipo de Respuesta a Incidentes de Seguridad de la Información - IRT.

Consolidar las lecciones aprendidas producto de los incidentes de seguridad de la información/seguridad digital (Ciberseguridad), identificando de puntos de mejora, actualización de riesgos y ajustes de controles, para incrementar las oportunidades

de prevenir la ocurrencia de futuros incidentes, mejorar la postura de seguridad y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes.

Definir los protocolos formales de reporte y escalamiento de los incidentes de seguridad de la información/seguridad digital (Ciberseguridad) clasificados como Muy Graves y Graves al CSIRT Gobierno/COLCERT, para su respectivo apoyo y coordinación de su gestión.

Garantizar que los incidentes de seguridad de la información y de seguridad digital (Ciberseguridad) se documenten de manera consistente, utilizando la taxonomía establecida por el COLCERT y estándares apropiados para la categorización, clasificación e intercambio de información producto de la gestión de incidentes.

Activar comités de crisis cuando se presenten incidentes que afecten infraestructura crítica y servicios esenciales e incidentes de impacto crítico y nacional, que involucren los diferentes lideres de proceso y articular las acciones que desde cada una de las áreas corresponda para la recuperación de las operaciones, las acciones jurídicas a desplegar, la asignación de recursos y las comunicaciones internas y externas entre otras.

6. Alcance

Estos lineamientos aplican a todos los incidentes de seguridad de información y seguridad digital que puedan afectar a la confidencialidad, integridad o disponibilidad de la información o los sistemas de información de entidades / organizaciones que forman parte de la Rama Ejecutiva, sin embargo, también puede ser aplicada a las demás ramas de poder público, teniendo en cuenta la adopción de buenas prácticas de seguridad digital. Además, debe comprender el relacionamiento de un efectivo tratamiento de la evidencia digital y la referenciación basada en la Resolución 500 del 2021 del MinTIC, la norma ISO/IEC 27001:2022 y la política de Gobierno Digital con el Modelo de Seguridad y Privacidad de la Información - MSPI.

Adicionalmente el presente lineamiento tiene como finalidad brindar a las entidades/ organizaciones una estructura y directrices claras para gestionar eficientemente los incidentes de seguridad digital y relacionar los efectos de cada uno de los factores de los Marcos de Trabajo del NIST Cybersecurity Framework (CSF) 2.0, el FIRST CSIRT Services Framework Version 2.1, 2019) y las mejores prácticas de gestión de incidentes.

7. Adaptabilidad al ciclo de vida de la ciberseguridad NIST

El Framework de Ciberseguridad (CSF) del NIST v4.0 es un marco integral de referencia para comenzar y mejorar los procedimiento y políticas de Seguridad digital (Ciberseguridad), con el propósito de mejorar la postura de Seguridad, incentivar la gobernanza, promover las comunicaciones y alinear los riesgos de Seguridad Digital con los riesgos de proceso.

El marco está organizado en seis funciones: gobernar, identificar, proteger, detectar, responder, recuperar, los cuales conjuntamente proporcionan una visión integral del ciclo de vida para la gestión del riesgo de ciberseguridad a lo largo del tiempo.

Gobernar: Incorporar en la estrategia de gestión de riesgos, actividades de gobernanza para conocer el contexto organizacional, el establecimiento de una estrategia de seguridad digital, gestión de riesgos en las cadenas de suministros, roles, responsabilidades, políticas y seguimiento.

Identificar: Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de datos, hardware, software, sistemas, instalaciones, servicios, personas y capacidades.

Proteger: Desarrollar e implementar las protecciones apropiadas para garantizar la entrega de servicios.

Detectar: Desarrollar e implementar las actividades apropiadas para identificar cuando ocurra un evento de seguridad digital (ciberseguridad).

Responder: Desarrollar e implementar las actividades apropiadas para tomar acciones en relación con un incidente de seguridad digital (ciberseguridad) detectado.

Recuperar: Desarrollar e implementar las actividades necesarias para implementar y mantener planes de recuperación para reestablecer los servicios y capacidades que hayan sido afectados durante el incidente de seguridad digital (ciberseguridad).

Ilustración 1 Figura adaptada al Modelo CSF NIST 2.0 – Funciones del CSF

8. Gestión De Incidentes

8.1. ¿Qué es la gestión De incidentes?

La gestión de incidentes es un proceso sistemático para identificar, documentar, clasificar, priorizar, resolver y registrar incidentes de seguridad de la información y seguridad digital que puedan afectar la confidencialidad, integridad o disponibilidad de la información o los sistemas de información de una entidad u organización.

8.1.1. Evento

Un evento es cualquier suceso observable en un sistema o red, como un usuario que se conecta a un recurso compartido de archivos, un usuario que envía un archivo electrónico o un firewall que bloquea un intento de conexión, entre otros.

Igualmente, los eventos adversos, son aquellos que tienen consecuencias negativas, como fallos en un sistema, usos no autorizados de privilegios en un sistema, acceso no autorizados y ejecución de malware.

8.1.2. Incidente de seguridad digital

Un incidente es una violación o amenaza inminente a las políticas de seguridad digital, políticas de uso aceptable y o prácticas de seguridad básicas. (Fuente: NIST.SP 800-62r2.)

Teniendo en cuenta las Guías del Instituto Nacional de Tecnologías de la Comunicación y el Centro Nacional para la Protección de las Infraestructuras Computer Security Incident Handling Guide (Cichonski et al., 2012) y la Guía de Recomendaciones y Consideraciones para los riesgos de Ciberseguridad - NIST - Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (Publications, 2023).

8.2. Objetivos

Los objetivos de la Gestión de incidentes de Seguridad Digital son:

- Minimizar el impacto de los incidentes de seguridad.
- Identificar y corregir la causa raíz de los incidentes.
- Prevenir que se repitan los incidentes.

- Mejorar la postura de seguridad de las entidades/organizaciones.
- Identificar precursores e indicadores para evitar incidentes mediante la implementación de medidas preventivas y correctivas adecuadas. Además de:

Cumplir con las obligaciones legales y contractuales con relación a la gestión de incidentes de Seguridad Digital en Colombia de acuerdo con la Política de Seguridad Digital, de Gobierno Digital, el Decreto 1078 de 2015, adicionado por el Decreto 338 del 2022 y la Resolución 500 del 2021 del MinTIC.

Ayudar a las entidades/organizaciones a mitigar los riesgos de los incidentes de seguridad digital proporcionando pautas sobre cómo responder ante éstos de manera eficaz y eficiente.

Proporcionar lineamientos para establecer un programa efectivo de respuesta a incidentes, con un enfoque principal en la detección, análisis, priorización y manejo de incidentes

8.3. Despliegue de acciones adecuadas para la gestión de incidente.

Desarrollar una política de gestión de incidentes: La política de gestión de incidentes debe definir los objetivos del programa, los roles y responsabilidades de las diferentes partes involucradas, así como los procesos para identificar, clasificar, priorizar, resolver y registrar incidentes de seguridad.

Establecer un Equipo de Respuesta a Incidentes (IRT):

El IRT debe estar integrado en el Modelo de Seguridad de la Información MSPI o Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, cuya función principal es gestionar y mitigar los eventos no deseados que afectan la seguridad de la información/Seguridad digital. Este equipo centraliza la coordinación y supervisión de la respuesta a los incidentes, articulando cada una de las acciones de contención, erradicación y recuperación con el equipo técnico y administrativo, así mismo proporcionado directrices a las diferentes dependencias de la entidad encaminadas a gestionar los incidentes de manera adecuada.

El IRT debe estar integrado al Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, cuya función principal es gestionar y mitigar los eventos no deseados que afectan la seguridad de la información y la seguridad digital. Este equipo centraliza la coordinación y supervisión de la respuesta a los incidentes, articulando cada una de las acciones de contención, erradicación y recuperación con los equipos técnicos y administrativos. Además, proporciona directrices a las diferentes dependencias de la entidad para gestionar los incidentes de manera adecuada.

Crear un plan de respuesta a incidentes: El plan de respuesta a incidentes debe describir los pasos a seguir para gestionar los incidentes de seguridad, incluyendo aquellos relacionados

con la seguridad de la información y seguridad digital (Incident management, 2022). El plan debe incluir información sobre cómo desarrollar e implementar cada una de las etapas, como son: preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas.

Capacitar al personal en gestión de incidentes: El personal de la entidad/organización debe estar capacitado en los procesos de gestión de incidentes. La capacitación debe cubrir temas como el análisis e identificación de incidentes de seguridad, la comunicación de incidentes, la respuesta a incidentes, la recuperación de incidentes y la investigación de éstos.

Probar y actualizar regularmente el plan de respuesta a incidentes: El plan de respuesta a incidentes debe probarse y actualizarse de manera regular para garantizar su efectividad y para que refleje los cambios en el entorno de amenazas.

Reporte de Incidentes:

Una vez identificado un incidente de seguridad digital/ciberseguridad por el IRT, el responsable de seguridad digital de la entidad (CISO) debe reportar al CSIRT Gobierno/COLCERT, a través de los canales de atención, los incidentes catalogados como Muy Grave y Grave. Esto permitirá el despliegue del apoyo y la coordinación en la gestión del incidente. Para ello, se debe utilizar el formato de reporte establecido, disponible en el sitio web del COLCERT.

De igual manera, los incidentes catalogados como Menos Grave y Menor deben ser registrados en el formulario disponible en el portal web del COLCERT una vez gestionados, con el propósito de identificar los tipos de incidentes que afectan a las entidades y mantener una estadística de estos.

Asimismo, los incidentes de seguridad digital/ciberseguridad que afecten bases de datos y archivos con datos personales deben ser reportados a la Superintendencia de Industria y Comercio (SIC) a través del portal de Registro Nacional de Bases de Datos o por los canales de atención establecidos.

9. Ciclo de vida de la gestión de incidentes

Para la gestión de incidentes de seguridad de la información y seguridad digital (Ciberseguridad) y teniendo en cuenta el Marco de Ciberseguridad (CSF) del NIST v4.0, se tomará como estándar para desarrollar los lineamientos de gestión de incidentes el estándar NIST.SP.800-61r2, así las cosas, el procedimiento de gestión de incidentes contempla varias fases, las cuales corresponde Preparación, Detección y Análisis, Contención, Erradicación y Recuperación y Actividades Post-Incidente.

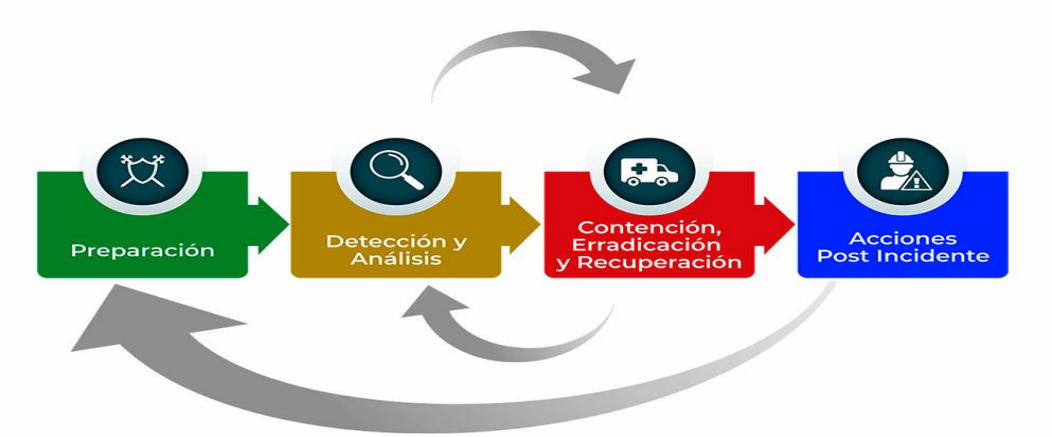


Ilustración 2 Ciclo de vida de Gestión de incidentes- NIST.SP 800-61 r2

Fuente: https://grupo-siayec.com.mx/images/blog/principal/thum31.jpg

9.1. Preparación

En esta fase inicial, se establece y capacita al Equipo de Respuesta a Incidentes (IRT) como parte del Modelo de Seguridad de la Información (MSPI) o Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando directrices a las diferentes dependencias de la entidad para gestionar los incidentes de manera adecuada. Asimismo, esta etapa contempla la asignación de recursos y la adquisición de herramientas tecnológicas y de seguridad digital para identificar y mitigar los eventos no deseados que afectan la seguridad de la información y la seguridad digital. La implementación de esta fase contribuye a la gestión de riesgos y al fortalecimiento de la postura de seguridad de la infraestructura tecnológica, de acuerdo con los lineamientos definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI).

Realizar periódicamente ejercicios de simulación de ciberataques con el propósito de evaluar la respuesta de los Equipos de Respuesta a Incidentes (IRT) y la resiliencia de los sistemas e infraestructura de la entidad ante incidentes de seguridad digital o cibernéticos. Asimismo, llevar a cabo ejercicios de mesas de crisis con simulaciones diseñadas para preparar a la entidad para enfrentar situaciones de emergencia o crisis, evaluando y mejorando la capacidad de respuesta y coordinación en todos los niveles estratégicos, tácticos y operacionales de la entidad.

Las siguientes son algunas herramientas y recursos para la gestión de incidentes por parte de las entidades/organizaciones.

Comunicaciones e Instalaciones: establecer un árbol telefónico con los miembros del equipo, lideres de proceso y entidades externas como el CSIRT Sectorial y el COLCERT, entre otros, para el apoyo y gestión. Este árbol debe incluir los datos de contacto básicos.

Mecanismos de reporte de incidentes: establecer un punto único de contacto para el reporte de eventos, habilitar buzones de correo, formulario en línea, números telefónicos y sistemas de mensajería instantánea.

Sala de crisis: Contar con un sitio para realizar reuniones y coordinaciones necesarias. Esta sala de crisis se utilizará para desarrollar las mesas estratégicas, táctica y operativas para

el abordaje integral de gestión de incidentes, con todos los líderes de proceso de la entidad/Organización.

Hardware y Software: Dotar de dispositivos para realizar respaldo para crear imágenes forenses, preservar archivos y log ´ s e información de los incidentes. Además, proporcionar computadoras portátiles con capacidad de procesamiento para análisis de datos e instalación herramientas especializadas en el manejo de la evidencia digital.

Recursos de análisis: Contar con Listados de puertos, diagramas de red, lista de activos de información y un inventario de la infraestructura tecnológica a recuperar. Este inventario debe incluir el detalle de las máquinas que soportan los sistemas de información, su ubicación, sus integraciones, sus mecanismos de autenticación y las observaciones necesarias para recuperar dichos servicios. También se debe disponer de documentación de sistemas operativos, aplicaciones, sistemas de información y herramientas de seguridad, así como procedimientos técnicos de recuperación de cada sistema de información.

Software de Mitigación de incidentes: construir y mantener un kit de herramientas especializadas para la investigación y análisis forense de incidentes. Además, mantener imágenes de sistemas operativos limpias y actualizadas para facilitar los procesos de restauración y recuperación operativa.

9.1.1. Acciones de prevención:

Realizar un ejercicio responsable de identificación de activos de información y gestión de riesgos, garantizará que los controles implementados sean lo suficientemente robustos para prevenir la materialización de riesgos.

Evaluación de riesgos: Realizar evaluaciones periódicas o cada vez que surjan cambios que puedan generar nuevos riesgos, a la matriz de riesgos de la entidad /organización, así como después de gestionar incidentes, para ajustar los controles de seguridad y minimizar los riesgos.

Seguridad de host: Gestionar vulnerabilidades para mantener los sistemas actualizados con las últimas actualizaciones de seguridad, habilitar la auditoria en los dispositivos y realizar un monitoreo constante para asegurar la visibilidad.

Seguridad de la Red: Bloquear y denegar cualquier actividad que no sea expresamente permitida, incluidas las VPN y conexiones dedicadas a otras entidades.

Prevención de Malware: Implementar software para detectar y detener malware en todos los equipos de cómputo, portátiles, servidores físicos y virtuales.

Sensibilización y formación de usuarios: Comunicar las políticas y procedimientos establecidos en el Modelo de Seguridad y Privacidad de la Información MSPI, y proporcionar información sobre los vectores de ataque identificados en incidentes previos.

9.2. Detección y Análisis

Los incidentes de seguridad pueden manifestarse de diversas formas, cada una requiriendo estrategias de respuesta específicas. Por ello, los Equipos de Respuesta a Incidentes (IRT) deben estar preparados para gestionar distintos escenarios, identificando y anticipando vectores de ataque comunes, tales como:

- Ataques desde medios extraíbles o periféricos.
- Fuerza bruta sobre credenciales.
- Correos electrónicos maliciosos.
- Suplantación de identidad.
- Uso indebido de la red institucional.
- Pérdida o robo de dispositivos.

La identificación y gestión adecuada de estos vectores es clave para garantizar una respuesta oportuna y eficaz ante los incidentes.

9.2.1. Identificación de incidentes

Para detectar y evaluar con precisión si ha ocurrido un incidente y conocer los niveles de detalle, se pueden utilizar diversas herramientas y soluciones, es así como la detección automatizada, soluciones de antivirus, correlaciones de eventos. Asimismo, los incidentes pueden ser detectados manualmente y comunicados por los usuarios a través de la mesa de servicios. Estas múltiples vías de detección permiten una evaluación más completa y precisa de los incidentes de seguridad.

Los signos de un incidente se dividen en Precursores e Indicadores, un precursor es una señal de que puede ocurrir un incidente en el futuro, mientras que un indicador es una señal de que un incidente pude haber ocurrido o puede estar desarrollándose.

Así las cosas, en muchos ataques no se evidencian precursores, ya que no siempre se conoce el objetivo del atacante. Sin embargo, algunos ejemplos de precursores pueden incluir:

- Logs del servidor web que muestran el uso de un escáner de vulnerabilidades.
- Anuncio de un nuevo "exploit" que puede ser explotado en un servidor de la entidad/organización.
- Amenaza de un grupo o actor de amenaza que anuncia un ataque.

Estos precursores pueden servir como alertas tempranas para preparar y reforzar las defensas contra posibles incidentes. Los indicadores son más fáciles de detectar. Algunos ejemplos incluyen:

- El software antivirus alerta cuando detecta que un equipo está infectado con malware.
- Una aplicación registra múltiples intentos fallidos de inicio de sesión.
- Un administrador de red evidencia una desviación de tráfico.

Por lo tanto, es esencial identificar las fuentes de precursores e indicadores en la infraestructura tecnológica. Estas fuentes pueden incluir:

- Firewall.
- Antivirus.
- NOC/SOC (Centro de Operaciones de Red/Centro de Operaciones de Seguridad).
- SIEM (Gestión de Información y Eventos de Seguridad).
- CVE (Common Vulnerabilities and Exposures).
- Registros e información pública disponible.
- Identificar y monitorear estas fuentes permite una detección temprana y una respuesta más efectiva a los incidentes de seguridad.

9.2.2. Análisis

Realizar un análisis inicial que proporcione suficiente información es crucial para que el IRT pueda priorizar actividades de contención y erradicación. Sin embargo, algunos incidentes no son fáciles de detectar debido a los signos mínimos que presentan. Por esta razón, es necesario trabajar en equipo con el personal técnico y de seguridad de la información para validar y tomar acciones necesarias para contener un incidente.

Una vez analizados los precursores e indicadores de manera eficientes y efectiva, el IRT debe realizar rápidamente un análisis detallado, identificando la ocurrencia de un incidente de seguridad de la información y seguridad digital, determinar el alcance de este, estableciendo que activos de información fueron afectados, cuál fue el vector de ataque y qué vulnerabilidades fueron explotadas. Esta información permitirá realizar acciones prioritarias de contención.

Las siguientes son recomendaciones para realizar análisis y validaciones iniciales.

- Perfiles de redes y sistemas: establecer una línea base de operación para detectar cambios fácilmente.

- Conocer los comportamientos normales: Comprender el comportamiento normal de redes, sistemas y aplicaciones, lo cual permitirá detectar actividades anormales.

- Crear políticas de retención de registros - Log ´ s: implementar una política de

- retención de registros - log ´ s de Firewall, IPS, servidores, aplicaciones bases de datos. Esta política debe especificar la duración de la retención de los datos con el propósito de:

    - Analizar las entradas de registros más antiguas, que pueden mostrar actividades de reconocimiento o ataques similares.

    - Revisar comportamientos y tácticas que los actores de amenaza utilizan antes de comprometer una infraestructura.

    - Realizar correlación de eventos: Para evidenciar un incidente, se debe revisar integralmente los eventos generados por las diferentes herramientas, sistemas y aplicaciones. Sin embargo, para hacerlo de manera constante, se recomienda utilizar herramientas de correlación de eventos (SIEM), las cuales proporcionan visibilidad completa de la infraestructura.

    - Mantener actualizados los relojes en todos los dispositivos y sistemas: para realizar una correcta correlación de eventos tanto manual como automatizada, es necesario que todos los componentes de la infraestructura estén sincronizados con servidores de hora (NTP). Esto puede hacerse utilizando equipos on-premise o servicios públicos, como los del Instituto Nacional de Metrología de Colombia (INM), a través de los dominios: ntp1.inm.gov.co y ntp2.inm.gov.co.

    - Instale analizadores de tráfico: Para realizar análisis de tráfico y complementar la información de precursores e indicadores, es fundamental contar con herramientas especializadas que monitoricen y analicen el tráfico de red. Esto permitirá una detección más precisa y una respuesta efectiva ante posibles accidentes de seguridad.

9.2.3. Documentación del incidente.

Una vez el IRT, identifique la ocurrencia de un incidente, debe comenzar a registrar todos los hechos y actividades realizadas en cada una de las fases el procedimiento

de gestión de incidentes, llevando una marca de tiempo. Además, todos los informes técnicos generados a nivel interno como para las autoridades judiciales deben ser fechados y firmados por el responsable del IRT. Es fundamental documentar minuciosamente las actividades y acciones realizadas para la preservación de la evidencia digital.

9.2.4. Clasificación de Incidentes de seguridad de la información y seguridad digital

La taxonomía de clasificación para los incidentes de seguridad digital empleada por COLCERT, se alinea a la utilizada por el CSIRT Américas (https://csirtamericas.org/) y por homólogos globales para la clasificación de los incidentes de seguridad de la información y seguridad digital.

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
Contenido abusivo	Ataques destinados a dañar la imagen de la organización o utilizar sus recursos electrónicos para usos ilícitos (como publicidad, extorsión o ciberdelincuencia en general)	Spam	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje compartido.
		Delito de odio	Contenido difamatorio o discriminatorio. Ej: Ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos o grupos.
		Materiales de abuso/explotación sexual infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	Incidentes relacionados con actividades maliciosas, aplicaciones y archivos dañinos para obtener acceso no	Sistema infectado	Sistema infectado con malware. Ej: Sistema, computador, dispositivos móviles infectado con un rootkit
		Servidor C&C	Conexión con servidor de Comando y Control (C&C) mediante malware o sistemas infectados.

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
	autorizado al sistema para sustraer, exfiltrar, eliminar, modificar su información privada que pretenden acceder a sus datos u.	(Comando y Control)	
		Distribución de malware	Recurso usado para distribución de malware. Ej: Recurso de una organización empleado para distribuir malware.
		Configuración de malware	Recurso que aloje archivos de configuración de malware Ej: Ataque de webinjects para troyano.
Obtención de información	Incidentes relacionados con la identificación y recopilación de información de personas, infraestructura tecnológica y activos de información de una organización a través de técnicas no autorizadas con fines delictivos.	Escaneo de redes (scanning)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: Peticiones DNS, ICMP, SMTP y escaneo de puertos.
		Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
		Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: Mentiras, trucos, sobornos, amenazas.
Intento de intrusión	Incidentes relacionados con la utilización de técnicas que intentan atacar una infraestructura tecnológica o un activo de información aprovechándose de una vulnerabilidad para obtener el control y privilegios administrativos o de ejecución.	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: Desbordamiento de buffer, puertas traseras y cross site scripting (XSS).
		Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: Intentos de ruptura de contraseñas, ataque por fuerza bruta.
		Ataque desconocido	Ataque empleando exploit desconocido
Intrusión	Ataques que aprovechar las vulnerabilidades de diseño, funcionamiento o configuración de las	Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
		Compromiso de cuenta	Compromiso de un sistema empleando cuentas sin privilegios.

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
	diferentes tecnologías, para entrar de forma fraudulenta a los sistemas de una organización	sin privilegios	
		Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades del software. Ej: Inyección SQL y defacement.
		Robo	Intrusión física. Ej: acceso no autorizado a Centro de Procesamiento de Datos.
Disponibilidad	Interrupción de la capacidad de procesamiento y respuesta de los sistemas y redes para dejarlos inoperativos Acción premeditada para dañar un sistema, interrumpir un proceso, cambiar o borrar información.	DoS (Denegación de Servicio)	Ataque de denegación de servicio. Ej: Envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
		DDoS (Denegación Distribuida de Servicio)	Ataque de Denegación Distribuida de Servicio. Ej: Inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
		Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
		Sabotaje	Sabotaje físico. Ej: Cortes de cableados de equipos, desconexión de equipos o incendios provocados
		Interrupciones	Interrupciones por causas ajenas. Ej: Desastre natural.
Compromiso de Información	Incidentes relacionados con el acceso, filtraciones (confidencialidad), la modificación o el borrado (integridad) de información.	Acceso no autorizado a información	Acceso no autorizado a información. Ej: Robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
		Modificación no autorizada de información	Modificación no autorizada de información. Ej: Modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
			de datos mediante ransomware.
		Pérdida de datos	Pérdida de información Ej: Pérdida por fallo de disco duro o robo físico.
Fraude	Incidentes relacionados con la pérdida de bienes causada con intención fraudulenta o deshonesta en procura de un beneficio económico para sí mismo, para otra persona o empresa	Uso no autorizado de recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
		Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez
		Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
		Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	Incidentes relacionados con la identificación del grado de debilidad inherente en un sistema de hardware o software que permitan a un atacante realizar actividades no autorizadas a la misma organización o en contra de otra.	Criptografía débil	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: Servidores web susceptibles de ataques POODLE/FREAK.
		Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
		Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
		Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
		Sistema vulnerable	Sistema vulnerable.

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
			Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Incidentes no clasificados en la taxonomía existente o amenazas persistentes avanzadas	Incidente no clasificado	Incidentes que no se ajustan a la clasificación existente, actuando como indicador para la actualización de la clasificación.
		APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Tabla 6 Taxonomía clasificación de incidentes

9.2.5. Priorización del incidente

La gestión de los incidentes no debe realizarse por orden de llegada. Este proceso es uno de los más críticos y debe priorizarse teniendo en cuenta los siguientes factores:

Impacto funcional del incidente: Este corresponde a las afectaciones de la operatividad y funcionalidad actual de las aplicaciones y servicios a los usuarios, tanto interno como externos. También se deben considerar el probable impacto funcional futuro si el incidente no se contiene de inmediato.

Impacto de la Información comprometida: Una vez Identificada la afectación a las funcionalidades de los activos en términos de confidencialidad, integridad y disponibilidad, se debe evaluar si el incidente ha causado una filtración de información. Es importante determinar el impacto de esta filtración tanto en la entidad/organización como en terceros, y cómo afecta la misionalidad de la entidad. La evaluación debe considerar el rol de la entidad como responsable y encargado de la información comprometida.

Recuperabilidad del incidente: La magnitud del incidente y los activos de información afectados determinarán el tiempo y los recursos necesarios para la recuperación de las operaciones. En algunos casos, un incidente puede requerir muchos más recursos de los que la entidad tiene disponible. Priorización atención de Incidentes y Tiempos de Respuesta.

Para permitir una gestión y respuesta a los incidentes, se debe determinar el nivel de prioridad para la atención por parte del IRT. A continuación, se definen algunas

variables que pueden ser utilizadas para realizar una adecuada priorización de los incidentes.

9.2.6. Criterios de valoración del Nivel de Impacto

Nivel	Valor	Descripción
Muy Grave	• 1,00	• Afecta activos de información de criticidad Alta y de Infraestructura crítica cibernética y servicios esenciales. • Afecta las funcionalidades a más del 75% de los sistemas de la organización. • Afecta la operación y funcionalidad de más del 75% de los usuarios internos y externos: • Afecta interdependencia de las operaciones y servicios en más de un 75% a otras entidades/organizaciones. • Compromete la confidencialidad de la información y los datos de la entidad, con filtración de cualquier porcentaje de Información pública Clasificada, Información pública Reservada, Información semi-privada e Información Privada. • Provoca daños reputacionales muy elevados y cobertura continua en medios de comunicación nacionales.
Grave	• 0,75	• Afecta activos de información de criticidad Media. • Afecta las operaciones y funcionalidades de más del 50% de los sistemas de la organización. • Afecta la operación y funcionalidad de más del 50% de usuarios internos y externos. • Afecta interdependencia de las operaciones y servicios en más del 50% de otras entidades/organizaciones. • Afecta a un servicio esencial. • Provoca daños reputacionales de difícil reparación, con amplia cobertura mediática y afectando la reputación de terceros. .
Menos Grave	• 0,50	• Afecta activos de información identificados de criticidad Baja. • Afecta las operaciones y funcionalidades de más del 25% de los sistemas de la organización. • Afecta la operación y funcionalidad de más del 25% de usuarios internos y externos. • Afecta interdependencia de las operaciones y servicios en más de un 25% a otras entidades/organizaciones.

Nivel	Valor	Descripción
		• Provoca daños reputacionales a menor escala, con mínima cobertura mediática y sin afectación a la reputación de terceros. .
Menor	• 0,25	• Afecta las operaciones y funcionalidades de los sistemas de la organización con interrupciones. • Afecta la operación y funcionalidad de hasta el 10% de usuarios internos. • Provoca daños reputacionales mínimo y puntuales, sin repercusión mediática en medios de comunicación
Sin Impacto	• 0.00	• No hay ningún impacto que afecte las operaciones, funcionalidades y reputación a la entidad.

Tabla 7 Descripción categorías de impacto función y de compromisos de información

9.2.7. Criterios de valoración del nivel de recuperabilidad - urgencia del Incidente

La Tabla 17, establece los criterios y categorías frente a los recursos y tiempo de recuperación de las operaciones.

Nivel	Valor	Descripción
Muy Grave	• 1,00	• Recuperación de las funcionalidades y operaciones de los activos afectados es superior a 24 horas. • La recuperación requiere recursos adiciones y ayuda externa.
Grave	• 0,75	• Recuperación de las funcionalidades y operaciones de los activos afectados es superior a 8 horas. • La recuperación requiere recursos adiciones.
Menos Grave	• 0,50	• Recuperación de las funcionalidades y operaciones de los activos afectados superior a 1 hora. • La recuperación se realiza con recursos propios.
Menor	• 0,25	• Recuperación de las funcionalidades y operaciones de los activos afectados superior a 15 minutos. • La recuperación se realiza utilizando mínimos recursos.

Tabla 8 Descripción de categorías de impacto de recuperabilidad de las operaciones

Luego de tener definidas las variables de impacto funcional actual, impacto funcional futuro y urgencia se obtiene la prioridad aplicando la siguiente formula:

Nivel de Prioridad = (Impacto funcional actual * 2) + (Impacto funcional futuro * 2) + (Urgencia * 4).

Impacto funcional actual: Se refiere al impacto actual del incidente, tomando en cuenta la afectación a los sistemas, usuarios, funcionalidades, interdependencia y reputación según los criterios establecidos en la Tabla 2.

Impacto funcional futuro: Se refiere al potencial impacto que podría tener el incidente si no se gestiona adecuadamente, evaluando la posible evolución y consecuencias adicionales, según los criterios establecidos en la Tabla 2.

Urgencia: Se refiere a la rapidez con la que debe ser resuelto el incidente, basada en la criticidad de la situación y los tiempos de respuesta necesarios, según los criterios establecidos en la Tabla 3.

Esta fórmula permite calcular una prioridad equilibrada considerando tanto el impacto inmediato como el potencial futuro del incidente, además de la urgencia de la respuesta necesaria.

Nivel de Prioridad	Nivel de Prioridad
Muy Grave	6,01 -8,00
Grave	4,01 – 6,00
Menos Grave	2,01 – 4,00
Menor	00,00 – 2,00

Tabla 9 Descripción de escalas de nivel de prioridad de atención de incidentes

9.2.8. Tiempos de Respuesta

Para la atención de incidentes, se han definido tiempos máximos de respuesta según la prioridad asignada, con el fin de asegurar una gestión oportuna y permitir la ejecución de acciones de contención, erradicación y recuperación. Estos tiempos aplican tanto al Equipo de Respuesta a Incidentes (IRT) como a las dependencias involucradas, conforme a sus responsabilidades.

Los plazos establecidos en la Tabla siguiente representan el tiempo máximo estimado para actuar según el nivel de criticidad del incidente. El IRT tiene a su cargo orientar, coordinar y supervisar la respuesta, garantizando que las dependencias cuenten con lineamientos y recursos para una gestión eficaz. Así, se asegura una atención proporcional al impacto del incidente sobre la seguridad de la organización.

Es importante aclarar que el tiempo de recuperación de las operaciones, varía dependiendo el impacto y los recursos disponibles, así las cosas, cada entidad está en la libertad de definir tiempos de atención a los incidentes como crean conveniente y dependiendo el nivel de criticidad de los activos impactados, los recursos disponibles, lo establecido en sus planes DRP Y BCP.

Nivel de Prioridad	Tiempo de Respuesta

Muy Grave	20 Minutos
Grave	45 Minutos
Menos Grave	1 Hora
Menor	2 Horas

Tabla 10 Descripción Tiempos Máximos de Atención de Incidentes por parte del IRT

9.3. Contención, Erradicación y Recuperación

Es fundamental para la entidad/organización diseñar estrategias que permitan tomar decisiones oportunas para evitar la propagación del incidente, acceso no autorizado, compromisos de otros sistemas y reducir el impacto en nivel la confidencialidad, integridad y disponibilidad de la información, así como los recursos tecnológicos.

Apagar un sistema, desconectar dispositivos de la red o desactivar funcionalidades son decisiones que pueden contemplarse en la estrategia a seguir durante el proceso de contención, con el objetivo de limitar el alcance y la afectación del incidente.

En este sentido, las estrategias y procedimientos establecidos para contener los diversos tipos de incidentes permiten facilitar la toma de decisiones y la implementación de acciones con mayor celeridad.

Los siguientes son algunos criterios que pueden ser adoptados para definir las estrategias de contención:

- Posibles daños y afectaciones.
- Necesidad de preservación de evidencia digital.
- Disponibilidad del servicio, interdependencia interna y externa.
- Tiempo y recursos necesarios para implementar la estrategia.
- Eficacia de la estrategia, determinando si la contención es parcial o total.
- Duración de la solución, evaluando si las acciones solucionar el incidente de manera parcial, temporal o total, si la solución es permanente o se eliminará después de un tiempo determinado.

9.3.1. Recopilación y preservación de evidencia

En paralelo con la gestión del incidente, se debe llevar a cabo una investigación de análisis forense para recopilar y preservar las evidencias, las cuales serán entregadas a las autoridades judiciales competentes (Fiscalía General de la Nación – Unidades de Policía Judicial). Es crucial documentar detalladamente como se han recolectado y preservado todas las evidencias para asegurar su admisibilidad en un proceso judicial. Por lo tanto, siempre que se transfiera la evidencia de una persona a otra, se debe diligenciar los formularios de cadena de custodia, que deben estar firmados por cada parte involucradas en el proceso.

Para la obtención de imágenes forenses, es recomendable que estás sean obtenidas antes de que los administradores de sistemas realicen cualquier actividad en el activo comprometido, utilizando las herramientas forenses recomendadas por la comunidad técnico-científica y documentando el proceso de acuerdo con los lineamientos establecidos por COLCERT para el manejo de la evidencia digital

Identificación de equipos atacantes: los IRT, deben centrar todas su acciones y actividades en la contención, erradicación y recuperación. Identificar un host atacante o paciente cero, puede ser un proceso que requiere mucho tiempo y, a veces, resulta inútil, impidiendo que el equipo minimice le impacto del incidente.

9.3.2. Erradicación y Recuperación

Una vez contenido el incidente, puede ser necesario realizar la erradicación para eliminar cualquier rastro dejado por el incidente y la amenaza a la infraestructura tecnológica, esto incluye eliminar el malware, deshabilitar cuentas comprometidas e identificar y mitigar las vulnerabilidades explotadas. Es crucial identificar todos los hosts y dispositivos afectados para llevar a cabo procesos de remediación y sanitización.

En algunos casos los incidentes, la erradicación se lleva a cabo durante la recuperación o simplemente no se realiza.

9.3.3. Recuperación

Los administradores de plataforma, sistemas, e infraestructura, deben restaurar el funcionamiento normal validando con las áreas funcionales la correcta operación. Así mismo, deben corregir las vulnerabilidades explotadas. Las restauraciones se pueden realizar a partir de copias de seguridad limpias, reconstruyendo sistemas y aplicaciones desde cero, reemplazando archivos comprometidos con versiones limpias, instalando parches de seguridad, renovación contraseñas, inactivando

usuarios con y sin perfiles de administrador, y ajustando las políticas en los equipos de seguridad perimetral.

En esta fase, es importante monitorear la infraestructura tecnológica para tener visibilidad, detectar precursores e indicadores y evitar futuros ataques.

En casos de incidentes clasificados como muy graves y grave la recuperación puede llevar meses, por esta razón, las estrategias de detección y las acciones de erradicación y recuperación deben estar orientadas a realizar cambios y ajustes rápidos, para evitar incidentes futuros.

Teniendo en cuenta los ajustes a la matriz de riesgos, los controles y ajustes a la postura de seguridad, deben realizarse a mediano y largo plazo, manteniendo las operaciones y la continuidad del negocio.

10. Actividades posteriores al Incidente.

10.1. Lecciones aprendidas.

La gestión de incidentes debe ser una oportunidad de aprendizaje y mejora para toda la entidad. Tanto el Equipo de Respuesta a Incidentes (IRT) como cada dependencia involucrada deben aprender de cada evento, independientemente de su gravedad. Por ello, es fundamental realizar reuniones de lecciones aprendidas con todas las partes involucradas, especialmente en incidentes clasificados como graves o muy graves. Para los de menor impacto, se recomienda programar espacios periódicos de revisión que fortalezcan la mejora continua.

Estas reuniones tienen como propósito no solo fortalecer la capacidad técnica del IRT, sino también mejorar las competencias de cada dependencia en la gestión de incidentes. En estos espacios se deben ajustar la matriz de activos y riesgos, mejorar controles, validar la eficacia de las acciones tomadas y revisar el procedimiento general.

Además, permiten formalizar el cierre del incidente, identificar a las partes interesadas y fortalecer la madurez institucional en seguridad de la información. Así, cada dependencia asume su rol en la gestión de incidentes y aporta activamente a la resiliencia organizacional.

Esta revisión permite establecer:

- ¿Qué pasó exactamente y en qué momentos?
- ¿Qué tan bien desempeñó el personal y la alta dirección en el abordaje del incidente?
- ¿Se siguieron los procedimientos y fueron adecuados?
- ¿Qué información se debía tener con antelación?

- ¿Qué acciones correctivas pueden prevenir incidentes similares en el futuro?
- ¿Qué precursores e indicadores se deben vigilar en el futuro para detectar incidentes?
- ¿Qué ajustes se deben realizar a la matriz de riesgos y qué controles deben ser ajustados e implementados para evitar futuros incidentes?
- ¿Qué herramientas o recursos adicionales se necesitan para detectar, analizar y mitigar incidentes futuros?

Igualmente, los temas abordados en las reuniones de lecciones aprendidas sirven como insumos para desarrollar campañas de concientización en seguridad de la información y seguridad digital y a capacitar a nuevos integrantes de los IRT. Asimismo, permite realizar ajustes a las políticas y procedimientos de gestión de incidentes.

En esta fase, se debe complementar los informes técnicos y de gestión del incidente, los cuales servirán como base de conocimiento para afrontar incidentes futuros.

10.2. Uso de datos e información recopilados del incidente.

Los datos permiten realizar una revisión a los riesgos y controles para realizar los ajustes correspondientes y fortalecer la postura de seguridad tanto a nivel del IRT como de las dependencias responsables de la gestión de incidentes.

Asimismo, los datos ayudan a establecer las capacidades y los recursos desplegados en la gestión del incidente, permitiendo identificar necesidades para justificar inversiones tanto en el IRT como en el fortalecimiento de las capacidades dentro de cada dependencia, asegurando que cuenten con los medios adecuados para responder de manera efectiva a los incidentes de seguridad de la información según su ámbito de responsabilidad.

Los datos obtenidos en la gestión de incidentes permiten cumplir con las obligaciones de reporte definidas en la **Resolución 500 de 2021 del MinTIC**. En particular, los incidentes clasificados como *Menos Grave* y *Menor* deben ser reportados al **Equipo COLCERT**, una vez gestionados, a través del siguiente enlace: https://www.colcert.gov.co/800/w3-article-198656.html#formulario_i__form_ReporteIncidentes_1.

Por su parte, los incidentes que involucren **datos personales** deben ser reportados a la **Superintendencia de Industria y Comercio (SIC)**, de conformidad con la normatividad vigente en protección de datos.

La recopilación estructurada de esta información facilita la clasificación y análisis de los incidentes, y permite identificar cómo las amenazas impactan los procesos institucionales.

Además, estos datos son clave para:

- Cumplir con los requisitos formales de notificación.
- Generar retorno de inversión en ciberseguridad.
- Detectar tendencias, nuevas amenazas y posibles vulnerabilidades.

Entre las métricas sugeridas para el monitoreo y mejora continua se encuentran:

- Número de incidentes gestionados.
- Tiempo total dedicado a su gestión.
- Tiempo de respuesta inicial del IRT.

Tiempo de notificación a la alta dirección y al CSIRT Gobierno/COLCERT

10.2.1. Evaluación Objetiva:

Busca determinar qué tan efectivas fueron las acciones y actividades desarrolladas por el IRT.

- Identificar los precursores e indicadores del incidente.
- Determinar si se identificó la causa raíz y el vector de ataque, las vulnerabilidades explotadas, y las características de la infraestructura afectada.
- Determinar si el incidente es producto de un incidente anterior.
- Medir la diferencia entre la evaluación de impacto inicial e impacto final.
- Identificar medidas y controles que se podrían haber implementados para evitar el incidente.

10.2.2. Evaluación Subjetiva:

Busca evaluar el desempeño de cada miembro del IRT y de las personas que intervinieron en cada una de las fases de la gestión del incidente, así como validar con el propietario del activo afectado si el incidente se gestionó de manera eficiente.

Igualmente, las entidades/organizaciones pueden realizar auditorías al procedimiento de gestión y respuesta a incidentes.

10.3. Retención de pruebas:

Para la retención de evidencia digital, la entidad/organización puede establecer un protocolo, en el cual indique que las evidencias preservadas se mantendrán resguardadas por el representante legal en un lugar seguro y que después de recolectadas y embaladas dentro del proceso de cadena de custodia (Manual cadena de custodia Fiscalía https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf) y entregadas a las autoridades judiciales (CTI de la Fiscalía y Delitos Informáticos de la DIJIN), estas se mantendrán en custodia durante tres (3) meses contados a partir de la entrega.

Sin embargo y entendiendo las capacidades disponibles para el restablecimiento de los servicios afectados, la entidad puede ajustar estos tiempos, en virtud de la recuperación las operaciones.

10.4. Lista de verificación para la gestión de incidentes.

Los siguientes son los principales pasos para seguir en la gestión del incidente, sin embargo, estos pueden variar según el tipo y naturaleza de incidentes a gestionar.

Item	Acción	Terminado
	Detección y Análisis	
1	Determinar si ha ocurrido un incidente	
1.1	Analizar los precursores e indicadores	
1.2	Buscar información de diferentes fuentes y correlacionarla	
1.3	Realizar investigación en motores de búsqueda y base de conocimientos	
1.4	Documentar el incidente, las actividades de investigación y la recolección de evidencias.	
2	Priorizar el incidente según los criterios de Impacto funcional, de información afectada y recuperabilidad.	
3	Informar el incidente internamente y al COLCERT/CSIRT Gobierno	
	Contención Erradicación y Recuperación	
4	Adquirir, preservar, proteger y documentar	
5	Contener el incidente	
6	Erradicar la amenaza	
6.1	Identificar y mitigar todas las vulnerabilidades que fueron explotadas	
6.2	Eliminar el malware, sanitizar equipos y dispositivos.	
7	Recuperación del incidente	
7.1	Restablecer los sistemas afectados y restablecer los servicios.	
7.2	Confirmar con los funcionales de los aplicativos y sistemas el funcionamiento de estos.	

7.3	Implementar seguimientos adicionales en búsqueda de afectaciones sin restablecer.	
	Actividad Posteriores	
8	Elaborar un informe de seguimiento de las gestiones y actividades de investigación realizadas	
9	Realizar reunión de lecciones aprendidas obligatorias para incidentes muy graves y graves.	

Tabla 11 Pasos para seguir en la gestión del incidente

11. Recomendaciones Generales

- Adquirir herramientas y soluciones que puedan apoyar la gestión de los incidentes.
- Identificar precursores e indicadores a través de alertas generadas por equipos de seguridad.
- Solicitar registros y eventos de todos los sistemas a un nivel básico.
- Perfilar redes y sistemas.
- Entender los comportamientos normales de las redes, sistemas y aplicaciones.
- Realizar correlación de eventos.
- Mantenga sincronizados todos los relojes de equipos y dispositivos.
- Mantener y utilizar una base de conocimiento de información de incidentes.
- Registrar todas las informaciones una vez se identifique un incidente.
- Preservar las evidencias.
- Priorizar la gestión de los incidentes según el resultado del análisis.
- Divulgar el procedimiento de gestión de incidentes del COLCERT/CSIRT Gobierno.
- Establecer estrategias y procedimientos de contención.
- Capture datos volátiles de los sistemas y equipos como evidencia.
- Celebrar reuniones de lecciones aprendidas.

12. Coordinación e intercambio de información.

Las entidades/organizaciones deben trabajar conjuntamente durante la gestión de los incidentes. Se debe realizar una coordinación con las múltiples partes interesadas para el intercambio de información sobre amenazas, vulnerabilidades y ataques (Indicadores de Compromiso (IoC)- Indicadores de Ataque -(IoA) para que sea validada y ajustada la postura de seguridad.

Para el intercambio de información se deben establecer los canales de comunicación con los proveedores de servicios onpremise y nube, infraestructura tecnológica, PRST, cadenas de suministro, autoridades y el CISRT Gobierno/COLCERT, para reportar los incidentes y solicitar los apoyos y coordinar las acciones en cada una de las fases de la gestión de incidentes.

Con el propósito de recibir apoyo y coordinación en la gestión de los incidentes catalogados como muy graves y graves, estos deben ser reportados al COLCERT/CSIRT Gobierno, por los canales de comunicación establecidos como son contacto@colcert.gov.co – csirtgob@mintic.gov.co.

Los incidentes catalogados como Menos Grave y Menor deben ser reportados al COLCERT/CSIRT Gobierno en el formulario establecido una vez sea gestionado. El cual se encuentra publicado en la siguiente URL https://www.colcert.gov.co/800/w3-article-198656.html#formulario_i__form_ReporteIncidentes_1, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.

La información de los incidentes debe ser protegida por el IRT, a través de accesos a los repositorios de manera restringida y controlada.

13. Lineamientos a considerar.

A continuación, se detallan lineamientos para ser considerados por las entidades:

Lineamiento Sugerido	Acciones Claves
- Los incidentes de seguridad relacionados con proveedores y terceros, como los servicios en la nube, deben ser abordados en los planes de respuesta, incluyendo cláusulas contractuales para notificación, gestión y mitigación oportuna, conforme al control A.5.19 de la ISO/IEC 27001:2022	- Actualizar los planes de respuesta a incidentes incluyendo procedimientos documentados y roles definidos para análisis, respuesta, recuperación y mejora continua.
- Los incidentes relacionados con datos personales deberán ser tratados	Definir protocolos de actuación diferenciados para incidentes que

conforme a la Ley 1581 de 2012 y las disposiciones de la ISO/IEC 27701, incluyendo la notificación oportuna a los titulares afectados y a la autoridad competente	involucren datos personales, incluyendo notificación a la SIC y a los titulares afectados.
- Se deben establecer procedimientos para la comunicación de incidentes relevantes a las partes interesadas, incluyendo notificación a autoridades regulatorias, terceros afectados y entes de control, según la criticidad del incidente y el tipo de información comprometida	Desarrollar una política de notificación de incidentes críticos con plazos, responsables y medios de comunicación hacia entes de control y ciudadanía.
- La entidad deberá articular su proceso de respuesta a incidentes con el CSIRT Gobierno, y cuando aplique, con otros CSIRT sectoriales o institucionales, a través de canales de reporte, protocolos de escalamiento y mecanismos de coordinación establecidos.	Incluir en el plan de respuesta procedimientos de escalamiento y cooperación con CSIRT Gobierno, incluyendo contacto permanente, roles compartidos y trazabilidad de casos.
Incluir la gestión de incidentes relacionados con proveedores o terceros, en especial en la cadena de suministro y servicios en la nube (control A.5.19).	Establecer cláusulas contractuales con proveedores que contemplen notificación, mitigación y reporte de incidentes; definir mecanismos de coordinación y seguimiento.

Tabla 12 Lineamientos a considerar

14. Referencias.

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August 6). Computer Security Incident Handling Guide. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

- Computer Security Incident Handling Guide. (2012, August 6). https://doi.org/10.6028/NIST.SP.800-61r2

- CSIRT Services Framework Version 2.1. (2019, November). https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

- FIRST - Improving Security Together. (2015, January 1). https://www.first.org/

- Incident management. (2022, May 31). https://www.wikiwand.com/en/Incident_response

- National Institute of Standards and Technology This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29 February 26, 2024 The NIST Cybersecurity Framework (CSF) 2.0. (2024, February 29). NIST, 2.0. https://doi.org/https://doi.org/10.6028/NIST.CSWP.29

- Prácticas recomendadas y tutoriales de gestión de incidentes. (2023, January 1). https://www.atlassian.com/es/incident-management

- Publications. (2023, February 6). https://csrc.nist.gov/publications

- Ruefle, R., Dorofee, A., Mundie, D A., Householder, A D., Murray, M., & Perl, S J. (2014, September 1). Computer Security Incident Response Team Development and Evolution. https://doi.org/10.1109/msp.2014.89

- Şeker, E., & Ozbenli, H H. (2018, June 1). The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. https://doi.org/10.1109/cybersecpods.2018.8560673

TIC

Lineamientos Relación con Proveedores de Tecnologías de la Información y las Comunicaciones

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de contenido

Tabla de contenido 186

Lineamientos Relación con Proveedores de Tecnologías de la Información y las Comunicaciones 187

1. Planificación de las relaciones con Proveedores. 188
2. Selección de proveedores. 191
3. Negociación de Acuerdos con Proveedores. 194
4. Gestión de relaciones con proveedores. 197
5. Proceso de terminación de la relación con el proveedor. 199

Listado de Tablas

Tabla 1 Lineamientos a considerar 202

Lineamientos Relación con Proveedores de Tecnologías de la Información y las Comunicaciones

Las entidades estatales del orden nacional y territorial deben establecer relaciones con proveedores para adquirir productos y servicios. Cuando estas adquisiciones están vinculadas a la gestión de la seguridad digital, es común que los proveedores tengan acceso directo o indirecto a los sistemas de información y a los datos institucionales, o que suministren componentes (software, hardware, procesos o personal) que intervienen en el procesamiento de dicha información.

Asimismo, durante el control o seguimiento de los procesos de producción y entrega, las entidades pueden acceder física o lógicamente a información de los proveedores. Esta interacción bilateral implica que ambas partes pueden representar riesgos mutuos en materia de seguridad digital.

Por ello, estos riesgos deben ser identificados, evaluados y gestionados adecuadamente mediante la implementación de controles proporcionales a la criticidad de la información tratada. Este anexo ofrece una guía con los aspectos clave para tener en cuenta en las relaciones contractuales con proveedores de productos y servicios de seguridad digital.

Los riesgos se acentúan cuando el proveedor carece de una adecuada gestión de seguridad de la información, particularmente en el caso de proveedores TIC que:

- Desarrollan aplicaciones o administran sistemas que tratan datos institucionales.

- Prestan servicios de infraestructura tecnológica que almacenan o procesan información crítica.

- Tienen conocimiento de elementos sensibles como configuraciones, vulnerabilidades, logs, direccionamiento interno, entre otros, asociados a procesos misionales de la entidad.

Ante este escenario, es indispensable que la entidad:

- Identifique claramente la información a la que pueden acceder los proveedores.

- Determine las operaciones autorizadas sobre dicha información.

- Establezca los controles necesarios para protegerla, incluyendo cláusulas contractuales como acuerdos de confidencialidad, sanciones por incumplimientos e indemnizaciones por negligencia comprobada.

En paralelo, el proveedor debe asumir responsabilidades específicas, tales como:

- Cumplir con los requisitos en materia de seguridad de la información y protección de datos personales.

- Notificar de manera inmediata cualquier incidente o brecha de seguridad que afecte los activos de información de la entidad.

- Colaborar activamente en la gestión, mitigación y análisis de los incidentes que involucren los activos de información gestionados.

Cuando se prevea la transferencia o acceso a la información fuera del país, la entidad debe gestionar los riesgos transfronterizos, asegurando que tanto proveedores nacionales como internacionales cumplan con las normas vigentes en seguridad digital y protección de datos.

La entidad debe tener plena conciencia de que la responsabilidad legal y contractual sobre la información permanece en todo momento bajo su control, incluso cuando un proveedor la administre. Por lo tanto, debe verificar que los controles aplicados por terceros estén alineados con su plan de tratamiento de riesgos, incluyendo los escenarios de cambio de proveedor o interoperabilidad entre tecnologías de distintos fabricantes.

Estas disposiciones deben estar documentadas en el plan de tratamiento de riesgos y reflejarse explícitamente en los acuerdos contractuales, garantizando así la trazabilidad y la responsabilidad compartida en la gestión de la seguridad de la información.

1. Planificación de las relaciones con Proveedores.

Para gestionar adecuadamente la seguridad de la información en las relaciones con proveedores, las entidades establecer un plan de relación que documente la decisión adoptada por el nivel directivo de iniciar la contratación de un producto o servicio relacionado con activos de información, así como las consideraciones de seguridad de la información relacionadas con esta contratación.

Lineamiento:	Establecer un plan de relación con proveedores que documente la decisión adoptada por el nivel directivo de iniciar la contratación de un producto o servicio relacionado con activos de información, así como las consideraciones de seguridad de la información relacionadas con esta contratación incluyendo la evaluación de seguridad de los proveedores y la gestión de riesgos asociados a servicios o sistemas de terceros.
Propósito:	Gestionar con éxito la seguridad de la información dentro del proceso de planeación de la relación con los proveedores de productos o servicios de seguridad de la información.

Entradas recomendadas	Salidas
• Decisión de adquisición de un producto o servicio relacionado con activos de información documentando necesidades, expectativas y motivos del proceso de adquisición. • Alcance previsto del producto o servicio que se prevé adquirir. • Si es aplicable: o Documentación existente de gestión de relaciones con proveedores, como planes y acuerdos de relaciones con proveedores.	I) Plan de evaluación y tratamiento de riesgos de seguridad de la información asociados al producto o servicio que se contrate; II) Decisión de gestión documentada que indica la aprobación del plan de evaluación y tratamiento de riesgos de seguridad de la información y que se puede iniciar la adquisición del producto o servicio; III) La decisión de no adquirir un producto o servicio también deberá documentarse con la información de las razones de seguridad que han inducido esta decisión. IV) Plan de relación con proveedores. V) Cuando aplique: análisis de impacto si se presenta un cambio en el acuerdo inicial que afecte la continuidad de negocio.

Actividades a realizar por parte de la entidad contratante:

Identificar y evaluar los riesgos de seguridad de la información que acompañan la posible adquisición del producto o servicio con base en el MSPI y en la estrategia de relación con proveedores.

- Las entidades deberán garantizar que esta evaluación de riesgos de seguridad de la información:

1) Es proporcional a la criticidad del producto o servicio que se planea adquirir.

2) Tiene en cuenta los requisitos legales y regulatorios aplicables a el producto o servicio que se planea adquirir para garantizar que se hayan obtenido los permisos y licencias formales antes de iniciar la relación con el proveedor.

3) En particular al adquirir productos de nube que durante su operación puedan resultar en tratamiento o transferencia de datos personales resulta fundamental planear dónde se

almacenarán los datos, el tipo de almacenamiento y la región geográfica de ese almacenamiento.

4) Se debe tener cuidado y considerar los posibles impactos en la seguridad de la información del producto o servicio que se adquirirá con respecto a los riesgos de seguridad de la información asociados con las relaciones existentes con los proveedores, particularmente si existe una alta dependencia de los proveedores. Para disminuir la complejidad y facilitar los procesos de gestión de Seguridad Digital se recomienda adoptar buenas prácticas en materia de consolidación de proveedores.

- Identificar el nivel aceptable de riesgos en la relación con el potencial proveedor;

- Identificar y evaluar opciones para el tratamiento de los riesgos identificados y evaluados;

- Definir e implementar un plan de tratamiento de riesgos de seguridad de la información para que los riesgos identificados y evaluados sean mitigados al nivel de riesgo aceptable;

  NOTA: No se debe proceder con la adquisición de los bienes o servicios cuando los riesgos de seguridad de la información identificados no puedan reducirse a un nivel aceptable de riesgos.

- Asesorar a la entidad sobre el plan de evaluación y tratamiento de riesgos de seguridad de la información como insumo para el proceso de negociación de la relación con proveedores;

- Definir un plan de relación con proveedores del producto o servicio que se prevé adquirir. En particular, el plan de relación con proveedores deberá contener lo siguiente:

  1) Especificaciones del producto o servicio que se prevé contratar, en particular su alcance, audiencia, tipo y naturaleza;

  2) Activos, tales como servidores, bases de datos, aplicaciones, infraestructura de red, que tengan relevancia para la seguridad de la información en el uso del producto o servicio, y sus propietarios asociados;

  3) Entradas de clasificación de información de la entidad, la clasificación de información del proveedor y otros controles de seguridad de la información;

  4) Los requisitos legales y regulatorios aplicables a la entidad, y las áreas de leyes y reglamentos que vinculan al proveedor potencial que deben revisarse durante el proceso de selección de proveedores, a saber:

  I) Control de exportaciones;

  II) Legislación de protección de datos personales y leyes laborales; en particular las previstas en la Ley 1581 de 2012, la CIRCULAR EXTERNA 10 de 2001 -Circular única Superintendencia de Industria y Comercio -SIC, y demás normatividad aplicable.

III) propiedad intelectual de terceros; y

IV) Otros requisitos legales y reglamentarios, como leyes fiscales, responsabilidad por productos defectuosos, facultades de investigación.

Si se requieren autorizaciones o licencias de autoridades internas o externas para el cumplimiento legal y reglamentario, estas deberán obtenerse antes de celebrar cualquier acuerdo de relación de proveedor con el proveedor.

5) Roles y responsabilidades de seguridad de la información asignados dentro de la entidad y específicos del producto o servicio que se puede adquirir;

6) Información de la entidad que se puede compartir con posibles proveedores del producto o servicio.

NOTA: La información del adquirente debe tener un propietario designado, responsable de su difusión y de garantizar que las reglas de manejo relacionadas se apliquen correctamente.

7) Requisitos mínimos de seguridad de la información que se acordarán con el proveedor seleccionado para la adquisición del producto o servicio. Estos requisitos deben resultar directamente del plan de evaluación y tratamiento de riesgos de seguridad de la información y del marco de requisitos de seguridad de la información definido en la estrategia de relación con el proveedor.
Estos requisitos también deben definirse considerando la criticidad del producto o servicio que se puede adquirir y lo siguiente:

- Clasificación de la información hecha por la entidad;

- Los requisitos de seguridad de la información definidos en los planes de relación con proveedores existentes y acuerdos.

- Realizar un proceso de articulación del entorno de red que contemple los elementos físicos, virtuales y en la nube y la interacción entre ellos.

2. Selección de proveedores.

Para gestionar con éxito la seguridad de la información dentro del proceso de selección de proveedores, las entidades deben establecer los controles de seguridad de la información específicos para cada producto o servicio de seguridad digital a adquirir de acuerdo con la criticidad de la información que van a tratar y así seleccionar un proveedor que brinde la seguridad de la información requerida.

Lineamiento:	Planificar la selección de los proveedores de productos o servicios de seguridad de la información.
Propósito:	Gestionar con éxito la seguridad de la información dentro del proceso de selección de proveedores de productos o servicios de seguridad de la información.

Entradas recomendadas	Salidas
• Criterios de seguridad para la selección de proveedores existentes para otros productos y servicios. • Acuerdos de confidencialidad existentes para otros productos o servicios. • Identificación de la información y los activos de información de la entidad a la que tendrá acceso: el proveedor, las herramientas y sistemas de información del proveedor.	VI) Nuevos criterios de seguridad para la selección de proveedores específicos para los productos o servicios a adquirir. VII) Acuerdos de confidencialidad específicos para los productos o servicios a adquirir. VIII) Permisos que tendrá el proveedor sobre la información y los activos identificados. IX) Análisis de riesgos de seguridad de la información incluyendo los riesgos asociados a posibles migraciones de datos entre diferentes proveedores y la interoperabilidad entre herramientas y servicios de diferentes fabricantes. X) Resultados de la evaluación del cumplimiento de los requisitos de seguridad de la información de los proveedores. XI) Plan de evaluación y tratamiento de riesgos de seguridad de la información asociados al producto o servicio que será suministrado este plan debe ser realizado por parte del proveedor seleccionado.

Actividades a realizar por parte de la entidad contratante:

Definir e implementar criterios de selección de proveedores que contenga especificaciones del producto o servicio que se puede contratar y en el marco de criterios de selección de proveedores definido; Los criterios de selección de proveedores cubrirán lo siguiente:

- Aceptación por parte del proveedor de los requisitos de seguridad de la información definidos en el pliego de condiciones;

- La madurez en seguridad de la información del proveedor podrá demostrarse mediante certificación ISO/IEC 27001:2022 o, en su defecto, a través de documentación técnica que evidencie controles implementados, tales como planes de continuidad, recuperación, gestión de incidentes y políticas internas. Esta flexibilidad busca asegurar condiciones mínimas de seguridad sin afectar la pluralidad de oferentes en procesos de contratación.

- Los términos bajo los cuales el proveedor permite ser auditado por la entidad o por un tercero autorizado para verificar el cumplimiento de los requisitos de seguridad de la información definidos;

- Aceptación transitoria cuando el producto o servicio a contratar haya sido previamente explotado o fabricado por la entidad o por otro proveedor;

- Aceptación de terminación para mantener la seguridad de la información en caso de terminación del contrato de relación con el proveedor;

- Gestión de la capacidad del proveedor para suministrar el producto o servicio que pueda contratar,

- Fortaleza financiera del proveedor que puede suministrar el producto o servicio; y la ubicación del proveedor y desde donde se suministrará el producto o servicio. Se debe tener especial cuidado para identificar esta ubicación con el fin de:

    - Identificar cualquier riesgo legal y regulatorio potencial causado por la diferencia en las leyes y regulaciones entre la entidad y el proveedor. NOTA: Es necesario realizar investigaciones relacionadas con la legislación extranjera en el caso de contratación interjurisdiccional.

    - Garantizar que las obligaciones legales y reglamentarias que se aplican al proveedor no puede afectar negativamente el acuerdo de relación con el proveedor en términos de seguridad de la información.

    - Evaluar las amenazas ambientales, como las tasas de criminalidad locales o los problemas geopolíticos, y sus impactos potenciales.

  NOTA: Los criterios de selección de proveedores existentes definidos para otros productos o servicios adquiridos también se pueden utilizar al definir e implementar los criterios de selección de proveedores del producto o servicio que se puede suministrar.

Preparar un acuerdo de confidencialidad para ser firmado por el proveedor para proteger los activos de la entidad, como información y sistemas de información. transmitidos durante el proceso de selección de proveedores. NOTA: Si corresponde, este acuerdo de confidencialidad debe ser firmado por la entidad y el proveedor potencial antes de cualquier intercambio de información que se relacione con el producto o servicio que se pueda contratar.

NOTA: Los acuerdos de confidencialidad existentes deben utilizarse como soporte para la elaboración del acuerdo de confidencialidad del producto o servicio que se vaya a adquirir.

Preparar y proporcionar un documento de licitación, al proveedor potencial; El documento debe contener información suficiente para que el proveedor pueda preparar su propuesta con fundamento. En particular, el pliego de condiciones deberá contener lo siguiente:

1) Especificaciones (p. ej., alcance, audiencia, tipo y naturaleza) del producto o servicio a adquirir;

2) Requisitos de seguridad de la información que el proveedor deberá seguir mientras suministre el producto o servicio;

3) Niveles de servicio o indicadores clave de desempeño a seguir durante el suministro del producto o servicio; Las posibles sanciones que puede imponer la entidad en caso de incumplimiento de los requisitos de seguridad de la información.

NOTA: En la medida de lo posible, el pliego de condiciones solo debe contener contenido público o desclasificado. Dicho documento solo debe contener la información necesaria para permitir que el proveedor responda justifica mente.

La información altamente sensible nunca debe incluirse en un documento de licitación en ninguna circunstancia.

Se deben recopilar los documentos de respuesta que han sido transmitidos por proveedores potenciales en respuesta al documento de licitación y estos deben ser evaluados con base a los criterios de selección de proveedores.

e) Seleccionar un proveedor basado en la evaluación de estos documentos de respuesta.

NOTA: Las entidades deben propender por seleccionar a los proveedores que proporcionan una mayor transparencia en toda la cadena de suministro de productos o servicios y garantías de que los requisitos de seguridad de la información de la entidad se cumplirán de acuerdo con lo definido en el pliego de condiciones.

3. Negociación de Acuerdos con Proveedores.

Con el objetivo de mantener la Seguridad de la información durante la negociación de los acuerdos con proveedores las entidades deberán mantener la seguridad de la información durante el período de ejecución de la relación con el proveedor de acuerdo con el contrato con el proveedor y considerando en particular lo siguiente: I) Evaluar el impacto del cambio

en el suministro del producto o servicio cuando haya sido previamente operado o fabricado por la entidad o por un proveedor diferente; II) Capacitar al personal involucrado en los requisitos de seguridad de la información definidos en el contrato con el proveedor; III) Gestionar cambios e incidentes que puedan tener impactos en la seguridad de la información en el suministro del producto o servicio; IV) Supervisar y asegurar el cumplimiento de las disposiciones de seguridad de la información definidas en el contrato con el proveedor.

Lineamiento:	Gestionar la seguridad de la información en el proceso en el proceso de negociación de acuerdos con proveedores.
Propósito:	Gestionar con éxito la seguridad de la información dentro del proceso de negociación de la relación con los proveedores de productos o servicios de seguridad de la información.

Entradas recomendadas	Salidas
• Decisión sobre quién llevará a cabo las actividades de supervisión del proveedor; • Resultados anteriores de las actividades de seguimiento y cumplimiento de los proveedores.	XII) Evaluación de riesgos de seguridad de la información e informes de auditoría relacionados con las actividades de supervisión y ejecución del cumplimiento. Cuando aplique: XIII) Evaluación de riesgos de seguridad de la información relacionada con cambios que no están cubiertos por el procedimiento de gestión de cambios de seguridad de la información; XIV) Informe de ejecución del plan de migración; XV) Historial de cambios de seguridad de la información e informes asociados; XVI) Historial de incidentes de seguridad de la información e informes asociados; XVII) Acuerdo de relación con proveedores actualizado; XVIII) Lista de acciones correctivas que se han acordado y el estado actual (por ejemplo, abierto, retirado o implementado).

Actividades a realizar por parte de la entidad contratante:

- Asegurarse de que la otra parte haya recibido el documento de relación con el proveedor y de que comprenda completamente los aspectos de seguridad de la información contenidos en el mismo;

- Exigir al proveedor el cumplimiento de las políticas de seguridad y privacidad de la información y de continuidad del negocio de la entidad, para el tratamiento de la información y los activos a los que tenga acceso.

- Operar la transición del producto o servicio de acuerdo con el plan de transición acordado y notificar a la otra parte de manera oportuna en caso de que ocurran eventos inesperados durante esta actividad;

- Gestionar los cambios e incidentes de seguridad de la información de acuerdo con los procedimientos acordados;

- Solicitar la autorización para poder realizar auditorías al proveedor, con el fin de verificar el cumplimiento a las Políticas de Seguridad de la Información.

- Capacitar periódicamente al personal que pueda estar involucrado en la ejecución del plan de terminación;

- Gestionar otros cambios, como los que no estén amparados por el procedimiento de gestión de cambios de seguridad de la información y que puedan impactar en el suministro del producto o servicio contratado, cuando sean notificados por la otra parte:

    - Cambio en el negocio, la misión o el entorno de la organización;

    - Cambio relacionado con la solidez financiera de la organización;

    - Cambio de propiedad de la organización, o creación de joint ventures;

    - cambio de ubicación desde donde se adquiere o suministra el producto o servicio;

    - Cambio en el nivel de seguridad de la información de la organización, como el logro o la pérdida de una certificación ISO/IEC 27001:2022;

    - Cambio en la capacidad de soportar las capacidades requeridas de continuidad del negocio; y

    - Cambio en los requisitos legales, regulatorios y contractuales aplicables a la organización.

- Asegurarse de que las actividades de monitoreo y supervisión cumplan con el plan asociado y el proceso de manejo de acciones correctivas. En caso de que ocurran cambios en los riesgos de seguridad de la información o de no conformidades de auditoría, la entidad con el apoyo del proveedor deberá:

    identificar y evaluar los impactos en la seguridad de la información resultantes de estos cambios o auditar las no conformidades;

Determinar si se deben reconsiderar los aspectos de seguridad de la información definidos en el contrato con el proveedor;

Determinar qué acciones correctivas se deben implementar dentro de una escala de tiempo definida y acordada para recuperar un nivel aceptable de seguridad de la información dentro del alcance del producto o servicio adquirido;

- Acordar con el proveedor:
    - Los cambios por realizar en los aspectos de seguridad de la información definidos en el contrato con el proveedor;
    - Medidas correctivas aplicables
- Aprobar el contrato con el proveedor.

4. Gestión de relaciones con proveedores.

Con el objetivo de mantener la seguridad de la información es necesario contar con una apropiada gestión de los proveedores, para ello debe ser considerado lo establecido en la Política de seguridad de la información en las relaciones con los proveedores y así mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización y mantener el relacionamiento acorde a lo establecido en los Acuerdos de Nivel de Servicio determinados.

Lineamiento:	Mantener la seguridad de la información durante el período de ejecución de la relación con el proveedor.
Propósito:	Gestionar con éxito la seguridad de la información durante la relación con el proveedor de productos o servicios de seguridad de la información**.**

Entradas recomendadas	Salidas
• Documento firmado que incluya cláusulas de cumplimiento al proveedor sobre las disposiciones de seguridad de la información, protocolos de migración, procedimientos de capacitación y plan de transición definidas por la organización, el cual debe mantener la reserva según los protocolos y normatividad existente.	XIX) Informes periódicos de los servicios o productos que evidencie el cumplimiento de los indicadores establecidos. XX) Evidencias de reuniones periódicas de seguimiento acorde a lo establecido en las cláusulas y según requerimiento del supervisor del contrato. XXI) Resultados de revisiones técnicas, administrativas o

	auditorias de cumplimiento en búsqueda de acciones de mejora o verificación del cumplimiento requerido

Actividades a realizar por parte de la entidad contratante:

Establecer las actividades que deben ser tenidas en cuenta por la entidad contratante, para la gestión de la prestación de los servicios o productos contratados, verificación de las responsabilidades y controles aplicables para dar alcance al objeto contractual, por lo cual se recomienda:

a) Asegurar que los documentos y pólizas estén se encuentren vigentes durante el periodo de ejecución, en caso de prorrogas estar atentos a las actualizaciones contractuales que den a lugar.

b) Realizar revisiones periódicas a los documentos, planes y procedimientos entregados por el proveedor, sobre los cuales basan la operación, para determinar la funcionalidad y/o necesidad de actualización o mejoras que permita ajustarse al proceso y políticas existentes de la entidad.

c) Evaluación de riesgos de seguridad de la información de forma periódica en acuerdo con el con el proveedor, para determinar posibles nuevas amenazas o vulnerabilidades en los productos o servicios contratados, los cuales como resultado deberán ser gestionados por el proveedor del servicio de acuerdo con los ANS establecidos en el contrato.

d) Adoptar los procedimientos del proveedor según corresponda, a los procesos existentes en la entidad, para así alinear las estrategias de continuidad del negocio entre las partes.

e) Verificar la ejecución del plan de capacitación y realizar las mediciones sobre la efectividad y nivel de apropiación de los conocimientos de los asistentes.

f) Ejecutar pruebas de verificación sobre los planes de continuidad del servicio, recuperación y gestión de incidentes.

g) Contar con un plan de gestión de cambios que permita tener control y trazabilidad de las acciones realizadas por el proveedor.

h) Establecer un plan terminación que incluya entre documentación para la transición, métodos de intercambio de datos, reglas o registros (si aplica), que permita un proceso transparente en el caso que no sea posible o adecuada la continuidad con el proveedor.

i) Contar con la bitácora de eventos relevantes que se presenten durante el desarrollo del contrato, ya que serán determinantes en la generación de los procesos de lecciones aprendidas al finalizar el relacionamiento con el proveedor.

j) Contar con un repositorio único en el cual se cuente con la información de la ejecución contractual tales como registros, documentos, procedimientos, manuales, listados y en general todos aquellos que sean considerados como elementos de valor o evidencias durante la ejecución contractual.

k) Realizar un monitoreo de las actividades y acciones de los servicios en la nube

5. Proceso de terminación de la relación con el proveedor.

La finalidad en todos los casos es proteger la confidencialidad, integridad y disponibilidad de la información, por ello, dar por terminado el relacionamiento contractual debe ser transparente y preciso para la organización, evitando traumatismo y materialización de eventos adversos en el proceso durante el cierre y entrega a un nuevo proveedor o a la entidad, para todos los casos, es imperante que el servicio o producto siempre este funcional según corresponda, para así evitar impactos operacionales, legales o económicos.

Es preciso tener presente los tiempos, documentos y elementos requeridos para el cierre, con base en lo establecido en los términos contractuales y la normatividad vigente.

Lineamiento:	Planificar el cierre contractual con los proveedores de productos o servicios de seguridad de la información.
Propósito:	Gestionar con éxito y de manera segura la terminación de la relación con el proveedor de productos o servicios de seguridad de la información garantizando la continuidad de la operación.

Entradas recomendadas	Salidas
• Contar con un plan de migración o de terminación avalado y probado para la entrega de los productos o servicios de seguridad de la información a la entidad o al proveedor entrante. • Documento con la evaluación de los riesgos existentes en los procesos de entrega o migración de los servicios o productos de seguridad de la información.	XXII) Acta de finalización del contrato avalada y firmada por el supervisor, en el cual certifica el cierre de la relación contractual. XXIII) Informe de lecciones aprendidas durante el tiempo del servicio y en el cierre del contrato.

• Activación del plan de continuidad del negocio, verificación de controles existentes y respaldo de información o dispositivos según corresponda.	

Actividades a realizar por parte de la entidad contratante:

Establecer las actividades a realizar para la finalización contractual con el proveedor de productos o servicios de seguridad de la información, para ello, es importante establecer y contar con un plan de terminación que contemple diversas actividades con el objetivo de mantener la continuidad en la operación para ello es necesario:

a) Describir las actividades y procedimientos generales para tener en cuenta durante el cierre y posterior a la finalización del servicio sin que se incurran en costos adicionales para las partes.

b) Establecer un comité técnico entre las partes, el cual tendrá como función coordinar las actividades de cierre de los servicios contratados acorde al plan de finalización.

c) Contar con la previa evaluación de riesgos y cronograma de ejecución correspondiente para la terminación contractual teniendo en cuenta los eventos adversos que pueden presentarse, la forma de mitigarlos y las desviaciones que puedan reflejarse en el cronograma por la materialización de las amenazas.

Nota: en caso tal que el servicio deba ser entregado de un proveedor a otro, debe ser conformado un comité técnico el cual estará compuesto por las partes incluyendo personal del proveedor saliente y entrante.

d) Durante el proceso de entrega, el proveedor deberá relacionar documentación técnica, bitácoras de procedimientos, registros actualizados, y en general toda la información que sea parte integral y de relevancia sobre las labores adelantadas durante la ejecución contractual.

Nota: de acuerdo con el servicio deberán ser requeridos en la entrega como mínimo:

- Documentación técnica del diseño y de la operación.
- Archivos de Imágenes de máquinas virtuales.
- Archivos de bases de datos.
- Archivos de bases de datos de administración de configuraciones (CMDB).
- Archivos que se encuentren dispuestos en los servicios de almacenamiento contratado.

- Toda aquella documentación sobre topologías o estructuras físicas o lógicas.

e) Solicitar apoyo al proveedor o al comité técnico durante el proceso de cierre contractual para la coordinación de los despliegues técnicos, y operativos que sean necesarios para verificar, probar, trasladar y ejecutar la entrega o migración de los productos o servicios de seguridad de la información.

Nota: La entidad compradora generará un acta que contenga la relación de los procedimientos realizados, documentación de configuraciones, parámetros y procedimientos sobre los servicios o productos de seguridad de la información entregados por el proveedor.

f) Solicitar certificación al proveedor la cual indicara la eliminación total y segura de los datos almacenados con herramientas especializadas que no permitan la recuperación o reúso.

g) Acta de finalización del proceso contractual avalada y firmada por el supervisor, en el cual certifica el cierre del proceso contractual.

h) Verificar el cambio de credenciales de acceso, eliminación de usuarios y cierre de conexiones remotas al proveedor saliente.

6. Lineamientos adicionales a considerar

A continuación, se detallan los siguientes lineamientos a considerar:

Lineamiento Sugerido	Acciones Claves
- Los contratos con proveedores deberán contemplar cláusulas específicas sobre la gestión de amenazas (control A.5.7) y seguridad en la nube (A.5.23), incluyendo requerimientos sobre evaluación de amenazas emergentes, responsabilidad compartida, trazabilidad, cifrado y protección de datos en servicios cloud.	- Incluir cláusulas contractuales que exijan al proveedor identificar, reportar y mitigar amenazas relevantes. - Solicitar evidencias de controles en la nube: cifrado, gestión de accesos, respaldo, monitoreo. - Establecer acuerdos de nivel de servicio (SLA) específicos en seguridad.
- La entidad debe identificar y evaluar los riesgos asociados a sus proveedores críticos, considerando elementos como la cadena de suministro, el manejo de información	- Elaborar una matriz de riesgos de proveedores: criticidad del servicio, sensibilidad de los datos, dependencia tecnológica.

sensible, y la continuidad del servicio. Se deben establecer mecanismos de evaluación inicial y periódica del cumplimiento en seguridad.	- Clasificar a los proveedores según su nivel de riesgo. - Establecer revisiones de cumplimiento en seguridad al menos una vez al año.
- Se deberán establecer protocolos de reporte y coordinación con proveedores frente a incidentes de seguridad, incluyendo tiempos de notificación, medidas de contención y responsabilidad en la remediación. Estas condiciones deberán estar formalizadas en los contratos.	- Definir en contrato el tiempo de notificación de incidentes por parte del proveedor (ej. 4 horas). - Acordar el procedimiento conjunto para análisis, contención y remediación. - Documentar responsabilidades compartidas para incidentes multientidad.
- En la contratación de servicios en la nube, se deberá considerar la ubicación geográfica del proveedor y del almacenamiento de datos, verificando que las condiciones contractuales y técnicas cumplan con las leyes nacionales y estándares de protección de datos. Se debe definir claramente el modelo de responsabilidad compartida.	- Identificar la ubicación física de los centros de datos donde se almacenan los datos institucionales. - Verificar cumplimiento de leyes colombianas (protección de datos, soberanía). - Establecer el modelo de responsabilidad compartida entre entidad y proveedor (p. ej., gestión de accesos: proveedor, contenido: entidad).
- Para activos de información compartidos o administrados por terceros, se deberán establecer lineamientos específicos que aseguren su identificación, clasificación, control de acceso, trazabilidad y eliminación segura. Estos lineamientos deberán aplicarse desde la etapa de contratación.	- Identificar activos tercerizados en el inventario (p. ej., bases de datos alojadas en proveedores). - Establecer controles de acceso, monitoreo y eliminación segura de información tercerizada. - Exigir reportes periódicos del estado de estos activos.
- La gestión de la seguridad de la información en relación con los proveedores debe abordarse de forma integral, incluyendo requisitos contractuales, evaluación de riesgos, participación en la gestión de incidentes, cumplimiento normativo y medidas técnicas específicas según el tipo de servicio prestado o el acceso a activos de información.	- Incorporar requisitos de seguridad en los términos de referencia, evaluaciones y contratos. - Incluir a los proveedores en pruebas de continuidad del negocio y simulacros de ciberseguridad. - Asegurar trazabilidad de accesos de proveedores a sistemas internos.

Tabla 13 Lineamientos a considerar

TIC

Lineamientos de seguridad de la información para el uso de servicios en la nube

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de contenido

Tabla de contenido 205
Lineamientos de seguridad de la información para el uso de servicios en la nube 208
1. Derechos de autor 208
2. Alcance 208
3. Introducción 208
3.1. Conceptos previos 208
3.2. Características de los servicios en la nube 209
3.3. Modelos de despliegues 221
3.3.1. Nube privada (Private cloud) 221
3.3.2. Nube comunitaria (Community cloud) 222
3.3.3. Nube pública (Public cloud) 222
3.3.4. Nube híbrida (Hybrid cloud) 223
3.4. Categorías o modelos de servicios 224
3.4.1. Software como Servicio (Software as a Service – SaaS) 225
3.4.2. Plataforma como Servicio (Platform as a Service – PaaS) 227
3.4.3. Infraestructura como Servicio (Infrastructure as a Service – IaaS) 228
3.5. Beneficios ir a la nube 229
a) Reducción de costos de operación. 229
b) Escalabilidad. 230
c) Reducción de costos de obsolescencia tecnológica 230
d) Acceso a tecnología de punta. 230
e) Rápida recuperación ante desastres y fallos. 230
f) Transferencia y reducción de riesgos técnicos 230
g) Entrega rápida y flexible 231
h) Permite concentrar esfuerzos en la misión y objetivos de la entidad 231
4. Seguridad y privacidad en la nube 231
4.1. Seguridad digtal y riesgos específicos del cloud 232
4.1.1. CSP y Algunos ejemplos 234
4.1.2. Vulnerabilidades: CVE y CVSS 234
4.1.3. Responsabilidad compartida (CSP y Cliente) 235
4.1.4. Autenticación y autorización (IAM) 236
4.1.5. MFA o Multi Factor Authentication 236

4.1.6. AK/SK, Access Key y Secret Key 237
4.1.7. Políticas (policies) 237
4.1.8. Usuarios, grupos y roles 238
4.1.9. IDP o Identity Providers 239
4.1.10. Criptografía 240
4.1.11. Secrets Manager 241
5. Computación en la nube en Colombia 242
6. Pasos fundamentales para dar el salto a la nube 243
6.2. Aprovisionamiento de servicios 244
6.3. Migración y Portabilidad 244
6.4. Escalonamiento 245
6.5. Definición De La Seguridad y Privacidad 245
6.6. Gestión de incidentes 245
6.7. Gestión de Cambios 246
6.8. Asuntos legales relacionados con la residencia física de los datos. 246
6.9. Servicio totalmente dependiente de una conexión a internet 247
6.10. Planes de continuidad del negocio (BCP) y recuperación de desastres (DR). 247
6.11. Acuerdos de Nivel de servicio (ANS). 247
6.12. Reputación y solvencia del proveedor de servicios 248
6.13. Cláusulas de derechos de proveedores y limitación de responsabilidad 248
6.14. Seguridad 248
6.15. Privacidad 249
7. Gobernanza de la Nube 249
7.1. Importancia de la gobernanza en la nube 250
7.2. Principios del modelo de gobernanza de la nube 251
7.3. Como se diseña e implementa un marco de gobernanza en la nube 251
8. Formato de auto diagnóstico como actor de la nube 254
9. Lineamientos específicos para la gestión de seguridad en la nube 255
10. Implementación y monitoreo de controles de seguridad en servicios en la nube 256
11. Referencias 257

Listado de Tablas

Tabla 1 Actividades del consumidor y proveedor de la nube 214

Tabla de ilustraciones

Ilustración 1 Modelo de referencia Conceptual – NIST.....212
Ilustración 2 Servicios disponibles para los consumidores.....213
Ilustración 3 Actividades principales de un Proveedor de la nube.....216
Ilustración 4 Proveedor de nube – Orquestación del Servicio.....217
Ilustración 5 Proveedor de nube – Administración del servicio en la nube.....219
lustración 6 Nube privada en sitio.....221
Ilustración 7 Nube privada subcontratada.....221
Ilustración 8 Nube comunitaria en sitio.....222
Ilustración 9 Nube pública.....223
Ilustración 10 Nube híbrida.....224
Ilustración 11 Modelos de servicios Cloud.....225
Ilustración 12 Capas de protección en el cloud para asegurar la información (datos).....233
Ilustración 13 Ejemplo de MFA físico modelo SafeNet IDProve 100 6-digit OTP Token.....237
Ilustración 14 Ejemplo Usuarios, grupos y roles.....239
Ilustración 15 Componentes de un marco de gobernanza de la nube.....266

Lineamientos de seguridad de la información para el uso de servicios en la nube

1. Derechos de autor

Para el desarrollo de este documento, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre por parte del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide), tomando como base los lineamientos recomendados en las Normas ISO/IEC 27017 e ISO IEC 27001 –2022.

2. Alcance

El presente documento, además de presentar definiciones sobre el modelo de computación en la nube, busca que las entidades del sector público puedan identificarse o clasificarse dentro de los actores y modelos de servicios de esta tendencia. Además, proporciona criterios y consideraciones que deben evaluarse y contemplarse al adquirir este tipo de servicios.

3. Introducción

3.1. Conceptos previos

En la actualidad el acceso a servicios a través de Internet se ha incrementado exponencialmente aunado a esto la pandemia del COVID-19 acelero el uso excesivo del internet como medio para apalancar sus negocios y obligando a la gran mayoría de las organizaciones a depender casi que un 100% de ella teniendo en cuenta el artículo publicado por **Data Center Market** (https://www.datacentermarket.es/tendencias-ti/el-90-de-las-empresas-ha-incrementado-el-uso-de-la-nube-por-la-pandemia/). Este hecho, así como la heterogeneidad de los dispositivos que dan acceso a estos servicios, ha supuesto un auge en el uso de las tecnologías web como un estándar.

La migración a entornos web, el uso de aplicaciones móviles y la introducción de dispositivos IoT han sido un catalizador para la externalización de los sistemas de información de un amplio número de organizaciones. Como consecuencia de esta situación surge el modelo de servicios en la nube, como una propuesta tecnológica capaz de ofrecer una gran cantidad de servicios en red de forma ágil y flexible, con grandes posibilidades de escalabilidad y reduciendo al mínimo los tiempos de despliegue.

Los servicios en la nube consisten en la disposición de software, plataformas o infraestructuras por parte de un proveedor (CSP, Cloud Servicie Provider) o por parte de la

propia entidad, accesibles en red, con independencia de donde se encuentren alojados los sistemas de información y de forma transparente para el usuario final.

Los sistemas “on premise” tradicionales ya no están tan aislados como en el pasado, presentando una mayor superficie de exposición y difuminando el perímetro de la red. El uso de la nube permite utilizar tecnologías diseñadas para responder a necesidades de externalización introduciendo arquitecturas y paradigmas de seguridad, por lo que son una alternativa segura para procesar y almacenar datos.

La provisión de servicios en la nube es un modelo que permite acceder por red a recursos de computación configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden suministrar y desplegar.

Este documento establece definiciones y criterios para identificar si una persona, natural o jurídica, pública o privada es proveedor de servicios de computación en la nube y presenta las consideraciones a tener en cuenta al contratar estos servicios. Además, ofrece un anexo para identificarse como actor dentro del ecosistema de computación en la nube y determinar si puede participar como proveedor de estos servicios.

Con el fin de proporcionar criterios y definiciones en referencia a la computación en la nube para Colombia, sus características, los modelos de servicios e implementación, beneficios y aspectos a considerar para proveer o adquirir servicios en la nube, el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC) desarrolla este documento y la pone a disposición de los interesados.

Es oportuno aclarar que este documento no es una norma o especificación técnica, es solo una orientación para facilitar la contratación de servicios de computación en la nube por parte de las entidades públicas y demás actores, así ofrecer criterios para determinar la adecuada clasificación de los proveedores de servicios en la nube.

3.2. Características de los servicios en la nube

La característica principal de la nube es la accesibilidad de la información. Este modelo, unido a la capacidad de despliegue automático de servicios en cuestión de segundos a nivel global, facilita el acceso a la información por parte de los usuarios, con independencia del lugar o el tipo de dispositivo que se emplee: basta tener acceso a la red, aunque el uso de este paradigma implica habitualmente la necesidad de disponer de conexiones con una capacidad significativa.

Otra de las características que hacen de la nube un área en expansión es el ahorro económico. Generalmente el modelo de servicios en la nube permite reducir costes a la organización con respecto al modelo de servicio y alojamiento tradicional. Esto es por el ahorro de recursos dedicados internamente a hardware, mantenimiento, personal dedicado, suministros, espacio e instalaciones, y por el uso de economías de escala en los servicios en la nube, donde cuanto mayor es necesario para proporcionar el servicio, menor coste de estos recursos.

Por otro lado, los servicios en la nube se caracterizan por la deslocalización de datos, donde la principal ventaja es que el cliente puede decidir la geolocalización de la información y permite llevar los datos y los procesos al lugar más conveniente para la organización, además de mantener el control de acceso estén donde estén los datos.

De esta forma se pueden mantener copias del servidor repartidas en distintos puntos del planeta tanto para mejorar los tiempos de acceso y reducir la latencia al mínimo, como para evitar pérdidas de datos o servicios por la caída de un centro de proceso, manteniendo alta disponibilidad y durabilidad. Esta deslocalización tiene implicaciones de seguridad que las organizaciones deben evaluar convenientemente antes de hacer uso de los servicios en la nube, como la aplicación de legislaciones regionales sobre los datos o la baja disponibilidad de la infraestructura de red en la región, y deben aplicar medidas de seguridad y configuraciones adecuadas a cada escenario.

Por consiguiente, es pertinente que existan normas regulatorias con orientaciones internacionales sobre el tema en cuestión.

Por ello, la Norma ISO/IEC 27017:2015 es un estándar que proporciona una serie de directrices para los controles de seguridad de la información que se aplican a los servicios en la nube teniendo en cuenta los siguientes puntos:

- Orientación adicional para los controles pertinentes especificados en la ISO/IEC 27002;
- Controles adicionales determinados con directrices que se relacionan específicamente a los servicios en la nube.

Además, esta norma también ofrece controles y orientaciones tanto para los clientes de los servicios como para el CSP, Por ejemplo, la sección 6.1.1, en la que se explican los roles y responsabilidades en la seguridad de la información, se han añadido, además de las indicaciones existentes en la sección 5.2 en la ISO/IEC 27002:2022, los siguientes aspectos:

Para el cliente de los servicios en la nube

El cliente de los servicios en la nube debe estar de acuerdo con el CSP de la asignación adecuada de los roles y responsabilidades en la seguridad de la información, y confirmar que pueda cumplir esa asignación. Los roles y responsabilidades en la seguridad de la información de ambas partes deben ser establecidos bajo un acuerdo común. El cliente de los servicios en la nube debe identificar y gestionar su relación con la parte de soporte del cliente y prestar atención a la función que desempeña el CSP.

Para el CSP En esta línea, recalcando los roles y responsabilidades en seguridad de la información se recoge lo siguiente:

El CSP debe redactar y concertar una adecuada asignación sobre los roles y responsabilidades en la seguridad de la información con su cliente, los otros CSPs y sus proveedores.

Se puede observar, evidentemente que, por un lado, la ISO/IEC 27017 ha completado la ISO/IEC 27002 con aspectos especializados en los asuntos sobre la seguridad de la información almacenada en la nube; por otro lado, aunque las responsabilidades están determinadas entre ambas partes (el cliente y el CSP), en realidad, el cliente es el responsable de la decisión sobre la utilización de los servicios en la nube. Esa decisión se debe tomar atendiendo a los roles y responsabilidades determinados por el CSP

Por otro lado hay que tener cuenta, para los servicios en la nube se identifican cinco (5) características

a) Esenciales según NIST:

- ✓ Autoservicio a demanda. El cliente puede ajustar la capacidad necesaria de forma unilateral, sin necesidad de involucrar al personal del proveedor.

- ✓ Amplio acceso a través de redes. Acceso estándar a través de redes, habilitando todo tipo de dispositivos de acceso: teléfonos, tabletas, portátiles, equipos personales, servidores, etc.

- ✓ Agregación y compartición de recursos. Los recursos del proveedor se agregan y se ponen a disposición de múltiples clientes para su compartición. La agregación incluye equipos físicos y equipos virtuales que se asignan dinámicamente bajo demanda. El cliente se independiza de la ubicación física de los recursos, aunque puede delimitar ubicaciones a un cierto nivel de abstracción (país, estado, etc.) y mantienen el control de acceso a sus recursos.

- ✓ Adaptación inmediata. La capacidad requerida puede provisionarse rápida y elásticamente para seguir las variaciones de la demanda. Desde el punto de vista del consumidor, los recursos parecen ilimitados, pudiendo disponer de cualquier volumen en cualquier momento.

- ✓ Servicio consumido. El proveedor puede controlar el servicio prestado efectivo en cada momento, al nivel de abstracción que se especifique por contrato; por ejemplo, capacidad de almacenamiento, capacidad de procesamiento, ancho de banda, cuentas de usuario, etc. El uso de recursos puede ser monitorizado, controlado y auditado, proporcionando una gran transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

Cabe destacar la posible dependencia de terceros en los servicios en la nube. La tendencia mayoritaria apunta hacia externalizar los servicios en la nube a terceros delegando en ellos todas las tareas de mantenimiento, adquisición de sistemas, gestión de la capacidad, etc.

Aunque se considera una ventaja, debe considerar que esta característica de externalización no debe conllevar una pérdida del control de la información o una despreocupación por la seguridad, ya que la responsabilidad final recae en el organismo contratante.

A la hora de contratar servicios en la nube es fundamental estudiar adecuadamente las condiciones del servicio y las medidas de seguridad aplicadas para confirmar que son adecuadas para los requisitos exigidos a la organización cliente, además de establecer medidas adecuadas de monitorización y vigilancia

b) Actores:

Los actores según NIST, representan los participantes dentro del modelo de computación en la nube. Un actor puede ser una entidad, una persona o parte de una organización, que participa en una transacción o proceso y realiza tareas dentro del modelo de computación en la nube. [4] [5]. Cabe aclarar que un mismo actor puede cumplir diferentes roles del modelo.

El siguiente diagrama representa una arquitectura de referencia de alto nivel y tiene por objeto facilitar la comprensión de los requisitos, usos, características y estándares de la computación en nube.

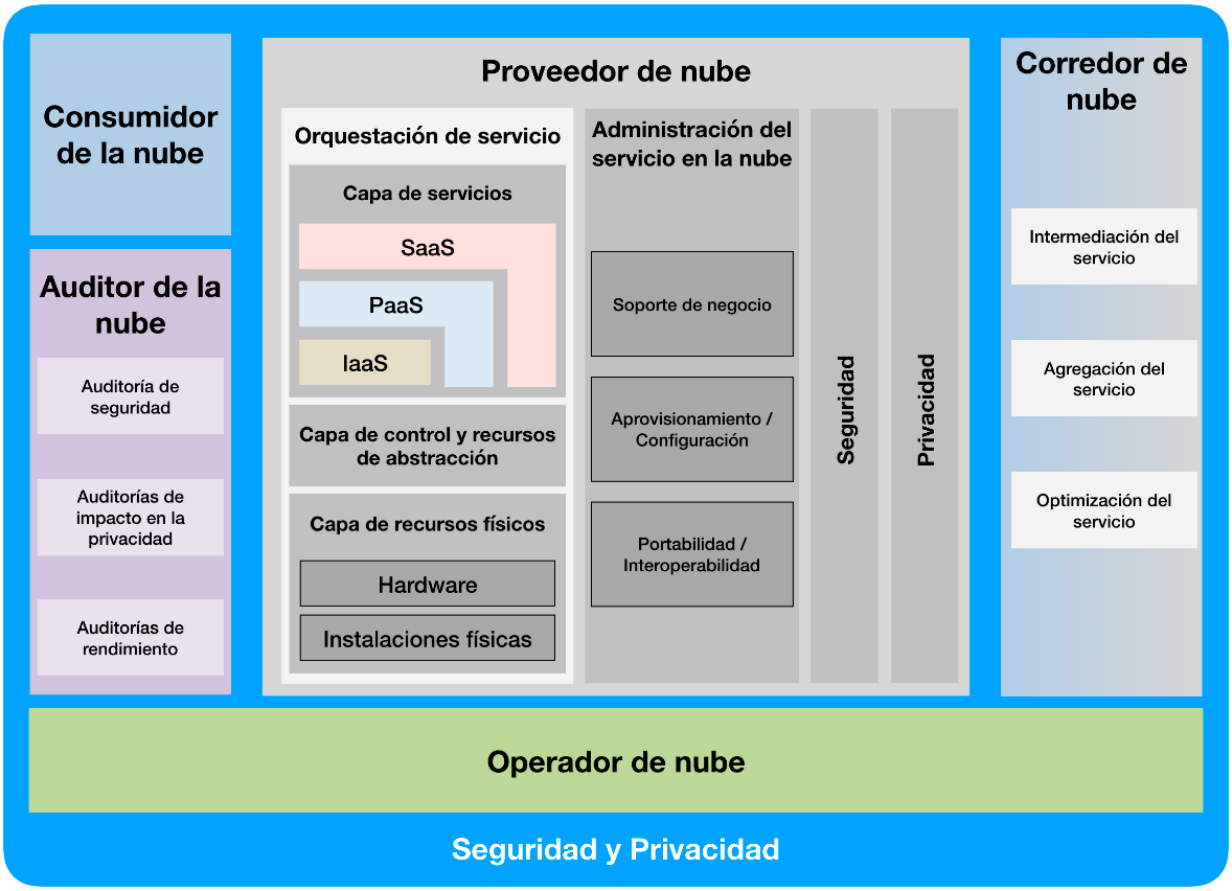


Ilustración 1 Modelo de referencia Conceptual – NIST

Como se muestra en la Figura 1, la arquitectura de referencia del NIST para la computación en nube define cinco actores principales: consumidor de nube, proveedor de nube, auditor de nube, corredor o agente de nube y operador de nube. Cada actor es una persona natural o jurídica que participa en una transacción o proceso y/o realiza tareas en la computación en la nube.

- ✓ Consumidor Una persona u organización que mantiene una relación comercial con un proveedor de servicios Cloud y utiliza el servicio. Los consumidores de la nube necesitan un SLA, es decir un acuerdo de nivel de servicio, para especificar los requerimientos de desempeño técnicos cumplidos por el proveedor de la nube. Un SLA puede cubrir términos relativos a la calidad del servicio, seguridad y soluciones por fallas. El proveedor de la nube también puede enumerar en los SLAs un conjunto de premisas explícitamente no hechas por los consumidores (por ejemplo, limitaciones y obligaciones que los consumidores de la nube deben aceptar).

La Ilustración 2 presenta algunos ejemplos de servicios disponibles para los consumidores de la nube.

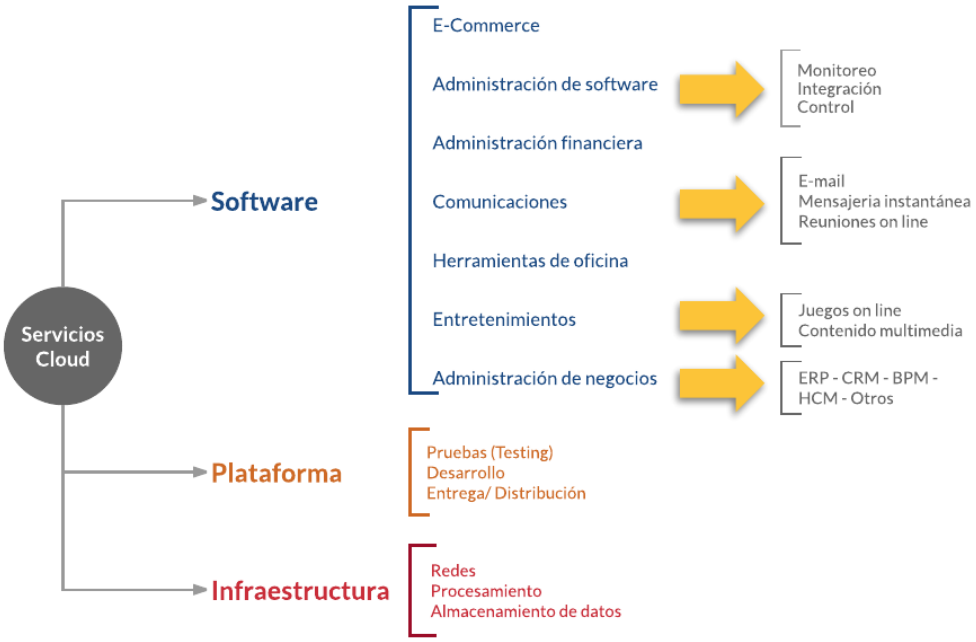


Ilustración 2 Servicios disponibles para los consumidores

Fuente: http://i.imgur.com/ItozCV2.png

- ✓ Proveedor Una persona, organización o entidad responsable de disponibilidad el servicio a las partes interesadas.

- ✓ Auditor Una parte que puede realizar una evaluación independiente de los servicios en la nube, de las operaciones del sistema de información, el rendimiento y la seguridad de las implementaciones en Cloud.

- ✓ Intermediario Una entidad que administra el uso, vela por el desempeño, por la entrega de servicios e intermedia en la relación entre los proveedores de servicios en Cloud y los consumidores finales.

- ✓ Operador Un intermediario que provee conectividad y transporte desde los proveedores de servicio hacia los consumidores.

- ✓ Operador Un intermediario que provee conectividad y transporte desde los proveedores de servicio hacia los consumidores.

La Tabla 1 enumera brevemente los actores definidos en la arquitectura de referencia de computación en la nube propuesta por el NIST [4][5].

Modelos de servicio	Actividades del Consumidor	Actividades del Proveedor
SaaS (Software como servicio)	Usa la aplicación o los servicios para soportar procesos de negocio.	Instala, administra, mantiene y soporta la aplicación de software en una infraestructura de nube.
PaaS (Plataforma como servicio)	Desarrolla, prueba (testing), despliega y administra aplicaciones alojadas en un sistema de nube (Cloud).	Gestiona la infraestructura de cómputo de la plataforma y ejecuta el software de nube que proporciona los componentes de la plataforma como las bases de datos y otros componentes de capa media para el intercambio
IaaS (Infraestructura como servicio)	Crea/instala, administra y monitorea lo servicios operacionales de la infraestructura de TI.	Ejecuta el software de la nube necesario para que los recursos informáticos estén disponibles para el consumidor de nube IaaS a través de un conjunto de interfaces de servicios y abstracciones de recursos de cómputo, como máquinas virtuales e interfaces de red virtual. El proveedor de nube IaaS tiene control sobre el software de nube que controla el hardware que hace posible el aprovisionamiento de

Tabla 1 Actividades del consumidor y proveedor de la nube

Las aplicaciones SaaS se hacen accesibles a través de una red (usualmente Internet) a los consumidores SaaS. Los consumidores de SaaS pueden ser organizaciones que proporcionan a sus miembros acceso a aplicaciones de software, usuarios finales que utilizan directamente aplicaciones de software o administradores de aplicaciones de software que configuran aplicaciones para usuarios finales.

Los consumidores de SaaS pueden ser facturados en función del número de usuarios finales, el tiempo de uso, el ancho de banda consumido en la red, la cantidad de datos almacenados, la duración de los datos almacenados, entre otros.

Los consumidores de PaaS pueden emplear las herramientas y recursos de ejecución proporcionados por los proveedores de nube para desarrollar, probar, implementar y administrar las aplicaciones alojadas en un entorno de computación en la nube.

Los consumidores de PaaS pueden ser desarrolladores de aplicaciones que diseñan e implementan software de aplicación, probadores de software que ejecutan y prueban aplicaciones en entornos basados en la nube, implementadores de aplicaciones que publican aplicaciones en la nube y administradores de aplicaciones que configuran y supervisan el rendimiento de aplicaciones en una plataforma. Los proveedores de PaaS pueden facturar según el procesamiento, el almacenamiento de la base de datos y los recursos de red consumidos por la aplicación PaaS, así como la duración del uso de la plataforma, entre otros.

Los consumidores de IaaS tienen acceso a computadoras virtuales, almacenamiento accesible en red, componentes de infraestructura de red y otros recursos informáticos fundamentales en los que pueden implementar y ejecutar software arbitrario. Los consumidores de IaaS pueden ser desarrolladores de sistemas, administradores de sistemas y administradores de TI que estén interesados en crear, instalar, administrar y monitorear servicios de gestión de infraestructura de TI.

Los consumidores Ias disponen de las capacidades para acceder a estos recursos informáticos y se les factura de acuerdo con la cantidad o duración de los recursos consumidos, como las horas de CPU utilizadas por los ordenadores virtuales, el volumen y la duración de los datos almacenados, el ancho de banda consumido, el número de direcciones IP usadas para ciertos intervalos, entre otros.

c) Actividades proveedor de nube

Un proveedor de servicios de computación en la nube (desde Colombia o desde el exterior), despliega, configura, mantiene y actualiza la operación de las aplicaciones de software en una infraestructura de nube (propia, compartida, o apoyada con otros proveedores) para que los servicios se aprovisionen en los niveles de servicio esperados para los consumidores de nube. El proveedor de SaaS asume la mayoría de las responsabilidades en la gestión y control de las aplicaciones y la infraestructura, mientras que los consumidores de la nube tienen un control administrativo limitado de las aplicaciones [4][5].
El proveedor de plataforma como servicio PaaS, gestiona la infraestructura de cómputo de la plataforma y ejecuta el software de nube que proporciona los componentes de la plataforma como las bases de datos y otros componentes de capa media para el intercambio de información (middleware). El proveedor de PaaS normalmente también soporta el proceso de desarrollo, despliegue y administración del consumidor de PaaS, proporcionando herramientas tales como entornos de desarrollo integrados (IDE), control de versiones en la nube, kits de desarrollo de software (SDK), herramientas de implementación y administración. El proveedor de PaaS no tiene control sobre las aplicaciones hospedadas (el control lo tiene el consumidor de SaaS), pero posiblemente si lo tiene sobre la configuración del entorno de hospedaje, así mismo, no tiene o tiene acceso limitado a la infraestructura subyacente de la plataforma, como la red, los servidores, los sistemas operativos o el almacenamiento.

El proveedor de Infraestructura como servicio IaaS, provee los recursos informáticos físicos subyacentes al servicio, incluidos los servidores, las redes, el almacenamiento y la infraestructura de alojamiento. El proveedor de nube ejecuta el software de la nube necesario para que los recursos informáticos estén disponibles para el consumidor de IaaS a través de un conjunto de interfaces de servicios y abstracciones de recursos de cómputo,

como máquinas virtuales e interfaces de red virtual. El consumidor de IaaS a su vez utiliza estos recursos de computación, como una computadora virtual, para sus necesidades de computación fundamentales.

Comparado con los consumidores de SaaS y PaaS, un consumidor de IaaS tiene acceso a formas más fundamentales de recursos de computación y más componentes de software, incluyendo el sistema operativo y la red. Por otro lado, el proveedor de IaaS tiene control sobre el software físico de hardware y nube que hace posible el aprovisionamiento de estos servicios de infraestructura, por ejemplo, servidores físicos, equipos de red, dispositivos de almacenamiento, sistema operativo host e hipervisores para la virtualización.

Las actividades de un proveedor de nube pueden describirse en cinco áreas principales, como se muestra en la Figura 9, un proveedor de nube lleva a cabo sus actividades en las áreas de despliegue de servicios, orquestación de servicios, gestión o administración de servicios en la nube, seguridad y privacidad.

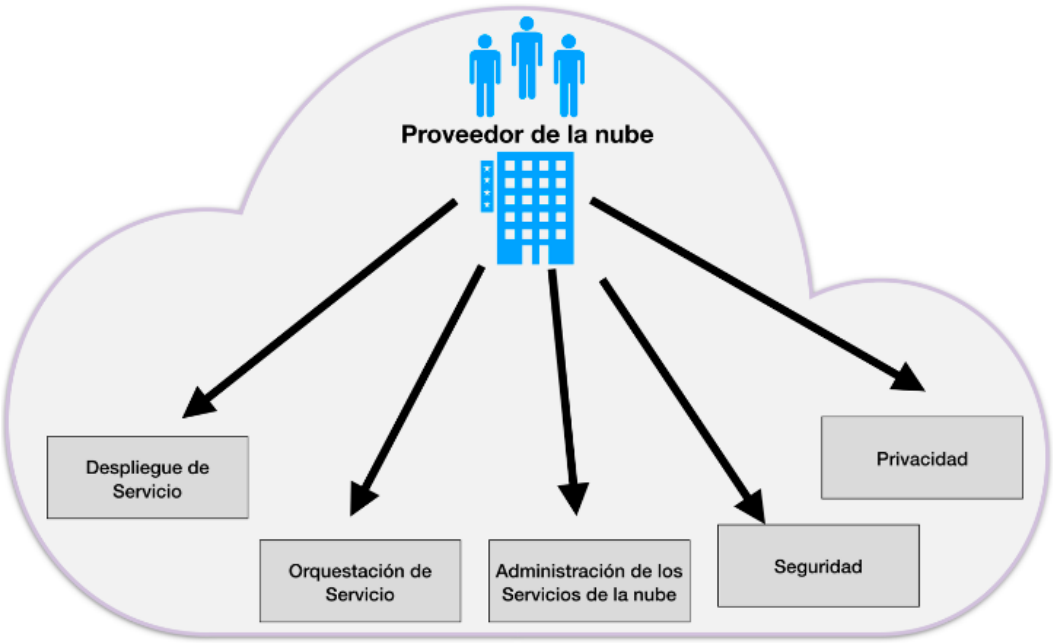


Ilustración 3 Actividades principales de un Proveedor de la nube

Despliegue de servicio: Una infraestructura de nube puede operarse en uno de los siguientes modelos de implementación: nube pública, nube privada, nube de comunidad o nube híbrida. Las diferencias se basan en la forma exclusiva en que están dados los recursos de computación a un consumidor de nube. Para mayor detalle, remítase al numeral 2.5 Modelos de implementación.

Orquestación del servicio: Se refiere a la composición de los componentes del sistema con el fin de proporcionar servicios en la nube a los consumidores de nube. La Figura 4 muestra un diagrama de pila genérico de esta composición que subyace al suministro de servicios en la nube.

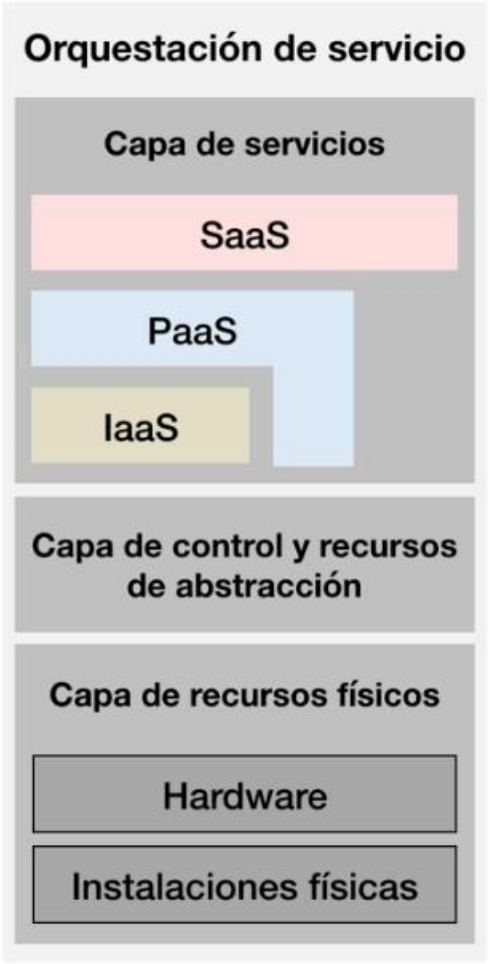


Ilustración 4 Proveedor de nube – Orquestación del Servicio

En esta representación se utiliza un modelo de tres capas, que representa la agrupación e integración de tres tipos de componentes del sistema que los proveedores de nube deben componer para entregar sus servicios.

En el modelo mostrado en la Figura 4, la parte superior es la capa de servicio, donde los proveedores de nube definen interfaces para que los consumidores de nube accedan a los servicios informáticos. Las interfaces de acceso de cada uno de los tres modelos de servicio se proporcionan en esta capa. Es posible, aunque no es necesario, que las aplicaciones SaaS puedan ser construidas sobre componentes PaaS y que los componentes PaaS puedan ser construidos sobre los componentes IaaS.

Las relaciones de dependencia opcionales entre los componentes SaaS, PaaS e IaaS se representan gráficamente como componentes que se apilan unos sobre otros, mientras que la inclinación de los componentes representa que cada uno de los componentes de servicio puede mantenerse por sí mismo. Por ejemplo, una aplicación SaaS se puede implementar y alojar en máquinas virtuales desde una nube IaaS o puede implementarse directamente encima de los recursos de la nube sin utilizar máquinas virtuales IaaS.

La capa media del modelo es la capa de abstracción y control de recursos. Esta capa contiene los componentes del sistema que los proveedores de nube utilizan para proporcionar y administrar el acceso a los recursos de computación física a través de la abstracción de software. Algunos ejemplos de componentes de abstracción de recursos incluyen elementos de software como hipervisores, máquinas virtuales, almacenamiento de datos virtuales y otras abstracciones de recursos informáticos. El aspecto de control de esta capa se refiere a los componentes de software que son responsables de la asignación de recursos, el control de acceso y la supervisión del uso. Esta es la estructura de software que enlaza los numerosos recursos físicos subyacentes y sus abstracciones de software para permitir la agrupación de recursos, la asignación dinámica y la medición del servicio.

La capa más baja de la pila es la capa de infraestructura que incluye los recursos físicos (hardware, redes, almacenamiento y otros aspectos de planta física). Esta capa incluye recursos de hardware, tales como computadoras (CPU y memoria), redes (enrutadores, firewalls, conmutadores, enlaces de red e interfaces), componentes de almacenamiento (discos duros) y otros elementos físicos de infraestructura de computación. También incluye recursos de instalaciones, tales como calefacción, ventilación y aire acondicionado (HVAC), energía, comunicaciones, entre otros.

Siguiendo las convenciones de arquitectura del sistema, la posición horizontal, es decir, la superposición, en un modelo que representa las relaciones de dependencia - los componentes de la capa superior dependen de la capa inferior adyacente para funcionar. La capa de abstracción y control de recursos expone los recursos de la nube virtual sobre la capa de recursos físicos y soporta la capa de servicios donde las interfaces de servicios en la nube están expuestas a los consumidores de la nube, mientras que los consumidores de la nube no tienen acceso directo a los recursos físicos.

Administración de los servicios en la nube: esta actividad incluye todas las funciones relacionadas con los servicios que son necesarios para la gestión y operación de los servicios requeridos o propuestos a los consumidores de nube. Como se ilustra en la Figura 5, la administración del servicio en la nube se puede describir desde la perspectiva del soporte empresarial, el aprovisionamiento y la configuración, y desde la perspectiva de los requisitos de portabilidad e interoperabilidad.

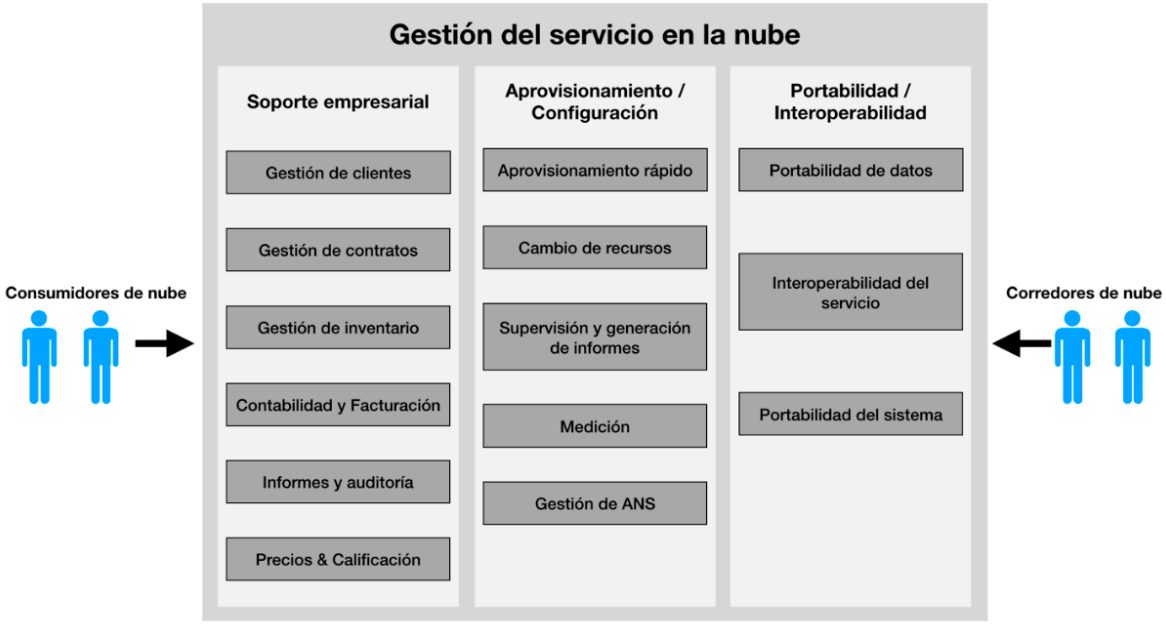


Ilustración 5 Proveedor de nube – Administración del servicio en la nube

- ✓ **Soporte empresarial o de negocios**: El soporte empresarial implica el conjunto de servicios relacionados con los negocios que se ocupan de los clientes y los procesos de apoyo. Incluye los componentes utilizados para ejecutar operaciones empresariales orientadas al cliente.
- ✓ **Aprovisionamiento y configuración**: Se refiere a las actividades del proceso que el proveedor debe ejecutar como parte de sus operaciones internas. Cuanto más maduras sean las capacidades de los proveedores en esta área, más efectiva y eficiente será la prestación del servicio. Una de las formas de aprovisionamiento que debería ofrecer un proveedor de nube es el aprovisionamiento rápido que consiste en proveer recursos, capacidades y servicios de manera automática cuando se cumpla una regla (umbral entre otros) establecida.
- ✓ **Portabilidad e Interoperabilidad**: Los proveedores de nube deben proporcionar mecanismos para apoyar la portabilidad de los datos, la interoperabilidad de los servicios y la portabilidad del sistema. La portabilidad de datos es la capacidad de los usuarios de la nube para copiar objetos de datos dentro o fuera de una nube o para usar un disco para la transferencia de datos a disposición del usuario sin intervención del proveedor.

La interoperabilidad de los servicios es la capacidad de los usuarios de la nube para usar sus datos y servicios a través de múltiples proveedores de nube con una interfaz de administración unificada. La portabilidad del sistema permite la migración de una instancia de máquina virtual totalmente detenida o una imagen de máquina de un proveedor a otro proveedor, o migrar aplicaciones y servicios y su contenido de un proveedor de servicios a otro.

Cabe señalar que varios modelos de servicios en la nube pueden tener diferentes requisitos en relación con la portabilidad y la interoperabilidad. Por ejemplo, IaaS requiere la capacidad de migrar los datos y ejecutar las aplicaciones en una nueva nube. Por lo tanto, es necesario capturar imágenes de máquinas virtuales y migrar a nuevos proveedores de nube que pueden

utilizar diferentes tecnologías de virtualización. Cualquier extensión específica del proveedor de las imágenes de las máquinas virtuales (VM por sus siglas en inglés Virtual Machine), debe eliminarse o registrarse al ser portada. Mientras que, para SaaS, el foco está en la portabilidad de datos, y por lo tanto es esencial para realizar extracciones de datos y copias de seguridad en un formato estándar.

d) Actividades del Auditor de nube

Un auditor de nube es una tercera parte (o una parte de la misma organización) que puede realizar una verificación independiente de los controles del servicio en la nube y así mismo, realizar auditorías para verificar la conformidad con las normas mediante la revisión de pruebas objetivas. Un auditor de nube puede evaluar los servicios proporcionados por un proveedor de nube en términos de controles pertinentes de seguridad, impacto sobre la privacidad, rendimiento, etc. [4][5]. Cabe aclarar que, por algún acuerdo de confidencialidad expreso entre proveedor y cliente, el auditor vería disminuido el alcance en la auditoría realizada. Por lo anterior es necesario que se establezca el alcance de la auditoria sin dejar excluidos los ANS respectivos, las características esenciales de un modelo de computación en la nube.

e) Actividades del corredor u agente (Intermediario) de nube

Un corredor de nube proporciona servicios comerciales y de apoyo a las relaciones (intermediación comercial), y servicios de soporte técnico (agregación, optimización e intermediación técnica). [4][5].

Intermediación de servicios: Un corredor de nube mejora un servicio añadiendo alguna capacidad específica y proporcionando servicios de valor agregado a los consumidores de nube. La mejora puede ser la gestión del acceso a servicios en la nube, gestión de identidades, informes de rendimiento, seguridad mejorada, etc.

Agregación de servicios: Un corredor de nube combina e integra varios servicios en uno o más servicios nuevos. El corredor (intermediario) proporciona integración de datos y asegura el movimiento seguro de datos entre el consumidor de nube y varios proveedores de nube.

Servicios de optimización: Este servicio es similar a la agregación de servicios, sin embargo, el corredor o intermediario tiene la flexibilidad de elegir y agregar servicios de varios proveedores. Por ejemplo, un proveedor puede agregar y seleccionar los servicios a partir del ranking obtenido por el cumplimiento de acuerdos de nivel de servicio.

f) Actividades del operador de nube

Un operador de nube actúa como un “intermediario” que proporciona conectividad y transporte de servicios en la nube entre los consumidores de nube y los proveedores de nube. Los operadores de nube proporcionan acceso a los consumidores a través de redes, telecomunicaciones. La distribución de servicios en la nube es normalmente proporcionada por operadores de redes y telecomunicaciones o un agente de transporte. [4][5].

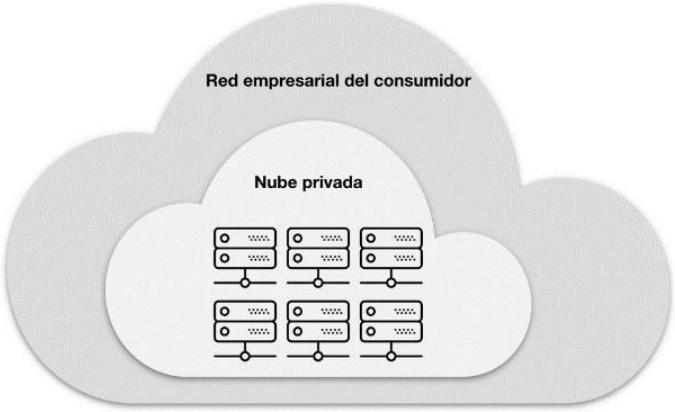
Hay que tener en cuenta que un proveedor de la nube establecerá ANS con un operador de nube para proporcionar servicios consistentes con el nivel de ANS ofrecidos a los consumidores de nube y puede requerir que el proveedor de nube proporcione conexiones seguras y dedicadas entre los consumidores de nube y los proveedores de nube.

3.3. Modelos de despliegues

Existen diferentes tipos de nubes [4] de acuerdo con las necesidades, al modelo de servicio ofrecido y a su despliegue, todo depende de dónde se encuentran instaladas las aplicaciones y qué clientes pueden usarlas, están los siguientes modelos:

3.3.1. Nube privada (Private cloud)

Una nube privada da a una sola organización de consumidores el acceso exclusivo y el uso de la infraestructura y los recursos computacionales. Puede ser administrado por la organización del consumidor de nube o por un tercero, y puede ser alojado en las instalaciones de la organización (por ejemplo, nubes privadas en el sitio) o subcontratado a una compañía de alojamiento (es decir, nubes privadas externalizadas) [4][5]. La Figura 8 y 9 representan una nube privada en el sitio y una nube privada subcontratada, respectivamente.



lustración 6 Nube privada en sitio

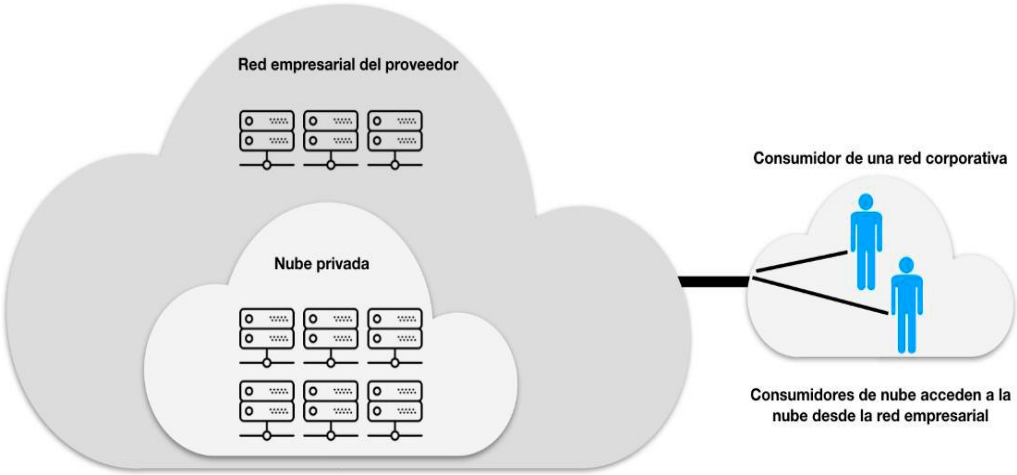


Ilustración 7 Nube privada subcontratada

3.3.2. Nube comunitaria (Community cloud)

Una nube comunitaria sirve a un grupo de consumidores que han compartido preocupaciones tales como objetivos de misión, seguridad, privacidad y política de cumplimiento, en lugar de servir a una organización como lo hace una nube privada. De forma similar a las nubes privadas, una nube comunitaria puede ser administrada por las organizaciones o por un tercero, y puede implementarse en las instalaciones del cliente (es decir, en la nube de la comunidad) o subcontratada a una compañía de hosting. La Figura 10 muestra una nube comunitaria en el sitio compuesta de varias organizaciones participantes. Un consumidor de nube puede acceder a los recursos de la nube local, y también a los recursos de otras organizaciones participantes a través de las conexiones entre las organizaciones asociadas. La Figura 9 muestra una nube de comunidad externalizada, donde el lado del servidor es subcontratado a una empresa de hosting. En este caso, una nube de comunidad externalizada construye su infraestructura fuera de la organización y sirve a un conjunto de organizaciones que solicitan y consumen servicios en la nube.

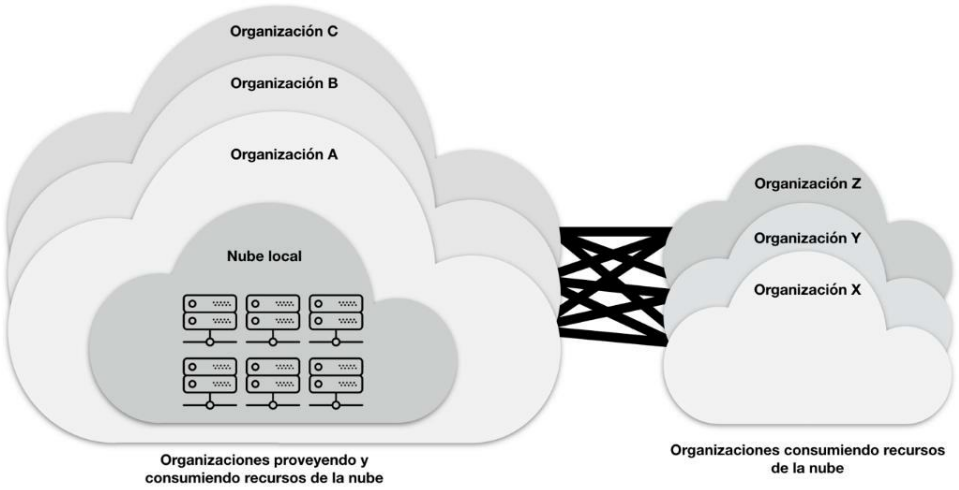


Ilustración 8 Nube comunitaria en sitio

3.3.3. Nube pública (Public cloud)

Una nube pública es aquella en la que la infraestructura en nube y los recursos informáticos se ponen a disposición del público en general a través de una red pública y es propiedad de una organización que vende servicios en la nube y sirve a una diversa cantidad de clientes. La Figura 11 presenta una vista simple de una nube pública y sus clientes.

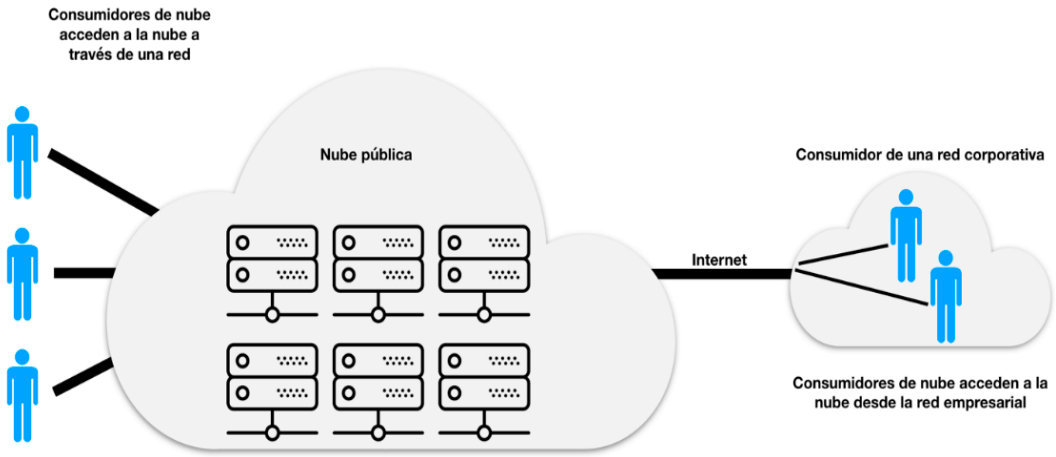


Ilustración 9 Nube pública

3.3.4. Nube híbrida (Hybrid cloud)

Una nube híbrida es una composición de dos o más nubes (en el sitio privado, en el sitio de la comunidad, fuera del sitio privado, fuera del sitio de la comunidad o público) que siguen siendo entidades distintas, pero están unidas por tecnología común entre las partes o propietaria que permite la portabilidad de datos y aplicaciones entre las nubes. La Figura 12 presenta una vista simple de una nube híbrida que podría ser construida con un conjunto de nubes en las cinco variantes del modelo de implementación.

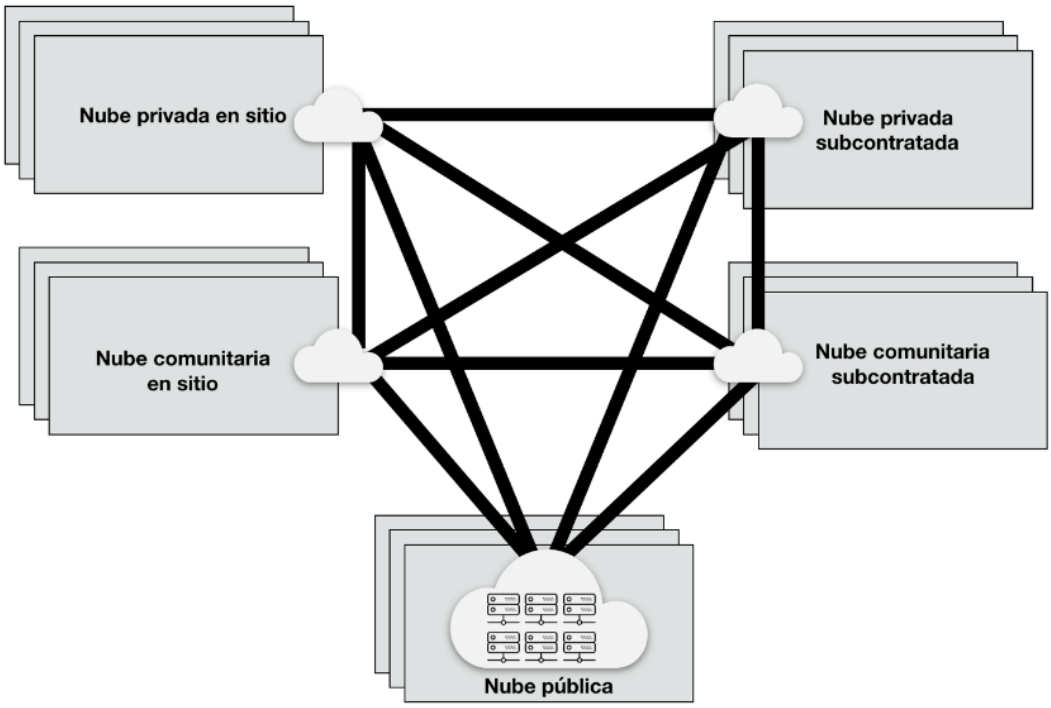


Ilustración 10 Nube híbrida

3.4. Categorías o modelos de servicios

La computación en la nube basa su arquitectura haciendo una separación entre infraestructura, plataforma y aplicaciones, como se ilustra en la figura 17 [5]:

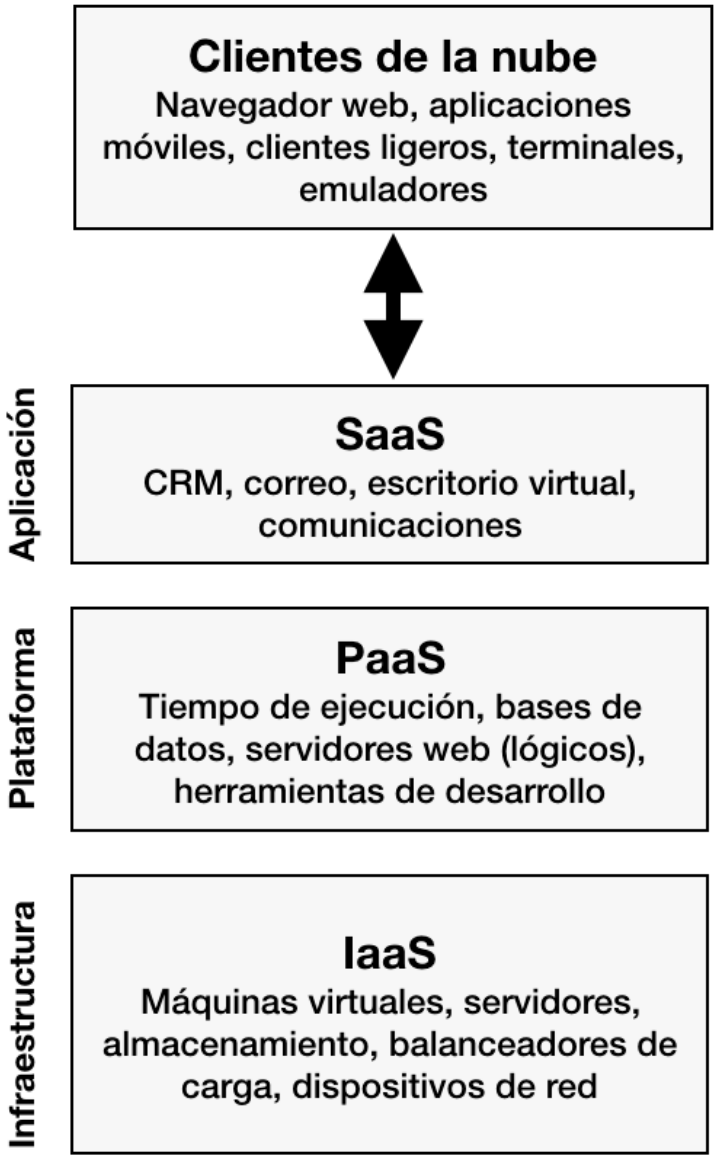


Ilustración 11 Modelos de servicios Cloud

3.4.1. Software como Servicio (Software as a Service – SaaS)

La capacidad proporcionada al consumidor consiste en utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de computación en la nube. Las aplicaciones son accesibles desde varios dispositivos cliente a través de una interfaz de cliente ligero, como un navegador web (por ejemplo, correo electrónico basado en web) o una interfaz de programa. El consumidor no gestiona ni controla la infraestructura subyacente de la nube, como la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades de las aplicaciones

individuales, con la posible excepción de los ajustes de configuración específicos de la aplicación específicos del usuario. El proveedor de SaaS es responsable del mantenimiento, operación y soporte del SaaS.

A continuación, algunos ejemplos de servicios de tipo SaaS: [5]:

- Correo electrónico y aplicaciones de oficina: Aplicaciones para correo electrónico, procesamiento de texto, hojas de cálculo, presentaciones, etc., dispuestos en la nube y con facturación según el uso.

- Facturación: Servicios de aplicación dispuestos en la nube, para gestionar la facturación de los clientes basándose en el uso y las suscripciones a productos y servicios.

- Sistemas de Gestión y manejo de relaciones con clientes (Customer Relationship Management-CRM): Aplicaciones de CRM dispuestas en la nube, que van desde las aplicaciones de centro de llamadas hasta la automatización de la fuerza de ventas y con facturación por demanda.

- Herramientas de Colaboración: Aplicaciones de software dispuestas en la nube, que permiten a los usuarios colaborar en grupos de trabajo, dentro de las empresas y entre empresas.

- Aplicaciones de gestión de contenidos: Servicio que permite el acceso a herramientas dispuestas en la nube para gestionar la producción y el acceso a contenidos de aplicaciones basadas en la web.

- Herramientas de gestión de documentos: Aplicaciones dispuestas en la nube para gestionar documentos, hacer cumplir los flujos de trabajo de producción de documentos y proporcionar espacios de trabajo para grupos o empresas para consultar y acceder a documentos.

- Finanzas: Aplicaciones para la gestión de procesos financieros que van desde el procesamiento de gastos y la facturación a la gestión tributaria.

- Recursos Humanos: Software para gestionar las funciones de recursos humanos dentro de las empresas.

- Aplicaciones de ventas: Las aplicaciones web dispuestas en la nube, facturación, compra y venta de productos y/o servicios, realización de pedidos, seguimiento de comisiones, etc.

- Redes de colaboración: software que permite la administración y seguimiento de diferentes tipos de plataformas de manera unificada, ya sean plataformas de redes sociales o plataformas de servicios.

- Planificación de Recursos Empresariales (ERP): Sistema integrado web, dispuesto en la nube para administrar recursos internos y externos, incluyendo activos tangibles, recursos financieros, materiales y recursos humanos. Para

que sea un SaaS, debe ser facturado por demanda y cumplir con las características definidas por el NIST, detalladas en este documento.

3.4.2. Plataforma como Servicio (Platform as a Service – PaaS)

Este modelo de servicio proporciona al consumidor la posibilidad de desplegar en la infraestructura de nube aplicaciones creadas por el mismo consumidor (o adquiridas a un tercero) utilizando lenguajes de programación, bibliotecas, servicios y herramientas soportadas por el proveedor de nube. El consumidor no gestiona ni controla la infraestructura subyacente de la nube, servidores, sistemas operativos o almacenamiento, pero tiene control sobre las aplicaciones desplegadas y posiblemente configuraciones para el entorno de hospedaje de aplicaciones. El proveedor de PaaS es responsable del mantenimiento, soporte y operación de las plataformas dispuestas como servicio. Esta capacidad no excluye necesariamente el uso de lenguajes de programación compatibles, bibliotecas, servicios y herramientas de otras fuentes.

A continuación, algunos ejemplos de servicios tipo PaaS: [5]:

- Inteligencia de Negocios: Plataformas para la creación de aplicaciones como paneles, sistemas de informes y análisis de datos.
- Base de datos: Servicios que ofrecen soluciones de base de datos relacionales escalables o almacenes de datos no SQL escalables.
- Desarrollo y pruebas: Plataformas para el desarrollo y los ciclos de pruebas de desarrollo de aplicaciones, que se expanden y se contraen según sea necesario.
- Integración: Plataformas de desarrollo para la construcción de aplicaciones de integración en la nube y dentro de la empresa.
- Implementación de aplicaciones: Plataformas adecuadas para el desarrollo de aplicaciones de uso general. Estos servicios proporcionan bases de datos, entornos de ejecución de aplicaciones web, entre otros.

3.4.3. Infraestructura como Servicio (Infrastructure as a Service – IaaS)

Este modelo de servicio proporciona al consumidor de nube, capacidades de procesamiento, almacenamiento, redes y otros recursos de computación fundamentales donde el consumidor es capaz de desplegar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no gestiona ni controla la infraestructura subyacente de la nube, sino que tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas y posiblemente un control limitado de componentes de red selectos (por ejemplo, firewalls de host).

A continuación, algunos ejemplos de servicios tipo IaaS [5]

- Copia de seguridad y recuperación: Servicios de copia de seguridad y recuperación de sistemas de archivos y almacenes de datos sin procesar en servidores y equipos de escritorio, siempre y cuando se garantice el autoaprovisionamiento y las demás características esenciales de la computación en las nubes antes mencionadas.

- Cómputo: recursos de servidor para ejecutar sistemas basados en la nube que se pueden aprovisionar dinámicamente y configurar según sea necesario, por ejemplo, memoria, procesador, entre otros.

- Redes de distribución de contenido (CDN): Una red de distribución de contenido es una gran red de servidores especializados distribuidos geográficamente que acelera la distribución de contenido web y multimedia a dispositivos conectados a Internet. La técnica principal que utiliza una red de distribución de contenido (CDN) para acelerar la distribución de contenido web a los usuarios finales es el almacenamiento en caché perimetral, que consiste en almacenar réplicas de contenido estático de texto, imagen, audio y vídeo en varios servidores alrededor del "perímetro" de Internet, de modo que las solicitudes de los usuarios se pueden responder mediante un servidor perimetral cercano, en lugar de mediante un servidor de origen lejano. Son ejemplos de uso de estos servicios los periódicos y emisoras de noticias cuando ocurren hechos como el ataque a las torres gemelas, que deben distribuir su contenido para soportar los altos volúmenes de concurrencia. También son muy usadas para la distribución de audio y video por internet en tiempo real.

- Gestión de servicios: Son servicios que permiten y facilitan la administración de plataformas de infraestructura en la nube. Estas herramientas aseguran rapidez en el despliegue, gestión y control de servicios IaaS sobre la nube. Un ejemplo en este caso es el software de capa media que permite administrar, verificar mediante informes de uso, desplegar servicios de IaaS

(almacenamiento, servidores, ampliación de infraestructura TI automática, empaquetadores) de manera centralizada.

- Almacenamiento: Capacidad de guardado de datos ampliamente escalable que puede utilizarse para alojar aplicaciones, copias de seguridad, archivos, entre otros siempre y cuando se garantice el autoaprovisionamiento y las demás características esenciales de la computación en las nubes antes mencionadas.

- Computación por lotes: Este servicio permite procesar cargas de trabajo que requieren informática de alto rendimiento (high-performance computing, HPC), análisis de grandes volúmenes de datos ("big data") y otras cargas de trabajo que requieran grandes cantidades de capacidad según demanda. No requieren de una alta disponibilidad, pero pueden requerir un alto rendimiento.

- Servicios tecnológicos de Internet de las cosas (Internet of Things, IoT): Estos servicios hacen referencia a infraestructura como sensores, cámaras, y otros dispositivos incluidos las aplicaciones de software que permiten su gestión y administración. Estos servicios se caracterizan por alta disponibilidad, capacidad flexible y escalable, interacción con dispositivos móviles, interoperabilidad y alta seguridad.

3.5. Beneficios ir a la nube

Como es conocido, la computación en la nube ofrece beneficios que permiten mayor flexibilidad para conectar y operar una empresa u organización desde cualquier lugar y en cualquier momento a través de la red, sin embargo, hay otros beneficios que provee el modelo de computación en la nube como los siguientes:

a) Reducción de costos de operación.

La adquisición de servicios de computación en la nube ofrece la posibilidad de pagar por la capacidad o servicio utilizado efectivamente, así como no pagar licencias de software, ni ocuparse de actualizaciones, compatibilidad con sistemas operativos, instalación, mantenimiento y soporte de equipos y servidores. Del mismo modo, se pueden optimizar costos en pago de servicios públicos, dado que el contratar servicios en la nube, puede disminuir el número de servidores y equipo de cómputo y por ende la reducción de servicios públicos en especial la energía eléctrica. Todos estos costos son conocidos como los costos de propiedad (TCO por sus siglas en ingles Total Cost Ownership) y en el sector público hacen parte del presupuesto de operación, donde el presupuesto de un área de TI, que está destinado en su mayoría o se emplea en cubrir los costos de operación y el presupuesto de inversión es cada vez más reducido. Los usos de estas alternativas hacen que una entidad pueda emplear o destinar estos recursos a inversiones de TI más estratégicas. En febrero de 2016, un estudio Gartner con recomendaciones e ideas para optimizar los costos de TI a través de soluciones computación en la nube, muestra que la reducción de costos en hardware y mantenimiento de TI, varia y depende del nivel de optimización y que cuando se utilizan soluciones y servicio de computación en la nube, se pueden alcanzar ahorros de hasta el 30% en costos TCO. [7][8][9]

b) Escalabilidad.

Las alternativas y servicios de computación en la nube ofrecen agilidad para desplegar nuevos servicios o trámites, flexibilidad y escalabilidad para responder a las demandas de capacidad y/o procesamiento que se requieran. Esto es especialmente útil en la prestación de servicios que tienen picos con gran número de solicitudes durante un periodo de tiempo que luego bajan y suben drásticamente [9]

c) Reducción de costos de obsolescencia tecnológica

La tecnología avanza todos los días y a una gran velocidad, por lo cual las inversiones o compra de bienes relacionados con TI tienen un mayor riesgo de presentar obsolescencia tecnológica. La obsolescencia se presenta como resultado del surgimiento de bienes de mejor calidad o con mejores características técnicas. Cuando se adquieren servicios de computación en la nube, ese riesgo se traslada al proveedor de servicios, dado que las entidades no invierten o compran tecnología (servidores, licenciamiento, aplicaciones de software) sino que pagan únicamente por su uso [7].

d) Acceso a tecnología de punta.

Gracias a que los proveedores de servicios de computación en la nube siempre están actualizando sus plataformas de software e infraestructura, las organizaciones de todos los tamaños pueden tener acceso a la misma tecnología y a los mismos avances tecnológicos. [9].

e) Rápida recuperación ante desastres y fallos.

Las capacidades de respaldo y recuperación ante fallos o eventualidades y las características de alta disponibilidad y continuidad del negocio son propios de la computación en la nube. Es conveniente revisar los contratos y acuerdos de niveles de servicio que cada proveedor ofrece [7][9].

f) Transferencia y reducción de riesgos técnicos

La implementación de nuevos servicios y sistemas de información para las entidades representan un menor riesgo técnico debido al respaldo del proveedor de servicios de computación en la nube, que a su vez posee y da soporte a otros clientes probando el mismo sistema y en procesos de mejora continua.

g) Entrega rápida y flexible

La adquisición de soluciones y servicios de computación en la nube, reducen el tiempo de salida y despliegue de nuevos servicios o trámites (reducción del time to market). Así mismo, permite aumentar o disminuir las capacidades y/o funcionalidades (ancho de banda, capacidad de procesamiento, capacidad de almacenamiento, entre otros) en algunos casos de forma automática (basado en reglas predefinidas). Las capacidades se pueden comprar prácticamente en cualquier cantidad y en cualquier momento. [7][9].

h) Permite concentrar esfuerzos en la misión y objetivos de la entidad

Los directores y líderes de Tecnología de las entidades públicas - CIO, pueden concentrar más recursos y esfuerzos hacia aspectos más estratégicos y de planeación que tengan impacto directo sobre los procesos de negocio de la organización, transfiriendo al proveedor la responsabilidad de la implementación, configuración y mantenimiento de la infraestructura requerida [9].

4. Seguridad y privacidad en la nube

En los últimos años, el uso de servicios en la nube por parte de entidades públicas ha aumentado significativamente debido a su flexibilidad, escalabilidad y eficiencia. Sin embargo, este crecimiento ha estado acompañado de nuevos desafíos en materia de seguridad y privacidad de la información. Los entornos de nube, por su naturaleza distribuida y altamente interconectada, introducen riesgos adicionales como la pérdida de control directo sobre los activos, la dependencia del proveedor, la exposición a legislaciones extranjeras, y la dificultad para auditar el cumplimiento de controles de seguridad.

En respuesta a estos desafíos, estándares internacionales como la **ISO/IEC 27017** (controles de seguridad en la nube) y la **ISO/IEC 27018** (protección de datos personales en entornos cloud) han establecido buenas prácticas específicas para mitigar los riesgos asociados al uso de la nube. Estas normas recomiendan, entre otros aspectos, garantizar la transparencia del proveedor, definir responsabilidades compartidas, asegurar el cifrado de la información y controlar la ubicación geográfica donde los datos son almacenados o tratados.

Por lo anterior, las entidades públicas deben exigir a sus proveedores de servicios en la nube **la declaración explícita de la ubicación física de los centros de datos donde se almacenará o procesará la información**, así como el cumplimiento de los **requisitos legales vigentes en Colombia en materia de protección de datos y soberanía digital**.

En lo posible, se deberá priorizar el uso de infraestructuras cuya geolocalización ya haya sido verificada en implementaciones anteriores dentro del país, o que se encuentren en jurisdicciones con marcos normativos equivalentes o convenios de cooperación en protección de datos personales.

Esta información deberá ser documentada como parte de la evaluación de riesgos, los contratos y los mecanismos de supervisión a proveedores, conforme a los principios de seguridad, privacidad, legalidad y responsabilidad institucional

4.1. Seguridad digtal y riesgos específicos del cloud

La seguridad en entornos cloud tiene exactamente el mismo objetivo que la seguridad digital en general: proteger nuestra infraestructura ante posibles ataques o interrupciones del servicio (ya sean accidentales o provocados). La principal diferencia la encontramos en la base de su diseño. En el caso del cloud, detrás de toda nuestra infraestructura tenemos un proveedor de servicios el cual también tiene su propia responsabilidad sobre los "assets" o "elementos" que nos ofrece como cliente de su nube. Todos conocemos las grandes ventajas de la computación en la nube o cloud computing. El principal de ellos es el considerable ahorro al no tener una infraestructura física, tanto en energía como en recursos para su configuración mantenimiento. También factores como la alta disponibilidad y las copias de seguridad de los elementos que componen la infraestructura son responsabilidades del proveedor, por lo que no tendremos que preocuparnos (al menos en principio) de ellas.

En los entornos cloud, los datos son la información más importante por proteger. Para mantener los datos lo más seguro posible es necesario cumplir tres requisitos básicos en el cloud:

1. Confidencialidad: garantizar que sólo los usuarios definidos dentro del sistema tienen acceso a la infraestructura y la información contenida en ella.

2. Integridad: los datos deben de mantenerse en su formato original, sin ningún tipo de alteración o modificación sin autorización.

3. Disponibilidad: debe de estar accesible y garantizar su acceso a todos los usuarios que necesiten acceder a la información. [21]

Ilustración 12 Capas de protección en el cloud para asegurar la información (datos)

En cambio, por otro lado, el estar en la nube implica tenerlo todo en internet, lo cual, sumado a las nuevas características del servicio ofrecido y la responsabilidad del proveedor, se abre una nueva ventana a vectores de ataques los cuales pueden ser totalmente nuevos aprovechando estas características o simplemente ser variaciones de los clásicos. Trabajar con un proveedor en el cloud, además de securizar todos los elementos que componen nuestra infraestructura (como máquinas virtuales, etc.) también debemos tener en consideración una correcta configuración y control de los servicios ofrecidos por el proveedor.

Todo lo que hemos aprendido sobre seguridad hasta ahora es aplicable al mundo del cloud, pero sin perder de vista algunos riesgos y amenazas que, aunque también sean similares en la informática en general, en el caso del cloud difieren debido a su naturaleza. Vamos a verlos en detalle para comprender mejor algunos de los riesgos específicos del cloud:

Accesos: es fundamental tener una buena política de control de accesos a nuestro sistema cloud, así como un acceso seguro y control a los servidores que componen nuestra infraestructura virtual. Una vez el usuario se ha validado correctamente es necesario controlar los diferentes recursos a los que puede acceder y evitar que tenga acceso o visibilidad a aquellos que no necesite (no sólo por seguridad, también por eficiencia del servicio). Los sistemas de doble factor de autenticación o 2FA así como las contraseñas seguras son elementos clave para evitar accesos no autorizados a nuestro entorno cloud. IAM (Identity and Access Management) es un framework que nos facilita la implementación de estos controles de accesos y gestión de la identidad presente en todos los servicios cloud.

Vulnerabilidades: el self-provisioning (autoaprovisionamiento) permite que un usuario pueda ejecutar o acceder a aplicaciones y servicios sin ser administrador del sistema o incluso sin ser parte del equipo técnico de IT. Está compuesta de una herramienta de gestión la cual controla los servicios o aplicaciones (backend). Cualquier vulnerabilidad en uno de estos servicios self-provisioning podría poner en riesgo toda la plataforma cloud. Las APIs creadas para gestionar este tipo de servicios también

tienen que estar completamente aseguradas y bien diseñadas desde el punto de vista de la seguridad.

Virtualización: todos los recursos ofrecidos por el proveedor son virtualizados y estos pertenecen a diferentes organizaciones, empresas o particulares. Por lo tanto, deben de estar aislados a nivel lógico (e incluso físico) entre ellos. Pero a pesar de este aislamiento, aparece una nueva amenaza la cual podría hacer que un potencial atacante explotara alguna vulnerabilidad, por ejemplo, del Hypervisor principal que almacena todas las máquinas virtuales de los diferentes entornos, y de esta forma tener acceso a toda la infraestructura cloud.

Tráfico de red cliente - proveedor: en el caso del cloud todas las peticiones al sistema se realizan entre cliente y proveedor del servicio cloud. Si un posible atacante puede interceptar o "esnifar" la información en tránsito nuestro servicio podría estar en peligro. Este riesgo se denomina Traffic Eavesdropping.

4.1.1. CSP y Algunos ejemplos

Vulnerabilidades: CVE y CVSS

Existen una gran variedad de proveedores de servicios cloud o CSP (Cloud Service Providers). Los más conocidos están Amazon con AWS (Amazon Web Services), Microsoft (Azure) y Google (Google Cloud), entre otros. Aunque los términos y las herramientas difieran entre los diferentes proveedores de servicios de computación en la nube, en general todos tienen un funcionamiento interno más o menos similar. El modelo de facturación es importante tenerlo claro debido a los altos costes por uso (se suelen tarificar por tiempo de utilización normalmente en fracciones de segundo).

4.1.2. Vulnerabilidades: CVE y CVSS

El mayor vector de ataque contra una infraestructura cloud se basa en aprovechar vulnerabilidades en todo tipo de software, desde aplicaciones hasta incluso el sistema operativo. Por lo tanto, es importante saber identificarlas teniendo claro qué significan las siglas CVE o Common Vulneratilities and Exposures. El etiquetado CVE tiene el siguiente formato general: CVE-AAAA-NNNN, AAAA es el año de descubrimiento de la vulnerabilidad y NNNN su número único asignado. Cuando una nueva vulnerabilidad solicita un código CVE, durante proceso de aceptación comenzarán con CAN-AAAA-NNNN.

Por otro lado, CVSS o Common Vulneratility Scoring System en la versión 3.0, ofrece una puntuación final indicando el nivel de amenaza de la vulnerabilidad con un valor entre 0 (menos importante) y 10 (crítica).

Ejemplo de etiquetado CVE y puntuación CVSS de la vulnerabilidad “Meltdown”: CVE-2017-5754. AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Puntuación CVSS: 5.6 Medium

Fuente: https://nvd.nist.gov/vuln/detail/CVE-2017-5754

4.1.3. Responsabilidad compartida (CSP y Cliente)

A la hora de contratar un servicio con un CSP es necesario tener perfectamente atados y claros los límites de la responsabilidad, tanto por parte del CSP como por parte del cliente, en los recursos y el servicio ofrecido. Es importante resaltar que contratar este tipo de servicios implica que todos nuestros datos, así como la infraestructura, pasa a manos de una empresa externa o un tercero y, por lo tanto, tener claro que el CSP no se hará cargo de todos los problemas de seguridad que puedan aparecer. Es decir, el CSP sólo será responsable de los servicios asociados directamente a su diseño, como por ejemplo ofrecer acceso seguro a bases de datos, almacenamiento, aislamiento, interrupción de energía, etc.

Nosotros como clientes, seremos responsables de cumplir e implementar lo que sea necesario para proteger nuestra infraestructura. El cliente es el responsable de toda la seguridad de sus activos en la nube. Pero no sólo eso, también es responsable de la correcta configuración y seguridad de la configuración de los servicios ofrecidos por el CSP como son por ejemplo los accesos, monitorización, gestión de logs, etc. La gestión de accesos es crítica ya que afecta no sólo a nuestra infraestructura ubicada en la nube, sino también a la gestión de la misma.

Haciendo un resumen estas son las responsabilidades clave de cada uno:

CSP:

- Accesos de administrador de los clientes.
- Actualizaciones y seguridad del Hypervisor que sustenta la infraestructura.
- Seguridad de los servicios.
- Aislamiento respecto a otros clientes del CSP.
- Protección ante ataques DDoS o similares.
- Almacenamiento, computación, bases de datos, red perimetral y cualquier otro servicio ofrecido por el CSP están bajo su responsabilidad

Cliente:

- Gestión, monitorización y securización de la red interna.
- Configuración, mantenimiento, monitorización y actualizaciones de las aplicaciones ubicadas en el servicio.
- Creación de políticas de seguridad para la red y todos los elementos que conforman la infraestructura.

- Cifrado.
- Fortificación de los servidores virtuales

4.1.4. Autenticación y autorización (IAM)

Antes, se ha mencionado el concepto de IAM o Identity and Access Management. Este servicio es realmente importante ya que es el portal principal que da acceso a todos nuestros servicios, así como su control, dentro de la nube. Por lo tanto, será necesario crear unas políticas responsables las cuales incluyan una asignación correcta de los usuarios y sus accesos mediante la creación de grupos y roles varios. Todos los proveedores de servicios cloud ofrecen utilidades o incluso un panel de control a los diferentes clientes del cloud. Cuando nos damos de alta por primera vez en uno de estos servicios, siempre lo haremos con una cuenta principal, a veces denominada también root.

La primera de las medidas de seguridad está asociada a esta cuenta: nunca utilizarla en tareas cotidianas, esta cuenta se debe de utilizar las tareas concretas de administración de cuentas y algunos servicios críticos. La segunda está orientada más a los accesos, es decir, será necesario tener un control con la máxima información detallada de los accesos a nuestro sistema por parte de clientes o trabajadores.

No debemos olvidar por otro lado, que los accesos no se realizan sólo por personas y contra el frontend del CSP los cuales tienen una estructura similar a esta en la cual tenemos que introducir nuestro usuario y contraseña:

También es posible que programas accedan a nuestros servicios utilizando APIs. Por lo tanto, será necesario también una serie de políticas y controles de seguridad a la hora de la creación de código.

4.1.5. MFA o Multi Factor Authentication

Es una capa adicional de seguridad además del usuario y la contraseña. En otras palabras, no es más que un 2FA o Doble Factor de Autenticación. Es decir, cuando el usuario acceda a la cuenta de del CSP, si tiene activada esta opción será necesario introducir también una respuesta adicional (suele ser un token) generada por un dispositivo externo o una aplicación. Dicho dispositivo (un Smartphone es el más extendido, aunque existen muchos otros) nos genera una nueva contraseña o token la cual introduciremos junto a nuestras credenciales normales.

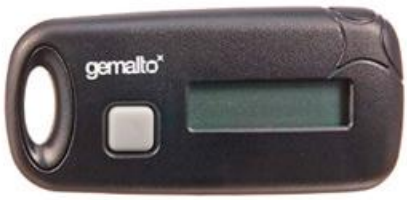


Ilustración 13 Ejemplo de MFA físico modelo SafeNet IDProve 100 6-digit OTP Token.

Fuente: https://aws.amazon.com/es/iam/features/mfa/?audit=2019q1

Las aplicaciones virtuales son las más extendidas ya que pueden instalarse en un teléfono móvil. Las principales opciones son: Google Authenticator y Authy 2FA.

Es importante destacar que la pérdida de nuestro elemento 2FA, ya sea físico o virtual (es decir, el dispositivo donde se encuentra almacenada la aplicación, un Smartphone, por ejemplo) implica perder el acceso a nuestros sistemas. Para poder volver a acceder será necesario hablar con nuestro proveedor CSP para dar de baja el dispositivo y volver a dar de alta otro nuevo.

4.1.6. AK/SK, Access Key y Secret Key

Aparte de los accesos habituales por parte de usuarios a nuestro cloud o los servicios que tengamos alojados en ella, también hay que tener en cuenta otro tipo de acceso: el realizado automáticamente por un programa desde una API. Si nuestro servicio ofrece una API para acceder a él o ejecutar algún servicio dentro de una aplicación diseñada a medida, debemos tener en cuenta y controlar su seguridad.

Una Access Key (AK) es un token alfanumérico de cierta longitud (más de 10 caracteres) la cual permite el acceso de la API desde un programa. Este token a su vez lleva asociada una Secret Key (SK) única para el usuario/programador la cual no se debe compartir ni poner visible en el código fuente. El CSP entrega estas contraseñas una vez solicitadas mediante una única descarga por lo tanto es necesario almacenarlas en un lugar seguro. Todos estos accesos mediante API se pueden controlar y gestionar desde el panel de control IAM.

4.1.7. Políticas (policies)

Antes incluso de empezar a crear los usuarios, grupos y roles, será necesario revisar y crear las políticas necesarias de las cuales definirán a qué recurso del sistema podrán acceder. Las políticas prácticamente en todos los proveedores están siempre relacionadas con dos factores: la identidad (el usuario o grupo) y un recurso concreto (por ejemplo, una instancia). Estas políticas son ficheros con formato JSON y el siguiente ejemplo muestra Script o líneas de códigos para configurar una política de un CSP de sólo lectura, es decir, si se aplica a un usuario este sólo podrá consultar los recursos, pero no podrá realizar ninguna acción sobre ellos:

```
{
“Version”: “2012-10-17”,
“Statement”: [{
“Effect”: “Allow”,
“Action”: “ec2:Describe*”,
“Resource”: “*”
}
]
}
```

El campo “Versión” como su nombre indica la versión de esta política. Por otro lado “Statement” se compone a su vez de las siguientes acciones: “Effect” (permite o deniega la acción que ahora tendrá definida), “Action” es la acción a realizar y “Resource” define el recurso sobre el cual estamos aplicando la política.

4.1.8. Usuarios, grupos y roles

La autorización de los diferentes usuarios es una tarea básica que a su vez necesita de una buena planificación y control para asignar correctamente desde sus privilegios de acceso como las tareas que puede ejecutar dentro del cloud. Como es lógico, esta será la primera de las tareas después de contratar nuestro servicio cloud pero no debe limitarse exclusivamente a crear los usuarios y sus accesos. Una vez creado el usuario y su perfil será imprescindible clasificarlo y es aquí donde entran los grupos. Aunque el primer paso después de crear un usuario será siempre aplicarle una política, el siguiente será asignado a un grupo concreto.

Un grupo en un CSP funciona igual que los grupos Linux, Windows, AD, etc. Un grupo tiene asociado una lista de elementos, en este caso usuarios, que se agrupan en un nombre (nombre del grupo). Esto nos permite manipular a dichos usuarios sin tener que hacerlo de forma individual ya que el nombre de grupo se asocia a todos ellos. Por ejemplo, el siguiente árbol muestra una organización donde podemos observar, entre otros detalles, que un usuario puede pertenecer a más de un grupo:

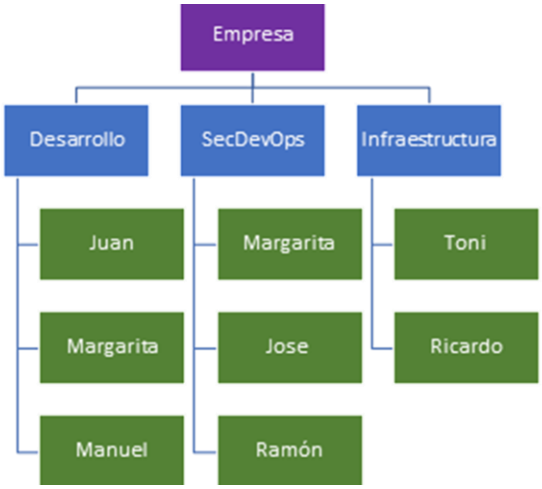


Ilustración 14 Ejemplo Usuarios, grupos y roles

Podemos observar tres grupos llamados "Desarrollo", "SecDevOps" e "Infraestructura". La usuaria Margarita está presente en dos ellos, "Desarrollo" y "SevDevOps" por lo tanto tendrá aplicadas todas las políticas asignadas dichos grupos.

El paso final una vez tenemos los grupos y los usuarios son los roles o conjunto de permiso que permiten realizar acciones sobre los recursos del CSP. Aquí tenemos que destacar el término cross-role, el cual permite que un mismo usuario pueda acceder a las cuentas de todo el sistema. Los permisos de los roles también se gestionan con las correspondientes políticas asignadas. Algunos de los usos prácticos de los roles son:

- **Role de servicio**. Se aplica a un servicio de CSP para realizar acciones como crear instancias, etc.
- **Role de servicio asociado a una instancia**. Permite que la instancia pueda por ejemplo ampliar el espacio de disco, etc.
- **Role vinculado a un servicio**. Son roles de servicio, pero vinculados exclusivamente a uno en concreto, como por ejemplo Elasticsearch el cual sirve para gestionar clúster.
- **Delegación de roles**. Necesario para que una cuenta maestra pueda controlar y por ejemplo ejecutar un servicio en otra cuenta. Federación, por ejemplo, para hacer login en la consola de CSP mediante el login de Facebook, Google, etc.
- **Encadenamiento de roles**. Concatenación entre diferentes roles entre ellos.

4.1.9. IDP o Identity Providers

Si nuestra organización ya tiene por defecto una estructura de usuarios, como por ejemplo puede ser un LDAP, con esta función tendremos la opción de administrarlas desde la cuenta de un CSP que la entidad halla contratado. De esta forma no será necesario dar de alta a dichos usuarios directamente en el CSP, ya que su

configuración, función y datos se heredan directamente del directorio de uso corporativo que estemos utilizando.

Para poder utilizar un IDP en un CSP es necesario siempre crear una relación de confianza entre el CSP y el IDP. Una vez creada la relación de confianza obtendremos algunas ventajas como por ejemplo utilizar un mismo usuario que pueda acceder al entorno cloud y también al resto de servicios corporativos fuera del cloud, facilidad a la hora de gestionar contraseñas (podemos hacerlo directamente desde nuestro servicio de directorio), reflejo inmediato en el cloud de cualquier cambio realizado en la estructura del directorio (altas de usuarios, bajas, cambio de contraseñas, etc.) Es necesario que el servicio de directorio que tengamos en nuestra organización sea compatible con OpenID Connect (OIDC) o SAML 2.0.

4.1.10. Criptografía

El mantener oculta la información que está almacenada o recorre nuestra infraestructura es una tarea fundamental y clave en nuestros sistemas, además de ser obligatoria como indica la GDPR. La criptografía se encarga de estudiar las diferentes técnicas o métodos de protección de la información. Para ello utiliza diferentes algoritmos de cifrado para de esa forma, conseguir ocultar la información real almacenada. Para poder obtener de nuevo la información original será necesario disponer de una clave secreta (o clave de descifrado).

Centrándose en los tipos de cifrado según sus claves:

Simétrico: la misma clave es utilizada tanto para cifrar como para descifrar la información. Los más conocidos son el DES, Triple DES, AES, etc.

Asimétrico (o clave pública): en este caso se utilizan claves distintas, en concreto dos: una pública y otra privada. La clave privada sirve para descifrar la información y la pública se utiliza sólo para el cifrado. RSA y PGP son los más conocidos.

Según la naturaleza de la arquitectura, debemos tener en cuenta de los datos están en reposo (por ejemplo, almacenados en alguna ubicación) o en tránsito (cuando se desplazan de un sistema o servicio a otro). El siguiente listado muestra algunos de los conceptos de criptografía y su definición utilizados en la gran mayoría de los CSP:

Datos autenticados adicionales (AAD): integridad y autenticidad de datos mediante el uso de datos autenticados adicionales durante el proceso de cifrado (datos autenticados, pero no cifrados).

Autenticación: Determina si una entidad es quien afirma ser, o que no la han manipulado entidades no autorizadas.

Autorización: Acceso legítimo autorizado de una entidad a un recurso.

Cifrado de bloque: se utiliza para cifrar información con una longitud aleatoria, es decir, la longitud (por ejemplo, en caracteres) del texto sin cifrar no es la misma que el texto cifrado.

Clave de datos: clave simétrica que genera el CSP, utilizada para cifrar o descrifrar información.

Descifrado: proceso de convertir la información cifrada en el formato que tenía antes del cifrado.

Cifrado: aplicar un algoritmo que oculte la información real ofreciendo confidencialidad de datos a un mensaje o datos no cifrados.

Contexto de cifrado: AAD específicos de los KMS con el formato de par “clave“: “valor”. Aunque no está cifrado, está vinculado al texto cifrado durante el cifrado y se debe pasar de nuevo durante el descifrado.

Clave maestra: Una clave creada por los KMS que solo se pueden utilizar en el servicio de estos KMS. La clave principal se utiliza habitualmente para cifrar claves de datos para que el servicio pueda almacenar la clave cifrada de forma segura. [21]

4.1.11. Secrets Manager

Los CSP ofrecen esta herramienta para gestionar los datos confidenciales (también llamados habitualmente “secretos”) relacionados con el acceso a los servicios. Es decir, es un gestor de credenciales (también tiene su propia API) el cual ayuda al administrador del sitio a ampliar la seguridad sobre sus diferentes elementos de la infraestructura. Por ejemplo, permite administrar el acceso a los datos confidenciales basándose en políticas creadas previamente con el IAM.

Un secreto puede ser cualquier tipo de información que ofrezca algún dato confidencial o sensible. Por ejemplo, el nombre de un servidor, un puerto, una dirección IP, nombre de usuario, contraseña, etc. Cifra esta información utilizando los KMS el cual se encarga de generar claves para el cifrado o descifrado. El transporte de este tipo de información también es importante y por lo tanto los Secrets Manager sólo lo hace utilizando el estándar TLS y PFS (Perfect Forward Secrecy). Una característica a tener en cuenta que aumenta también la seguridad es la rotación. La rotación permite crear de forma automática nuevas versiones del tipo de cifrado del secreto. En general estas herramientas, Secrets Manager cuentan con una interfaz web de control y un CLI. [21]

4.1.12. Certificate Manager (CM)

Esta herramienta permite gestionar los certificados SSL/TLS, los cuales se utilizan para proteger las comunicaciones. En definitiva, los Certificate Manager es un gestor de certificados que permite la compra, carga, renovación o cualquier otra gestión asociada a un certificado (ya sea público o privado), todo de forma automática. Esta herramienta, se integra con el resto de los servicios de la nube del CSP. CM también genera sus propios certificados públicos basados en el dominio (DV) y tienen una validez por lo general de 13 meses. [21]

5. Computación en la nube en Colombia

5.1. Contexto normativo

La legislación colombiana consagra como uno de sus principios rectores de las Tecnologías de la Información y las Comunicaciones la neutralidad tecnológica cuyo concepto fue definido en la Ley de TIC 1341 del 30 de Julio de 2009 y se ratifica en el decreto 1078 de 2017 articulo 2.2. 9.1.1.1 de la estrategia de Gobierno Digital . Este principio plantea: "El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible. [10] [11]

Así mismo, el Marco de Referencia de Arquitectura empresarial para la gestión de TI, adopta entre sus principios el principio de Neutralidad Tecnológica, el cual plantea que el Estado no debe privilegiar tecnologías, ni proveedores y por lo tanto las entidades del Estado deben hacer una evaluación de las alternativas de inversión, aplicando criterios y evaluando todas las posibilidades para obtener una buena relación costo/beneficio. Por lo anterior las entidades públicas, especialmente al adquirir servicios de computación en la nube deben evaluar y justificar la selección de servicios y tecnología de manera objetiva, siendo deseable las alternativas de computación en la nube.

De otro lado, la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente, con el apoyo técnico del Ministerio de TIC, puso a disposición de las entidades estatales los siguientes Acuerdos Marco de TI relacionados con los servicios de computación en la nube: (i) Servicios de Centro de Datos/Nube Privada, I y II generación, y (ii) Servicios de Nube Pública (actualmente en estructuración la II generación). Estos Acuerdos Marco de TI le permiten a las Entidades Estatales adquirir los servicios de este tipo, mediante un proceso ágil y transparente; aprovechando el poder de compra del Estado para generar economías de escala y adquirir servicios de TI con características técnicas uniformes, generando importantes ahorros al Estado Colombiano, teniendo en cuenta a sección abreviada de la Ley 80 de 1993 y la Ley 1150 de 2007 para acceder a los Acuerdo Marco de Precios.

Así mismo, los diferentes conceptos, cartillas y demás que la Superintendencia de Industria y Comercio publicó para aplicarlo en cuanto a los datos y computación en la nube [12] [18].

6. Pasos fundamentales para dar el salto a la nube

6.1. Identificación y análisis de riesgos de migrar a la nube.

Con el análisis de Riesgo, los objetivos misionales y funcionales de la Entidad, así como la estrategia de TI para apoyar dichas actividades, es de vital importancia para la toma de decisiones de lo que se debe o puede migrar a la Nube. Teniendo en cuenta lo anterior estos pueden ser:

- Datos.
- Servicios.
- Aplicaciones.
- Funcionalidades o Procesos.

Una de las actividades más importante es la evaluación de riesgo de los activos que se van a mover a la nube, en esta la entidad identifica los datos y funcionalidades a mover. También debe tener presente el aumento de tráfico, operaciones y datos; los cuales pueden ser mayores de lo planeado.

Identificar que tan importantes son las operaciones y/o datos para la entidad; donde se determine qué tan confidencial es la información, el proceso, la operación o función a migrar. La entidad puede realizar una autoevaluación a través de preguntas sencillas donde identifique el valor de los activos en términos de confidencialidad, disponibilidad, integridad y su riesgo asociado al llevar los datos a la nube parcial o totalmente.

Por ejemplo: Que impacto tendría en la entidad si:

- El activo estuviera expuesto públicamente
- Un funcionario del tercero o proveedor accediera al activo
- Un proceso fuera modificado por un externo
- Un proceso o alguna de sus funciones entregaran resultados erróneos
- La información o datos fueran modificados de manera inesperada
- Se presentarán fallas de disponibilidad

6.2. Aprovisionamiento de servicios

Dentro del ámbito de la Gestión de Servicios [5], que significa proveer, acondicionar y habilitar un servicio, para que el usuario final se pueda beneficiar con él, satisfaciendo sus requerimientos con la calidad acordada. En otras palabras, el aprovisionamiento de servicios de computación en la nube debe ser provisto bajo demanda acorde con los acuerdos de nivel de servicios y demás condiciones contractuales, de una manera eficiente en tiempo, costo y uso de recursos. [16]

Como se mostró anteriormente, una de las características esenciales de la computación en la nube es el Autoservicio bajo demanda (On-demand self-service) donde un consumidor puede de manera unilateral proveer capacidades de computación (almacenamiento, procesamiento entre otros) según sea necesario o automáticamente, prácticamente sin interacción con el proveedor de servicios. Por lo anterior, es necesario aclarar que los Acuerdos Marco (AM) de Nube Pública y Nube Privada II generación, habilitados por Colombia Compra Eficiente, buscan ser instrumentos que faciliten la adquisición de estos servicios para las Entidades del Estado, sin embargo, en concordancia con las leyes colombianas referentes al presupuesto y gasto público, esta característica esencial de auto-aprovisionamiento es limitada según el valor y servicios definidos en las ordenes de compras emitidas por cada Entidad Estatal a través de la Tienda Virtual del Estado Colombiano (TVEC). Así pues, es necesario que las entidades del Estado tengan en cuenta esta limitante al momento de adquirir servicios de Nube Pública y Nube Privada a través de los AM de TI.

6.3. Migración y Portabilidad

Las organizaciones que revisan como alternativa la computación en la nube, deben ser conscientes que pueden tener que cambiar de proveedor en el futuro, en especial si se utilizan servicios de computación en la nube contratados a través de los Acuerdos Marco de TI, en donde, dado que se tiene un bien o servicio de características uniformes, el único diferenciador que queda es el precio, de manera que el proceso de adjudicación se da al proveedor que cotice el menor valor por los servicios de nube solicitados y cotizados a través de la Tienda virtual del Estado Colombiano (TVEC) y dicha adjudicación no siempre se realiza por el periodo de vigencia del AM, el cual puede ser en algunos casos de 2 años prorrogable a 3, si no que corresponde más a las condiciones de planificación de cada entidad.

La contratación de servicios de computación en la nube por parte de las entidades públicas debe garantizar la portabilidad de los datos entre los prestadores de servicios en el menor tiempo posible. Deben existir reglas claras que permitan a la entidad propietaria de la información (contratante) acceder a toda su información y poderla migrar nuevamente a sus sistemas o a otros proveedores del servicio con total garantía de la integridad de la información y sin incurrir en costos adicionales [13] [14].

Para ello deben existir cláusulas que garanticen que, al término del contrato ya sea por decisión del contratante, del proveedor del servicio, por eventos tales como quiebra o insolvencia entre otros, toda la información suministrada por los usuarios y almacenada por los proveedores pueda ser restituida a los usuarios o a terceros designados por estos, recuperada por los usuarios con herramientas provistas por el proveedor, sin contratiempos. La migración y la portabilidad suelen ser parte del plan de continuidad de las entidades.

6.4. Escalonamiento

Hay que tener presente que no es necesario migrar de inmediato ni en su totalidad todos los servicios de tecnologías de la información (TI) a la nube. Se recomienda realizar este paso gradualmente e iniciar con pequeños pasos. Para mover los servicios a la nube hágase los siguientes cuestionamientos: 1) Qué vale la pena migrar a la nube de manera inmediata. 2) Qué puede esperar, 3) Qué aplicaciones es preferible mantener internas en el futuro previsible.

Este abordaje permite que se migren a la nube las aplicaciones que determine la entidad, manteniendo (sin migrar a la nube) las que según el caso se considere adecuado mantener alojadas en centros de datos propios

6.5. Definición De La Seguridad y Privacidad

La mayoría de las infraestructuras en esquemas de computación en la nube son compartidas por múltiples empresas o usuarios y una mala definición de los niveles de seguridad puede generar accesos no autorizados a datos confidenciales, sin embargo, cabe aclarar que los esquemas de computación en la nube cuentan con las herramientas necesarias que garantizan un ambiente seguro entre usuarios. La definición de una buena política de identidad y control de acceso, basado en el mínimo privilegio, es esencial en entornos Cloud [13] [14] [15]. Además, es importante aclarar que, al ser un modelo de seguridad compartido, la responsabilidad de la seguridad recae en ambas partes y se debe verificar: que el proveedor cuente con las herramientas y condiciones requeridas y que la entidad las usa bien.

Así mismo, las entidades deben a partir de la clasificación de la información de la ley de transparencia y acceso a la información pública (ley 1712 de 2014), Ley de Protección de datos personales 1581 de 2012 y demás normatividad aplicable y vigente, determinar qué información puede o debe llevarse a la nube.

De otro lado, la entidad contratante debe asegurarse de cumplir con la reglamentación que para tal efecto prevé la legislación colombiana sobre protección de datos personales, dentro y fuera de país y para ello debe exigir al proveedor los mecanismos que garanticen el borrado seguro de los datos al finalizar el contrato. (Un mecanismo apropiado es requerir una certificación de la destrucción emitido por el proveedor del servicio) [13] [14] [15].

Una estrategia que implique usar los servicios en la nube en empresas tiene sentido en primera instancia, solo si los aspectos de seguridad sean garantizados en su totalidad. [20].

6.6. Gestión de incidentes

Se debe definir de manera explícita y clara el proceso o procedimiento para la gestión de incidentes en donde el proveedor de nube le informe al contratante si ha ocurrido algún incidente con el servicio o se ha puesto en riesgo la seguridad de la información. El procedimiento debe indicar: a) acciones y secuencia de las acciones a seguir durante el

procedimiento, b) responsables e interlocutores, c) tipología de incidentes incluidos en el servicio, d) procedimientos específicos ante incidentes de seguridad, e) tiempos de respuesta y resolución de incidentes y f) gestión y resolución de incidentes, entre otros que defina el proveedor de nube. [13]

6.7. Gestión de Cambios

Las entidades deberán establecer contractualmente la obligación de mantener actualizados los sistemas para garantizar su funcionamiento, así como eliminar las vulnerabilidades que pueden afectar los servicios de computación en la nube prestados. Para ello se podrá definir un procedimiento de coordinación en el mantenimiento de la infraestructura que soporta los servicios entre ambas partes para prevenir interrupciones o errores en la prestación del servicio; este procedimiento debe incluir la notificación con suficiente antelación de la realización de mantenimientos por parte del proveedor, identificando los tiempos en los que puede interrumpirse el servicio. La notificación deberá realizarse previa y posteriormente al mantenimiento y tras éste la entidad contratante deberá notificar la conformidad del correcto funcionamiento del servicio. [9]

Así mismo, siempre que el mantenimiento o actualización implique un cambio mayor o pueda suponer el funcionamiento incorrecto de los sistemas de la organización cliente o entidad contratante del servicio, la entidad deberá solicitar al proveedor la habilitación de un entorno actualizado de pruebas que permita verificar el correcto funcionamiento de sus sistemas en preproducción. Se debe exigir a los proveedores informar periódicamente de los mantenimientos y actualizaciones realizados en los sistemas que albergan los sistemas del cliente

6.8. Asuntos legales relacionados con la residencia física de los datos.

El contratante debe asegurarse de que siempre tendrá la propiedad y el control de su información independientemente del lugar donde se almacenen los datos. Las entidades deberán evaluar y revisar el marco normativo vigente en esta materia. [13].

Adicionalmente la entidad debe asegurarse que la residencia física de los datos se encuentre en uno de los países que ofrecen un nivel adecuado de protección de datos de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, garantizando el cumplimiento del artículo 26 de la Ley Estatutaria 1581 de 2012

6.9. Servicio totalmente dependiente de una conexión a internet

Contratación de un mayor ancho de banda en la empresa cliente e implementación de políticas de calidad de servicio o conexiones alternas, para evitar problemas de cuellos de botella en el acceso a las aplicaciones, o accesibilidad lenta que puedan poner en juego el desempeño de las aplicaciones. Se recomienda actualizar los planes de capacidad sobre los servicios de TI y revisar condiciones técnicas como el ancho de banda, latencia del servicio y tecnologías a utilizar. Se aclara que, para nubes privadas, hibridas o comunitarias, el servicio se puede prestar a través de redes MPLS, Metroethernet entre otras.

6.10. Planes de continuidad del negocio (BCP) y recuperación de desastres (DR).

Dependiendo la criticidad del servicio, los clientes o entidades contratantes pueden inspeccionar y hacer parte de las pruebas de los planes de recuperación de catástrofes y de continuidad del negocio del proveedor en la nube (sin ir en contra de los acuerdos de confidencialidad establecidos con los usuarios). Así mismo, se deben integrar a los planes de continuidad y recuperación de la entidad contratante con los planes de continuidad del negocio y recuperación del proveedor. [9]

6.11. Acuerdos de Nivel de servicio (ANS).

Para todos los servicios de informática en la nube se deben establecer acuerdos de nivel de servicio donde se detallen aspectos como: controles, reglamentación, medidas de protección y seguridad, plazos de recuperación del servicio, indicadores y forma de medición de indicadores de calidad del servicio, valores mínimos aceptables, tiempos de respuesta ante una eventual falta de disponibilidad, penalizaciones y el régimen de responsabilidad por daños y perjuicios ocasionados por un incumplimiento del proveedor, limitaciones al servicio o a sus garantías, solicitudes de cambio, gestión de incidentes, regulación de la seguridad y el tratamiento de datos y terminación del servicio/contrato. Se recomienda revisar las fichas técnicas de los Acuerdos Marco de TI, las cuales contienen criterios y niveles de servicio mínimos definidos por el Estado colombiano. [13]

6.12. Reputación y solvencia del proveedor de servicios

Este criterio no solo aplica para servicios de computación en la nube, sino para cualquier servicio o bien a comprar. Se debe revisar la experiencia, la relación con los clientes, la estabilidad financiera del proveedor y su reputación

6.13. Cláusulas de derechos de proveedores y limitación de responsabilidad

Se debe poner especial atención a aquellas cláusulas incluidas en los términos de acceso a los servicios en la nube que puedan otorgar a los proveedores de servicios derechos sobre la información que pueda estar alojada en sus servidores, cualquiera que sea el propósito de ellas. Así mismo, deben examinarse con mucho cuidado las cláusulas de limitación de responsabilidad de los proveedores de los servicios por incumplimiento de las obligaciones esenciales que surgen de la relación de servicios con los usuarios. Tales cláusulas podrían afectar adversamente a los usuarios que trasladen información reservada o confidencial a la nube y a aquellos que puedan experimentar daños resultantes de incumplimientos en los términos de prestación de los servicios, sin embargo, estas cláusulas no impiden la contratación de servicios en la nube. [12] [13].

6.14. Seguridad

Es fundamental reconocer que la seguridad es un aspecto transversal de la arquitectura que abarca todas las capas del modelo de nube [3] descrito en este documento, desde la seguridad física hasta la seguridad de las aplicaciones. Por lo tanto, las preocupaciones de seguridad en la arquitectura de computación en nube no están únicamente bajo el control de los Proveedores de Nube, sino también de los Consumidores de Nube y otros actores relevantes.

Los sistemas basados en la nube todavía necesitan abordar los requisitos de seguridad como autenticación, autorización, disponibilidad, confidencialidad, administración de identidad, integridad, auditoría, monitoreo de seguridad, respuesta a incidentes y administración de políticas de seguridad. Aunque estos requisitos de seguridad no son nuevos, discutimos las perspectivas específicas de la nube para ayudar a discutir, analizar e implementar la seguridad en un sistema de nube [13] [14] [15].

Una forma de ver las implicaciones de seguridad desde la perspectiva del modelo de implementación es el diferente nivel de exclusividad de los usuarios en un modelo de implementación. Una nube privada está dedicada a una organización de consumidores, donde una nube pública podría tener usuarios impredecibles coexistiendo entre sí, por lo que el aislamiento de la carga de trabajo es menos un problema de seguridad que en una nube

pública (se debe considerar que los protocolos de seguridad de estas nubes se encuentran definidos con estándares o buenas prácticas internacionales que aseguran menos problemas de seguridad). Otra forma de analizar el impacto en la seguridad de los modelos de despliegue en la nube es usar el concepto de límites de acceso. Por ejemplo, una nube privada en el sitio puede o no necesitar controladores de límites adicionales en el límite de la red de la organización de consumidor de nube, mientras que una nube privada externalizada tiende a requerir tal protección perimetral en el límite [13] [14] [15].

Hay que hablar de seguridad compartida, ya que el proveedor y el consumidor de nube tienen diferentes grados de control sobre los recursos informáticos de un sistema de nube [17]. En comparación con los sistemas de TI tradicionales, donde una organización tiene control sobre toda la pila de recursos informáticos y todo el ciclo de vida de los sistemas, los proveedores de nube y los consumidores de nube diseñan, construyen, implementan y operan sistemas basados en la nube.

La división del control significa que ambas partes ahora comparten las responsabilidades de proporcionar protecciones adecuadas a los sistemas basados en la nube. La seguridad es una responsabilidad compartida. Los controles de seguridad, es decir, las medidas utilizadas para proporcionar protecciones necesitan ser analizados para determinar qué parte está en mejor posición para implementar. Este análisis debe incluir consideraciones desde la perspectiva de un modelo de servicio, donde diferentes modelos de servicio implican diferentes grados de control entre los proveedores y los consumidores de nube. El proveedor suele realizar controles de administración de cuenta para usuarios privilegiados del sistema inicial en escenarios IaaS, mientras que la administración de cuentas de usuarios de aplicaciones para la aplicación desplegada en un entorno IaaS no es responsabilidad del proveedor [13] [14] [15].

6.15. Privacidad

Los proveedores de nube deben proteger la recopilación, el procesamiento, la comunicación, el uso y la disposición de la información personal y de la información de identificación personal en la nube de acuerdo con la normatividad vigente [17].

De acuerdo con las leyes colombianas de privacidad y tratamiento de datos personales, la información personal puede usarse para distinguir o rastrear la identidad de una persona, como su nombre, servicios parafiscales, registros biométricos etc. Aunque la computación en nube ofrece una solución flexible para recursos compartidos, software e información, también plantea desafíos de privacidad adicionales a los consumidores que usan las nubes.

7. Gobernanza de la Nube

La gobernanza de la nube es un conjunto de reglas y políticas adoptadas por las empresas que ofrecen servicios en la nube. El objetivo de la gobernanza de la nube es mejorar la seguridad de los datos, gestionar los riesgos y permitir el funcionamiento sin problemas de los sistemas en la nube.

La nube facilita más que nunca que los equipos de las entidades desarrollen sus propios sistemas e implementen activos con un solo clic. Si bien esto promueve la innovación y la productividad, también puede causar problemas como:

- Mala integración entre sistemas en la nube, incluso dentro de la misma organización
- Duplicación de esfuerzos o datos entre diferentes partes de la organización
- Falta de alineación entre los sistemas de nube y los objetivos comerciales
- Nuevos problemas de seguridad, por ejemplo, el riesgo de implementar sistemas en la nube con un control de acceso débil o inexistente

La gobernanza de la nube garantiza que la implementación de activos, la integración de sistemas, la seguridad de los datos y otros aspectos de la computación en la nube se planifiquen, consideren y gestionen adecuadamente. Es muy dinámica, porque los sistemas en la nube pueden ser creados y mantenidos por diferentes grupos de la organización, involucrar a proveedores externos y pueden cambiar a diario.

Las iniciativas de gobernanza de la nube garantizan que este entorno complejo cumpla con las políticas organizacionales, las mejores prácticas de seguridad y las obligaciones de cumplimiento.

7.1. Importancia de la gobernanza en la nube

A continuación, se presentan algunas formas en las que la gobernanza de la nube puede beneficiar a una organización que ejecuta servicios críticos en la nube.

- Mejora la gestión de recursos en la nube

La gobernanza de la nube puede ayudar a dividir los sistemas de la nube en cuentas individuales que representan departamentos, proyectos o centros de costos dentro de la organización. Esta es una práctica recomendada por muchos proveedores de servicios en la nube. Separar las cargas de trabajo de la nube en cuentas separadas puede mejorar el control de costos y la visibilidad, y limitar el impacto comercial de los problemas de seguridad.

- Reduce la TI en la sombra

Los riesgos y los costos de los sistemas en la nube aumentan significativamente si la organización no sabe qué sistemas y datos se implementan y dónde. Hoy en día, es muy común que los empleados recurran a sistemas de TI ocultos cuando no obtienen una respuesta rápida de los servicios de TI tradicionales. La gobernanza de la nube permite a los empleados solicitar recursos en la nube de una manera cómoda, pero que aplica los controles y la visibilidad pertinentes para la organización. En lugar de recurrir a TI en la sombra, los empleados pueden recibir acceso a los sistemas en la nube, dentro de las limitaciones presupuestarias y de cumplimiento de la organización.

- Reduce los gastos administrativos

Sin un programa de gobernanza de la nube y soluciones tecnológicas que lo respalden, las organizaciones tienden a utilizar hojas de cálculo u otros procesos manuales para realizar un seguimiento de las cuentas de la nube, los costos y los problemas de cumplimiento, o para controlar el acceso y los presupuestos de los recursos de la nube. Esto es ineficiente, propenso a errores y falla a gran escala. Una solución completa de gobernanza de la nube permite a las organizaciones definir políticas de forma centralizada y aplicarlas a toda la

infraestructura de la nube. Centraliza el control sobre el acceso y los costos, genera alertas y facilita la respuesta ante infracciones. Esto ahorra tiempo y esfuerzo, reduce el riesgo de actividades no conformes y costos inesperados en la nube.

Mejora los problemas de seguridad en la nube

Un modelo de gobernanza de la nube establece una estrategia de autenticación para proteger la confidencialidad, integridad y disponibilidad de la información. Permite a la organización que, sin importar dónde se encuentren los datos o se implementen los sistemas críticos, haya visibilidad de la información confidencial y garantías de que se implementen los controles de seguridad adecuados.

7.2. Principios del modelo de gobernanza de la nube

Los siguientes cinco principios son un buen punto de partida para construir su modelo de gobernanza de la nube:

1. Cumplimiento de políticas y estándares: los estándares de uso de la nube deben ser coherentes con las regulaciones y los estándares de cumplimiento utilizados por su organización y otros en su industria.

2. Alineación con los objetivos empresariales: la estrategia de la nube debe ser parte integral de la estrategia empresarial y de TI general. Todos los sistemas y políticas de la nube deben respaldar de manera demostrable los objetivos empresariales.

3. Colaboración: debe haber acuerdos claros entre los propietarios y usuarios de la infraestructura de la nube y otras partes interesadas en las unidades organizativas pertinentes, para garantizar que hagan un uso apropiado y mutuamente beneficioso de los recursos de la nube.

4. Gestión de cambios: todos los cambios en un entorno de nube deben implementarse de manera consistente y estandarizada, sujetos a los controles adecuados.

5. Respuesta dinámica: la gobernanza de la nube debe basarse en la supervisión y la automatización de la nube para responder dinámicamente a los eventos en el entorno de la nube.

7.3. Como se diseña e implementa un marco de gobernanza en la nube

Los siguientes son los componentes principales de un marco de gobernanza de la nube.

Ilustración 15 Componentes de un marco de gobernanza de la nube

Gestión financiera en la nube

En muchas organizaciones, los costos de la nube se salen rápidamente de control. Los servicios en la nube a menudo prometen reducir los costos de TI, pero esto solo es cierto si los costos se gestionan adecuadamente. Hay tres elementos de la gestión financiera de la nube:

- Políticas financieras que aclaren cómo la organización planea utilizar la nube. Por ejemplo, las políticas pueden definir en qué casos se deben utilizar servicios gestionados para reducir los costos operativos internos o especificar una lista de verificación de gestión de costos que se debe seguir antes de implementar nuevos servicios en la nube.
- Los presupuestos definen la asignación específica para diferentes partes de la organización o diferentes categorías de servicios en la nube.
- Es difícil lograr informes de costos de manera consistente. Algunos servicios en la nube tienen cargos impredecibles que pueden aparecer en diferentes lugares de la infraestructura en la nube; por ejemplo, las instantáneas de la nube que se usan para realizar copias de seguridad se pueden almacenar en diferentes regiones y cuentas. Puede usar herramientas de informes de costos proporcionadas por el proveedor de la nube o adoptar herramientas de terceros que cubran varias nubes.

Gestión de operaciones en la nube

La gestión de operaciones implica definir procesos para la implementación de servicios. Estos procesos deben incluir:

- Una definición clara de los recursos asignados al servicio a lo largo del tiempo
- Acuerdos de nivel de servicio (ANS) para definir el rendimiento esperado
- Monitoreo continuo para garantizar que se cumplan los ANS
- Proceso y comprobaciones necesarias antes de implementar el código en producción

- Requisitos de control de acceso

Una gestión eficaz de las operaciones en la nube es una forma excelente de evitar la TI en la sombra. Puede ahorrar costes al evitar el uso innecesario de recursos en la nube y puede mejorar drásticamente el retorno de la inversión en la nube a largo plazo.

Gestión de datos en la nube

La nube facilita la recopilación y el análisis de grandes cantidades de datos, pero esto hace que la gestión de datos sea un desafío mucho mayor. La gobernanza de la nube debe especificar cómo gestionar todo el ciclo de vida de los datos en la nube. Esto incluye:

- Elaborar un esquema de clasificación de datos y establecer políticas para los datos en diferentes niveles de sensibilidad
- Garantizar que todos los datos estén cifrados, en reposo y en tránsito
- Establecer controles de acceso adecuados para cada tipo de datos
- Uso del enmascaramiento de datos para reducir el riesgo de datos confidenciales cuando se utilizan para escenarios como desarrollo, pruebas o capacitación
- Desarrollar una estrategia de niveles, moviendo datos a lo largo del tiempo desde sistemas de acceso rápido de alto costo a sistemas de archivo de menor costo
- Garantizar que la gestión del ciclo de vida de los datos esté automatizada: esto es fundamental para aplicar políticas en implementaciones de nube a gran escala.

Gestión de la seguridad y el cumplimiento normativo en la nube

La gobernanza de la nube asume la responsabilidad de todos los temas clave de la seguridad empresarial. Determina cuáles son los requisitos de seguridad y cumplimiento de la organización y garantiza su cumplimiento en el entorno de la nube:

- Evaluación de riesgos
- Gestión de identidad y acceso
- Gestión de datos y cifrado
- Seguridad de la aplicación
- Recuperación de desastres

La gobernanza de la nube debe lograr un equilibrio entre los impulsores y requisitos del negocio, los riesgos de seguridad reales y los requisitos de las normas de cumplimiento. Debe utilizar las políticas y prácticas de seguridad existentes, extendiéndolas a la nube y traduciéndolas al entorno de la nube. [22]

8. Formato de auto diagnóstico como actor de la nube

El anexo denominado: "Formato de autodiagnóstico como actor de la nube" debe entenderse e interpretarse como una manera rápida de evaluar si los servicios ofrecidos por un actor determinado de la nube cumplen con lo definido en este documento. Según esto, es necesario que este formato sea diligenciado por los responsables TI de la organización y anexe la documentación necesaria para probar que el servicio ofrecido realmente es un servicio de computación en la nube. La información allí contenida se debe asegurar con la firma del responsable TI y debe ser salvaguardada para los diferentes fines en que pueda ser usada (auditorias, revisiones y demás).

Hay que aclarar que cualquier servicio de computación en la nube debe cumplir con las cinco características esenciales antes descritas, alguno de los tres modelos de servicio y como mínimo desplegado en alguno de los cuatro de implementación. Por lo anterior, si se evita la falta de alguno de estos mediante el formato en cuestión, se entiende que dicho servicio está incompleto y necesita la implementación de soluciones que completen los requisitos para diagnosticarlo satisfactoriamente. También es necesario que la organización asegure la trazabilidad de este formato y los cambios realizados en los servicios de computación en la nube, con el fin de presentar reportes si son requeridos por un auditor de nube o cualquier otra entidad competente.

Este autodiagnóstico está dirigido, por ahora, únicamente a los actores: consumidor y proveedor de nube. El consumidor de nube podrá diligenciarlo para reconocer que el servicio que está contratando con el proveedor sí es un servicio de computación en la nube. En cualquier momento el consumidor de nube podrá informar al proveedor su inconformidad o dudas en cuanto a la prestación del servicio y clasificación del servicio.

El proveedor de nube deberá cumplir los requisitos mínimos del formato, así como también los requisitos mínimos de: gestión del servicio, portabilidad, y seguridad y privacidad [17].

Deberá anexar toda la documentación necesaria asegurando la veracidad de la información en las respuestas dadas. Para los “requisitos a tener en cuenta u opcionales”, el proveedor deberá establecer un plan de trabajo que le permita cumplirlos en el mediano plazo.

Así mismo, no se podrán auto diagnosticar los actores: auditor, corredor y operador de nube. En el caso del auditor y operador: los servicios, aunque son necesarios para garantizar un entorno de alto nivel de computación en la nube, estos no están catalogados dentro de los modelos de servicio, por ejemplo, el servicio de conectividad del operador (redes, internet, redes privadas de transporte de datos entre otros) es necesario para que la computación en la nube sea una realidad, sin embargo, este no es SaaS, PaaS o IaaS. Por lo anterior, buscando tener un nivel de madurez en el tiempo acorde a las capacidades tecnológicas de los actores de la nube citados anteriormente, el Ministerio de TIC ha decidido no clasificarlos. En el caso del corredor o agente de nube, tampoco podrá auto diagnosticarse porque, aunque sus actividades forman parte del modelo de referencia de NIST en una etapa avanzada y madura de la computación en la nube, tampoco se consideran modelos de servicio. En la ruta de definición e implementación de la computación en la nube en Colombia liderada por el Ministerio TIC, se considerarán las normas técnicas y las posibilidades tecnológicas

(incluyendo todos los actores y actividades, estándares, entre otros) de un entorno de alto nivel que aseguren la madurez esperada para los próximos años.

Nota: El auditor de nube, podrá ser una tercera parte (otra organización), o un área funcional del mismo proveedor que presta servicios en la nube. Se deberá asegurar la trazabilidad de las actividades de verificación y/o auditoria buscando así el cumplimiento de los ANS pactados y la mejora continua de los servicios. Así mismo, los servicios de auditoria si bien son necesarios para garantizar un entorno de nube de alto nivel, estos no están catalogados dentro los modelos de servicio antes citados.

9. Lineamientos específicos para la gestión de seguridad en la nube

Para fortalecer la gestión de seguridad en servicios en la nube, se sugiere que las entidades públicas adopten los siguientes lineamientos alineados al control A.5.23 de la norma ISO/IEC 27001:2022:

- Definir controles de seguridad compartida con el proveedor, incluyendo las responsabilidades de cada parte (cliente y proveedor) mediante cláusulas contractuales explícitas.

- Solicitar evidencias técnicas o certificaciones (como ISO/IEC 27001:2022 o 27017) que permitan validar la madurez en seguridad del proveedor sin limitar la pluralidad de oferentes. En caso de no contar con la certificación, se aceptará documentación robusta de políticas y prácticas internas.

- Incluir en el contrato cláusulas sobre la notificación de incidentes, tiempos máximos de respuesta, canales oficiales y niveles de severidad.

- Realizar auditorías o revisiones periódicas al cumplimiento de los controles de seguridad aplicados por el proveedor, incluyendo los servicios en nube bajo el modelo SaaS, PaaS o IaaS.

- Establecer mecanismos de control para la residencia y ubicación de los datos, de forma que se garantice el cumplimiento normativo nacional e internacional sobre protección de datos.

- Implementar políticas para la clasificación de la información previa a su migración a la nube, que definan qué categorías de información pueden o no ser tratadas en entornos externos.

10. Implementación y monitoreo de controles de seguridad en servicios en la nube

Con base en el control A.5.23 de la norma ISO/IEC 27001:2022, las entidades públicas deben establecer una relación clara y controlada con sus proveedores de servicios en la nube, que permita garantizar la seguridad de la información procesada o almacenada en dichos entornos. Para ello, se deberán tener en cuenta las siguientes acciones:

Controles exigidos al proveedor

Definir en los contratos los controles mínimos de seguridad exigibles, tales como: cifrado de datos en tránsito y en reposo, autenticación multifactor, control de accesos privilegiados, trazabilidad, respaldo y recuperación, así como la ubicación geográfica de los datos.

Exigir la presentación de certificaciones vigentes (como ISO/IEC 27001, 27017 o 27018) o documentación equivalente que evidencie un sistema de gestión de seguridad de la información implementado.

Incluir cláusulas sobre la notificación obligatoria de incidentes de seguridad, con tiempos de respuesta establecidos y mecanismos de comunicación definidos.

En concordancia con las mejores prácticas definidas por la ISO/IEC 27017 y los controles de la norma ISO/IEC 27001:2022, toda cuenta con privilegios administrativos o acceso a servicios críticos en la nube deberá contar con mecanismos de autenticación multifactor (MFA). Este requisito aplica tanto a cuentas internas como a las utilizadas por proveedores o terceros autorizados.

Cada entidad definirá el mecanismo técnico más adecuado según sus condiciones, siempre que garantice la validación en dos o más factores independientes (algo que se sabe, algo que se tiene, algo que se es), sin restringir tecnologías o marcas específicas.

Acciones de monitoreo por parte de la entidad

Realizar revisiones periódicas (documentales o técnicas) sobre el cumplimiento de los controles contractuales establecidos.

Solicitar reportes de auditoría externa, resultados de pruebas de seguridad (pentesting o escaneo de vulnerabilidades), y evidencia de implementación de medidas correctivas.

Monitorear continuamente los niveles de servicio relacionados con la disponibilidad, integridad y confidencialidad de la información en la nube, conforme a los SLA definidos.

Establecer mecanismos internos de verificación de seguridad para los servicios cloud críticos, incluyendo herramientas de monitoreo de actividad y acceso.

Este enfoque permite a las entidades mantener el control sobre los riesgos inherentes al uso de servicios en la nube, asegurar el cumplimiento de sus políticas institucionales de seguridad y responder adecuadamente a incidentes, auditorías o requerimientos legales.

11. Referencias

[1] Ministerio de Tecnologías de la Información. Colombia. Marco de Referencia de Arquitectura Empresarial para la gestión de TI [Online]. Disponible: www.mintic.gov.co/arquitecturati.

[2] Microsoft. Azure. ¿Que és el Middleware? [Online]. Disponible: https://azure.microsoft.com/es-es/overview/what-is-middleware/

[3] P. Mell, T. Grance (2011, Sep.), "The NIST Definition of Cloud Computing", Special Publication 800-145, p. 2 [Online]. Disponible: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[4] Working Group members (2013, Jul.), "NIST Cloud Computing Standards Roadmap", Special Publication 500 - 291v2, p. 12-24[Online]. Disponible: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909024 .

[5] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf (2011, Sep.), "NIST Cloud Computing Reference Architecture", Special Publication 500-292, Appendix B: Examples of Cloud Services p. 24-25 [Online]. Disponible: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

[6] Colombia compra eficiente. Acuerdos Marco de TI [Online]. Disponible: https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia.

[7] Mesa Sectorial Cloud Computing (2010), Cloud Computing una perspectiva para Colombia.

[8] Jim Mc Gittigan, Sanil Solanki. The Gartner Top 10 Recommended IT Cost Optimization Ideas, 2016.

[9] Junta de Andalucía. Consejería de economía, Innovación, ciencia y empleo. Cloud Computing. Aplicado a los sectores de agroindustria, eficiencia energética, industrias culturales y turismo. 2012.

[10] Congreso de Colombia. Ley de TIC, 1341 del 30 de Julio de 2009.

[11]Ministerio de Tecnologías de la Información y las comunicaciones. Decreto 1078 de 2017 articulo 2.2. 9.1.1.1. Estrategia de Gobierno Digital (GEL).

[12] SIC (2015), "Protección de los datos personales en los servicios de computación en la nube (Cloud Computing)", [Online]. Disponible: http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf.

[13] Guía para clientes que contraten servicios de Cloud Computing (2013), Agencia Española de Protección de datos.

[14] Cloud Security Alliance (2011). Guía de seguridad de áreas críticas en Cloud Computing. 3.0

[15] Luis Joyanes Agilar. Computación en la nube. Notas para una estrategia española en Cloud Computing.

[16] V. Hernández (2010, Feb.), "El papel del aprovisionamiento de la gestión en la nube", [Online]. Disponible: https://www.ibm.com/developerworks/community/blogs/b35561d9-e0ef-48e0-b455-001f4a64b4da/entry/cloudcomputing?lang=en

[18] SIC Concepto 16-263922 (2016, Nov.),[Online]. Disponible: http://www.sic.gov.co/sites/default/files/normatividad/Concepto_16-263922_0.pdf

[19] Gartner. Gartner IT Glossary > Data Center [Online]. Disponible: https://www.gartner.com/it-glossary/data-center/

[20] Peter Mell. Computación en la Nube – Perspectiva de NIST. Semana de Gobierno Digital. 2017.

[21] Centro Europeo de Postgrados – Fundamentos de Seguridad Cloud e Infraestructuras Industriales. 2023.

[22] Articulo Cloud Governance**,** **https://www.imperva.com/learn/data-security/cloud-governance/**

TIC

Lineamientos de ciberseguridad

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de Contenido

Tabla de Contenido.....261
Lineamientos en ciberseguridad.....262
1. Marco Legal y Político.....262
2. Instituciones Clave.....263
3. La ciberseguridad para todos.....263

Lineamientos en ciberseguridad

El contexto de ciberseguridad en Colombia y el mundo ha evolucionado significativamente en los últimos años, impulsado por el aumento de los riesgos y amenazas cibernéticas, el crecimiento de la digitalización y la necesidad de proteger tanto la infraestructura crítica como los datos personales de los ciudadanos. El país enfrenta diversos desafíos en el ámbito de la ciberseguridad, pero también ha logrado avances importantes en términos de políticas, legislación y cooperación internacional.

1. Marco Legal y Político

Colombia ha avanzado en la creación de un marco normativo y de políticas públicas para abordar los riesgos cibernéticos. Algunas de las iniciativas clave incluyen:

- **Ley 1273 de 2009:** Esta ley establece disposiciones para la protección de la información y la prevención de delitos informáticos, incluyendo fraudes electrónicos, acceso no autorizado a sistemas informáticos y otros crímenes cibernéticos. Aunque la ley es un paso inicial importante, su implementación y actualización se han visto desafiadas por la rapidez con la que evolucionan las amenazas.

- **Ley 1581 de 2012:** Esta ley regula la protección de datos personales en Colombia, estableciendo principios y derechos para la protección de la información personal de los ciudadanos. La Ley 1581 también se complementa con la creación de la Superintendencia de Industria y Comercio (SIC), que supervisa y garantiza el cumplimiento de la normativa en esta área.

- **Política Nacional de Seguridad Digital:** En el CONPES 3854 de 2016, busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.

- **Política Nacional De Confianza Y Seguridad Digital:** En el CONPES 3995 de 2020, establece una estrategia integral para proteger las infraestructuras críticas y mejorar la resiliencia del Estado frente a los riesgos cibernéticos. Este documento orienta la creación de políticas, normativas y mecanismos de protección para los sistemas e información más relevantes a nivel nacional.

- El Decreto 338 de 2022 de Colombia establece nuevas disposiciones para la ciberseguridad y la protección de datos personales en el país, especialmente en lo relacionado con la gestión de incidentes de ciberseguridad y la implementación de políticas para la protección de infraestructuras críticas. Este decreto tiene como objetivo mejorar la resiliencia digital del país, fortalecer la protección de los sistemas informáticos y garantizar la seguridad en el entorno cibernético. Es un desarrollo clave.

2. Instituciones Clave

Varios organismos y entidades colombianas desempeñan un papel importante en el ámbito de la ciberseguridad:

- **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC):** Este ministerio tiene una función central en la formulación de políticas, la promoción de la ciberseguridad y la coordinación de iniciativas nacionales en la materia.

- **CERT Colombia:** El Equipo de Respuesta ante Incidentes de Ciberseguridad (CERT por sus siglas en inglés) es un organismo clave en Colombia que proporciona soporte técnico y coordina la respuesta ante incidente

3. La ciberseguridad para todos

La ciberseguridad y las crecientes dinámicas en el ciberespacio presentan cada vez más desafíos para Colombia. En ese sentido, para que la ciberseguridad esté al alcance de la población, se requieren mecanismos y buenas prácticas que sirven para la protección de IT y OT, en aras de salvaguardar la seguridad y privacidad al momento de navegar por la red.

La ciberseguridad requiere el seguimiento del modelo, el cuidado de los dispositivos, y los consejos más básicos, es relevante comprender que no se requiere grandes conocimientos técnicos, de redes o de equipos, por el contrario, la ciberseguridad es un modelo para todos.

En el presente anexo se entregan las guías básicas en ciberseguridad para poner en marcha el modelo de seguridad y privacidad de la información. Este sistema está compuesto por la identificación de activos críticos, infraestructuras críticas, la guía de gestión de incidentes y la guía de gestión de riesgos. Esta propuesta está concebida para integrar la ciberseguridad bajo un modelo que permita la gestión y anticipación de las afectaciones cibernéticas.

TIC

Lineamiento para la identificación de las infraestructuras críticas cibernéticas

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	Observaciones
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de Contenido

Tabla de Contenido 266
Lineamiento para la identificación de las infraestructuras críticas cibernéticas 267
Resumen ejecutivo 267
Introducción 267
1. Normativa 268
2. Normativa Internacional 269
3. Algunos sectores y subsectores con alta criticidad 271
4. Antecedentes de las Infraestructuras Críticas y su metodología en Colombia 272
5. Roles y responsabilidades con la Ciberseguridad y Ciberdefensa de la infraestructura crítica cibernética: 275
6. Sectores Críticos Nacionales 2024 278
7. Amenazas y Riesgos a la infraestructura crítica digital 280
8. Derechos comprometidos por las ICC. 282
9. Casos comparados: Metodología Infraestructura Crítica Cibernética 283
10. Metodología para identificación de ICC en Colombia 286
11. Definición de las variables y explicación en la metodología: 293
12. Actualización en la metodología: 299
13. Orientación 301
14. Fuentes 309
15. ANEXOS: 310

Listado de Tablas

Tabla 21 Sectores y sus responsables 276

Tabla de ilustraciones

Ilustración 21 Comparativo de metodología de ICC internacional 286
Ilustración 22 Interdependencia de Infraestructura Crítica Cibernética de Estados Unidos 287
Ilustración 23 Interdependencia de infraestructura Crítica Cibernética de Colombia 288
Ilustración 24 Paso 3 identificación de ICC 299

Lineamiento para la identificación de las infraestructuras críticas cibernéticas

Resumen ejecutivo

Las infraestructuras críticas son los sistemas físicos y virtuales esenciales que forman la espina dorsal de nuestras sociedades modernas, sirviendo de sustento para el bienestar de la sociedad en funcionamiento. Cualquier daño o interrupción de las infraestructuras críticas puede tener importantes repercusiones negativas para la seguridad de la nación. A menudo, estos sistemas se extienden más allá de las ciudades y prestan servicios a regiones enteras. En el mundo conectado de hoy, a medida que aumenta la interconexión de nuestros sistemas que son vitales para nuestra cotidianidad, también lo hacen las amenazas a las infraestructuras críticas abarcan un amplio abanico de sectores como la energía, las comunicaciones, las telecomunicaciones, el transporte, los sistemas financieros, la sanidad, el suministro de alimentos y numerosos servicios gubernamentales, estos servicios son esenciales para la vida cotidiana de los colombianos.

Dada su importancia, la protección de las infraestructuras críticas frente a posibles amenazas es una prioridad absoluta para todos los gobiernos y organizaciones del mundo. A medida que aumenta la interconexión de nuestros sistemas, también lo hacen las amenazas que son tan vitales para nuestra vida cotidiana. Estas amenazas pueden adoptar la forma de ciberataques, catástrofes naturales, sabotaje físico o muchos otros peligros. Aunque Colombia no ha dispuesto una guía oficial del “paso a paso" para la identificación de Infraestructuras Críticas, sí tenemos lecciones aprendidas de otros Estados y un trabajo de ministerio de defensa nacional que pueden ayudar mejor al establecimiento de los lineamientos para la identificación de Infraestructuras Críticas Cibernéticas.

Introducción

La norma ISO IEC 27001 hace referencia al sistema de seguridad de la información la cual incluye infraestructura crítica física, personas, información física e información digital. Así las cosas, cada uno de los elementos que conforman cada uno de estos enunciados pueden ser críticos en los casos en que se comprometa un servicio esencial para la sociedad, cuya afectación podría tener consecuencias devastadoras en la seguridad, economía, salud o bienestar de la población. Esto incluye sectores como energía, agua, transporte, salud y telecomunicaciones entre otros.

De este modo, esta guía contempla el paso a paso para la identificación critica cibernética la cual abarca los sistemas informáticos y redes que son fundamentales para el funcionamiento de la infraestructura crítica. Esto incluye servidores, bases de datos, redes de comunicación y sistemas de control industrial. La seguridad de esta infraestructura es

vital, ya que un ciberataque puede paralizar servicios esenciales y comprometer la seguridad nacional.

Englobando aquellos activos y servicios esenciales que sostienen la vida, la seguridad y el bienestar de la sociedad. Siendo la base sobre la que se construye la economía, la atención médica, la educación, la seguridad pública y muchos otros aspectos de la vida cotidiana.

En el caso de la infraestructura digital, es esencial para la seguridad nacional debido a su papel fundamental en la gestión y control de servicios críticos como el suministro de energía, el transporte y la comunicación. Sumado a la información gubernamental, financiera y personal sensible que alberga. De modo que, un ataque cibernético a la infraestructura crítica puede implicar afectaciones políticas, económicas, políticas, ambientales, entre otras, en un Estado.

Por ejemplo, un ataque cibernético puede afectar el suministro de energía eléctrica, interrumpir el transporte, causar interrupciones en las comunicaciones o afectar la prestación de servicios de atención médica. Afectando la movilidad de las fuerzas de seguridad o la capacidad del gobierno para responder a una crisis.

Por lo que la validación de los sectores y subsectores estratégicos de la infraestructura crítica es importante para la identificación y priorización de los activos y servicios críticos esenciales para el funcionamiento de la sociedad y la seguridad nacional. Lo que permite una mejor coordinación y colaboración entre las entidades públicas y privadas, así como una mayor capacidad de respuesta y resiliencia en caso de un evento disruptivo o una amenaza de seguridad.

Ambas infraestructuras requieren protección y resiliencia ante amenazas, tanto físicas como cibernéticas, y son objeto de atención por parte del gobierno y el sector privado para asegurar su funcionamiento interrumpido y su protección contra incidentes. En este contexto, este documento pretende proporcionar un marco de referencia teórico para identificar, validar y gestionar los sectores y subsectores estratégicos de la infraestructura crítica cibernética, especialmente en lo relativo a la ciberseguridad y el sector IT/OT.

En ese sentido, se toman documentos como “Cybersecurity and Infrastructure Security Agency (CISA), titulado “A Guide to Crítical Infrastructure Security and Resilience CISA 2019” de Estados Unidos.

Además, el documento incluye casos de estudio y la base teórica de metodologías internacionales que amplían la perspectiva sobre la infraestructura crítica y su importancia para la seguridad nacional. Se presentan los casos de estudio de Reino Unido, Estados Unidos, Estonia y Canadá, así como la metodología ENISA para la identificación de activos y servicios de Infraestructura de Información Crítica.

1. Normativa

En el presente estudio se han tenido como fundamento algunas normativas que establecen lineamientos generales tendientes a identificar los diferentes sectores vulnerables en las infraestructuras críticas, tales como, el artículo 333 de la Constitución Política de Colombia[15],

[15] Constitución Política de Colombia, artículo 333, (1991).

el cual define la empresa, como base del desarrollo económico del país, el artículo 365 de la Constitución Política de Colombia[16], que determina como finalidad social del Estado la prestación de los servicios públicos, dentro de los cuales, la Corte Constitucional en Sentencia C-691/08, ha declarado

que servicios como la banca central; el transporte; las telecomunicaciones; la explotación, refinación, transporte y distribución de petróleo y los servicios públicos domiciliarios, son materialmente servicios públicos esenciales, lo que eleva el grado de necesidad y vulnerabilidad al que pueden estar expuestos.

Por otro lado, el Consejo Nacional de Política Económica y Social, estableció mediante el Conpes 3995 de 2020, la Política Nacional de Confianza y Seguridad digital y definió como Infraestructura crítica cibernética nacional, aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado.

Ahora bien, con base en lo anterior y teniendo en cuenta el principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009[17] "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las Comunicaciones - "TIC-,(...)", y debido a la imposición que tienen las entidades públicas de adoptar las medidas necesarias que les permitan garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones, el Ministerio de Tecnologías de la Información y las Comunicaciones, determinó mediante el Decreto 1078 de 2015 adicionado por Decreto 338 de 2022, la necesidad de definir la metodología para realizar el levantamiento del inventario de infraestructuras críticas cibernéticas y de servicios esenciales a cargo de las autoridades, así como, la incorporación de mejores prácticas que le sean aplicables.

2. Normativa Internacional

DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea. Establece respecto a infraestructuras con alto nivel de criticidad que:

- Las entidades incluidas en el ámbito de aplicación de la presente Directiva para gestionar riesgos de ciberseguridad deben clasificarse en dos categorías, entidades esenciales e importantes, según el grado de criticidad de sus sectores o del tipo de servicio que prestan, y de su tamaño.

- Deben considerarse debidamente las evaluaciones de riesgos sectoriales o las orientaciones de las autoridades competentes.

[16] Constitución Política de Colombia, artículo 365, (1991).
[17] Ley 1341 de 2009, Congreso de Colombia.

- Se han de diferenciar los regímenes de supervisión y de garantía del cumplimiento de las dos categorías de entidades para garantizar un equilibrio justo entre los requisitos y las obligaciones en función del riesgo.

- Los Estados miembros deben exigir a las entidades que presenten, al menos, la siguiente información a las autoridades competentes, a saber, el nombre, la dirección y los datos de contacto actualizados, incluidas las direcciones de correo electrónico, los rangos de IP y los números de teléfono de la entidad, y en su caso, el sector y subsector pertinente contemplados en los anexos, así como en su caso, una lista de los Estados miembros en los que prestan servicios incluidos.

- Cuando las disposiciones de un acto sectorial de la Unión exijan a las entidades esenciales o importantes que cumplan obligaciones de notificación de efecto al menos equivalente a las obligaciones de notificación establecidas en la presente Directiva, deben garantizarse la coherencia y la eficacia de la tramitación de las notificaciones de incidentes.

- Las disposiciones del acto sectorial de la Unión sobre notificación de incidentes deben proporcionar a los CSIRT, autoridades competentes o puntos de contacto únicos sobre ciberseguridad, designados con arreglo a la presente Directiva acceso inmediato a las notificaciones de incidentes presentadas de conformidad con el acto jurídico sectorial de la Unión.

- Los Estados miembros deben establecer un mecanismo de notificación automática y directa que garantice un intercambio sistemático e inmediato de información con los CSIRT, las autoridades competentes o los puntos de contacto únicos en relación con la tramitación de dichas notificaciones de incidentes sectoriales.

- Las entidades del sector de las infraestructuras digitales se basan en sistemas de redes y de información, por lo que las obligaciones impuestas a dichas entidades por esta Directiva deben abordar de manera exhaustiva la seguridad física de estos sistemas como parte de sus medidas para gestionar los riesgos de ciberseguridad y obligaciones de notificación.

- La Directiva reconoce las crecientes interdependencias son el resultado de una red cada vez más transfronteriza e interdependiente de prestación de servicios que utilizan infraestructuras clave de toda la Unión en sectores como la energía, el transporte, la infraestructura digital, el agua potable y las aguas residuales, la sanidad y determinados aspectos de la administración pública, así como el espacio en la medida en que se trate de la prestación de determinados servicios que dependen de infraestructuras terrestres.

3. Algunos sectores y subsectores con alta criticidad

Acorde al estudio preliminar se presentan algunos de los sectores y subsectores[18] con alta criticidad, estos, probablemente se actualicen con el levantamiento de la infraestructura crítica cibernética del Estado:

1. Energía

1.1 Electricidad

1.2 Sistemas Urbanos de calefacción y refrigeración

1.3 Crudo

1.4 Gas

1.5 Hidrogeno

2. Transporte

2.1. Transporte aéreo

2.2. Transporte por Ferrocarril

2.3. Transporte Marítimo
2.4. Transporte por carretera

3. Financiero

3.1 Infraestructuras de los mercados financieros

3.2 Sector sanitario

3.3 Agua potable

3.4 Aguas residuales

4. TIC

4.1 Infraestructura digital

4.2 Gestión de servicios de TIC (de empresa a empresa)

5. Estado

5.1 Entidades de la Administración pública, con exclusión del poder judicial, los parlamentos y los bancos centrales

Por consiguiente, esto es solo un ejemplo del alcance del documento, el cual tiene como objetivo exponer un análisis motivado en unos parámetros normativos que enuncian de forma general aquellas infraestructuras críticas cibernéticas y por otro lado la definición y

[18] Esto es una referencia, la criticidad de los sectores se determina con la nueva metodología. Del mismo modo, en esta se procura por la identificación de los subsectores.

el reconocimiento que se han dado de las mismas en el ámbito nacional e internacional con el fin de brindarles las herramientas precisas que conlleven asegurar la efectividad en la implementación de la metodología de las infraestructuras críticas cibernéticas y el uso de las buenas prácticas en seguridad digital.

Del mismo modo, se plantea que el levantamiento de la Infraestructura crítica Cibernética se realizará por fases:

1. **Primera fase:** Levantamiento de Infraestructura Crítica Cibernética y clasificación de la criticidad en los sectores. (Se identifican los subsectores a nivel general)

2. **Segunda fase:** Levantamiento de la Infraestructura Crítica Cibernética en los Subsectores e identificación de los operadores.

3. **Tercera Fase:** Levantamiento de la Infraestructura Crítica Cibernética de los operadores.

La propuesta se actualizará cada 02 años, y se procura por partir de lo general a lo particular, estableciendo los principales riesgos y amenazas sobre la Infraestructura Crítica Cibernética.

4. Antecedentes de las Infraestructuras Críticas y su metodología en Colombia

Algunos países han adoptado una estructura similar de sectores críticos, como la utilizada por los Estados Unidos, hay diferencias en la forma en que se agrupan los subsectores y la forma en que se gestionan los riesgos y amenazas específicas de cada sector. En Colombia, esta información se empieza a desarrollar con la primera versión del Catálogo Nacional de Infraestructuras Críticas Cibernéticas V1.0 [1].

Esta nace con el propósito de definir los sectores estratégicos de Colombia, para realizar la identificación de la infraestructura crítica cibernética del país, en el marco del manejo de riesgo operacional nacional, la ciberseguridad y la ciberdefensa y en su momento estas actividades lideradas por el comando conjunto cibernético coordinación con el equipo de respuesta a emergencias cibernéticas de Colombia quien hacia parte del ministerio de defensa nacional.

En ese sentido, se procedió a la construcción de un documento que serviría como referencia a todas las entidades publico privadas o de economía mixta que cuente con infraestructura de tecnologías de información de comunicaciones o tecnologías de operación.

El 31 de octubre de 2012 se activa con el primer congreso de ciberseguridad llevado a cabo en las instalaciones del hotel capital en Bogotá y con la creación del Comando Conjunto Cibernético de las Fuerzas Militares, y cumpliendo con lo dispuesto en el documento CONPES 3701 de 2011 en donde se debía realizar con el COLCERT la identificación y taxonomía de las infraestructuras críticas cibernéticas en Colombia.

Con la autorización del ministerio de defensa en donde se encontraba la dirección del COLCERT, se procedió a realizar la primera fase para que el Comando Conjunto Cibernético de las Fuerzas Militares realice la convocatoria de los responsables y dueños de las infraestructuras críticas cibernéticas para iniciar con las reuniones pertinentes. Así pues, se realizó una lista de contactos y un inventario de estas y fijar

unos criterios de periodicidad de las reuniones hasta culminar el proceso de realizar la identificación y elaborar una cartilla de los sectores de infraestructura crítica cibernética que existen en Colombia.

Así mismo se realizó el cronograma de reuniones una por mes y se definió en el cronograma anual el cual era aprobado por los mismos participantes en las reuniones de infraestructuras críticas cibernéticas.

Teniendo en cuenta los puntos anteriores de organización se desarrollaron las mesas de infraestructura críticas cibernéticas, en ellas se empezó a trabajar en la metodología. Es importante resaltar que inicialmente asistieron gran número de sectores entre otros COLCERT, Isagen, Bancolombia, Universidad de los Andes, Empresas Públicas de Medellín, Instituto Tecnológico De Medellín, Asobancaria, Banco Bilbao Vizcaya Argentaria, Ministerio De Comunicaciones, Ministerio De Justicia, Diferentes Empresas Del Sector De La Tecnología, Isa, Registro Único de Tránsito, Acueducto Bogotá, Departamento Nacional de Planeación, Pacific Rubiales, Davivienda, Banco De La República, Presidencia De La Republica CSIRT-Gobierno, Ecopetrol, Aeronáutica Civil, XM, entre otros.

La taxonomía en Colombia, para este estudio se realizó tomando como referencia la metodología aplicada por la Unión europea para la identificación de la taxonomía en el país estableciendo los niveles y subniveles de categorización de la infraestructura colombiana de forma jerárquica basado en sectores y subsectores.

Los 13 sectores elegidos se basan en la propuesta del Catálogo Nacional de Infraestructura Crítica Cibernética (CNICC), el cual fue un estudio realizado en 2015 a una muestra de más de 90 empresas e instituciones del sector público, privado y mixto, con el fin de determinar el listado priorizado de instituciones, entidades y empresas que ostentan la responsabilidad de garantizar el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos y la defensa nacional.

Dicho catálogo en su primera versión fue el resultado de treinta y siete (37) meses de trabajo continuo del Ministerio de Defensa Nacional en coordinación con otros ministerios, y con la participación de varias empresas e instituciones representativas de los sectores público, privado, la academia y la sociedad civil a fin de garantizar, se contara una visión y un análisis holístico y complementario para estudiar los sectores estratégicos del país que cuentan con oportunidades de desarrollo, consolidación y brindan un aprovechamiento a través de plataformas tecnológicas de información o de operación y mantienen potencialidades de crecimiento sustentable en el largo plazo y la posterior identificación de Infraestructura Crítica Cibernética (ICC).

Estos sectores seleccionados se basan en el estudio ya realizado de “los sectores Estratégicos de la República de Colombia desde la óptica Cibernética”: el cual en 2015 estableció los trece sectores de estudio en los cuáles se aplicará la actualización metodológica de la ICC del país y el impacto que tiene el componente cibernético y el ciberespacio en la prestación de los servicios esenciales a la población en cada uno de los

sectores. En este sentido, los 13 sectores nacen del trabajo ya realizado, y son los que serán adoptados por la propuesta de metodología que se actualiza para 2024.

1. Alimentación Y Agricultura

2. Agua

3. Comercio, Industria, Turismo

4. Defensa

5. Educación

6. Electricidad

7. Financiero

8. Gobierno/Estado

9. Recursos Naturales-Medio Ambiente

10. Recursos Minero-Energéticos

11. Salud Y Protección Social

12. Tecnologías De La Información Y Comunicaciones

13. Transporte

Durante el desarrollo de las mesas de trabajo se realizó una clasificación por sectores, la cual dio la elaboración del borrador de la guía para la definición de infraestructuras críticas digitales en Colombia, entre los años 2013, 2014, 2015 y finalizando el 2016 se cumplió con la elaboración de la cartilla en donde se definieron los 13 sectores de infraestructura crítica para Colombia**.**

Es importante anotar que, en el trabajo realizado, las mesas identificaron, priorizaron y catalogaron las infraestructuras críticas digitales y así mismo se determinó que las IC eran interdependientes, complementarias y heterogéneas entre las mismas, conceptos que se llevaron a cabo gracias a la metodología empleada.

En conclusión, el trabajo del primer catálogo fue el desarrollo del trabajo de Infraestructuras críticas cibernéticas que se realizó desde 2016 y es la base de la actualización metodológica que aborda el presente documento.

5. Roles y responsabilidades con la Ciberseguridad y Ciberdefensa de la infraestructura crítica cibernética:

Los roles y responsabilidades en cuanto a la seguridad digital (ciberseguridad) y ciberdefensa de la infraestructura crítica cibernética pueden variar entre países, y esto depende del contexto y la estructura de gobernanza de cada país. En algunos países, la responsabilidad de la protección de la infraestructura crítica puede estar centralizada en una entidad específica, como un departamento de seguridad nacional o un organismo regulador. En otros, las responsabilidades pueden ser compartidas entre varias entidades, incluidos los sectores público y privado.

En el caso de Colombia, se reconoce que, aunque la Ciberseguridad y Ciberdefensa son responsabilidad de todos, cada uno de los trece sectores debe contar con un delegado visible, en ese sentido se plantea que el líder de cada sector sea el oficial de seguridad o el jefe de la oficina de TI quienes son los encargados de supervisar, coordinar y garantizar la seguridad, continuidad y eficiencia de un conjunto de servicios o sistemas esenciales para el funcionamiento del sector, asegurando su

información; así pues, esto se alinea a los mismos representantes del Comité Nacional de Seguridad Digital.

Igualmente, se requiere que cada sector cree un buzón de correo con la siguiente estructura seguridad.ciber@entidad.gov.co ejemplo: (seguridad.ciber@mintic.gov.co), esto para mantener una comunicación fluida y generar mayor sinergia:

Sector	Representante del Sector	Usuario/Contacto
1) Alimentación Y Agricultura	Ministerio de Agricultura	
2) Agua	Ministerio de Ambiente	
3) Comercio, Industria y Turismo	Ministerio de Comercio, Industria y Turismo	
4) Defensa	Ministerio de Defensa	
5) Educación	Ministerio de Educación	
6) Electricidad	Ministerio de Minas y Energías	
7) Financiero	Ministerio de Hacienda	
8) Gobierno/Estado	Presidencia de la República/Función Pública	
9) Recursos Naturales-Medio Ambiente	Ministerio de Ambiente	
10) Recursos Minero-Energéticos	Ministerio de Minas y Energía	

Sector	Representante del Sector	Usuario/Contacto
11) Salud Y Protección Social	Ministerio de Salud y Protección Social	
12) Tecnologías De La Información Y Comunicaciones	Ministerio TIC	
13) Transporte	Ministerio de Transporte	

Tabla 21 Sectores y sus responsables

Fuente. Construcción Propia

La entidad líder encargada de la gestión de la Infraestructura Crítica Cibernética (ICC) es clave para coordinar y supervisar las acciones relacionadas con la protección de las infraestructuras críticas del sector. A continuación, se detallan las características, roles y funciones de dicha entidad líder:

Características de la Entidad Líder de ICC del sector.

- La entidad debe tener un mandato legal claro y la autoridad necesaria para establecer y hacer cumplir políticas y regulaciones de ciberseguridad.
- Debe contar con los recursos técnicos y humanos necesarios para desarrollar e implementar estrategias de ciberseguridad a nivel de las entidades del sector.
- Capacidad para coordinar y colaborar eficazmente con otras entidades gubernamentales, el sector privado y organizaciones internacionales.
- Compromiso con la transparencia en sus operaciones y la responsabilidad en la gestión de la seguridad cibernética.

Roles de la Entidad Líder de ICC del sector.

- Actuar como la entidad reguladora que establece normas y supervisa su cumplimiento en materia de seguridad cibernética.
- Funcionar como el centro de coordinación para la respuesta a incidentes cibernéticos a nivel de las entidades del sector.
- Promover la colaboración y el intercambio de información entre diferentes sectores y actores relevantes.
- Proporcionar recursos, apoyo técnico y capacitación a las entidades del sector para mejorar sus capacidades de ciberseguridad.
- Realizar evaluaciones periódicas de los riesgos cibernéticos a nivel de las entidades del sector y proporciona directrices para la mitigación de estos riesgos.

Funciones de la Entidad Líder de ICC del sector

- Desarrollar y actualizar políticas, normas y guías de ciberseguridad para la protección de infraestructuras críticas, asegurando que estas políticas sean adoptadas por las entidades del sector.

- Establecer criterios y participar en la creación o adaptación de metodologías para la identificación y clasificación de infraestructuras críticas cibernéticas, manteniendo un registro actualizado de las infraestructuras críticas a de las entidades del sector.

- Realizar evaluaciones de riesgo a nivel de las entidades del sector para identificar amenazas y vulnerabilidades que puedan afectar a las infraestructuras críticas, desarrollando estrategias y planes de mitigación de riesgos.

- Establecer un monitoreo de ciberseguridad para detectar y responder a incidentes cibernéticos, coordinando la respuesta a incidentes a nivel de las entidades del sector, incluyendo la comunicación y colaboración con entidades afectadas y otros actores relevantes.

- Desarrollar programas de capacitación en ciberseguridad para las entidades del sector, mediante campañas de concientización sobre la importancia de la seguridad cibernética y las mejores prácticas.

- Facilitar la colaboración y el intercambio de información entre entidades gubernamentales, el sector privado y organizaciones internacionales, facilitando la realización de foros y grupos de trabajo de ciberseguridad a nivel sectorial e internacional.

- Proporcionar retroalimentación y apoyo para mejorar las prácticas de ciberseguridad en las entidades del sector.

- Propender por la inversión en el desarrollo y mantenimiento de infraestructuras tecnológicas avanzadas para la protección de infraestructuras críticas en las entidades del sector.

- Fomentar la investigación y desarrollo en ciberseguridad para estar a la vanguardia de las tecnologías y amenazas emergentes en las entidades del sector.

Es importante indicar que la entidad líder de ICC del sector juega un papel fundamental en la protección de la infraestructura crítica cibernética del sector,

asegurando que las entidades del sector cuenten con el apoyo, la orientación y los recursos necesarios para enfrentar las amenazas cibernéticas de manera eficaz.

Del mismo modo, es preciso establecer algunos roles y responsabilidades específicas que permitan armonizar los planes y estrategias previstas para tal fin [2]:

a. Gobierno: Ser referente y modelo a seguir en el buen uso del ciberespacio y en la aplicación de las buenas prácticas en Ciberseguridad y Ciberdefensa.

- El Equipo de Respuesta a Emergencias Cibernéticas COLCERT, responsable de la coordinación nacional en materia de gestión de incidentes y seguridad digital.

b. Sector Público: Liderar política pública y establecer el MSPI así como alinear un modelo para protección y defensa para las Infraestructuras Críticas Cibernéticas; bajo altos esquemas de Ciberseguridad y Ciberdefensa para las infraestructuras críticas y la sociedad en general.

c. Empresas Privadas y Mixtas: Adoptar y tomar medidas de operadores alineados una conciencia y cultura de Ciberseguridad, así como adoptar el MSPI y las políticas y guías para dar respuesta ante afectaciones a la seguridad digital. Este actor es fundamental, ya que no solo debe cumplir el MSPI, sino debe articularse con el sector público.

d. Propietarios y/o Operadores de Infraestructura Crítica Cibernética: Trabajar de la mano con las autoridades de Ciberseguridad y Ciberdefensa, así como desarrollar y aplicar planes de protección y defensa.

e. Sector Defensa:

- **El Comando Conjunto Cibernético (CCOCI):** Será responsable de la Ciberdefensa Nacional.

- **El Centro Cibernético Policial de la Ciberseguridad Ciudadana:** Quienes trabajarán de manera coordinada a fin de focalizar esfuerzos y minimizar los riesgos cibernéticos que puedan afectar la Seguridad y Defensa Nacional.

f. Agencias de Inteligencia: Fortalecer las capacidades de inteligencia y contrainteligencia en el ciberespacio para proteger los derechos y libertades de los ciudadanos y de las personas residentes en Colombia, así como identificar oportunidades y riesgos, al igual que identificar, conocer y contrarrestar amenazas internas o externas contra el bienestar de los colombianos, la vigencia del régimen democrático, el orden constitucional y legal, la seguridad y la defensa nacional.

g. Academia y Centros de Investigación: Fortalecer la capacitación en Ciberseguridad y Ciberdefensa a todo nivel.

h. Agremiaciones: Gestionar con sus asociados la aplicación de buenas prácticas y medidas de Ciberseguridad y Ciberdefensa.

6. Sectores Críticos Nacionales 2024

1. **Sector:** Alimentación y agricultura

En Colombia, hoy, esto se refiere a todas las actividades agropecuarias como alimentos, piensos, ganado y técnicas para la cría. Colombia es uno de los principales productores de café, aceite de palma y caña de azúcar del mundo. Se espera que el mercado agrícola colombiano crezca un 7% para 2028, totalizando alrededor de 14 mil millones de dólares.

2. **Sector:** Agua

a. Colombia posee actualmente algunos de los mayores depósitos de recursos de agua dulce del mundo. La capacidad de suministrar agua potable limpia y segura es una estructura crítica para una sociedad sana y productiva.

3. Sector: Comercio, Industria y Turismo

a. Colombia sigue fomentando ser un destino líder para los viajes internacionales y un socio cada vez más vital para la inversión del sector privado. El crecimiento económico

del comercio ha visto un aumento en varios sectores en Colombia, permitiéndole ser un exportador e importador de varios productos a través del mundo.

4. **Sector:** Defensa

a. La industria de Defensa se compone de varios sectores interconectados, como el tecnológico, el financiero y el comercial. Este sector ayuda a posibilitar actividades de investigación y desarrollo en varios sectores. El Ministerio de Defensa es el principal organismo gubernamental de este sector y está compuesto por el Ejército Nacional, la Armada, la Fuerza Aéreo Espacial colombiana y la Policía Nacional.

5. **Sector:** Educación

a. El Sector Educativo es la base para proporcionar habilidades relevantes, así como un camino hacia futuras oportunidades para los ciudadanos de toda Colombia. La capital cuenta con más de 30 universidades que reciben candidatos de todo el mundo. El Ministerio de Educación esbozó áreas clave para que Colombia sea "El país con más educación de América Latina en 2025".

6. **Sector:** Electricidad

a. La gran mayoría del sector eléctrico en Colombia se genera a través de energía hidroeléctrica y térmica. Este sector depende en gran medida de los socios del sector privado para trabajar con los organismos gubernamentales en el suministro de energía fiable a la red crítica nacional. La mayor parte de esta energía se utiliza para el consumo residencial e industrial.

7. **Sector:** Financiero

a. El sector financiero es una parte clave del buen funcionamiento de la sociedad. Los ataques o compromisos al sector financiero pueden debilitar las funciones críticas nacionales de Colombia.

8. **Sector:** Gobierno/Estado

a. El sector público ayuda a las distintas partes interesadas a comprender mejor los riesgos de sus carteras específicas. El sector gubernamental incluye entidades del sector público y entidades descentralizadas a nivel departamental, municipal y verdal que se apoyan en una fuerte asociación para asegurar mejor sus sistemas.
b. En este sector se encuentran los organismos de control, la rama legislativa, judicial, los concejos distritales y municipales y organismos de control como Procuradurías, veedurías, personerías, contralorías, etc.

9. **Sector:** Recursos Naturales-Medio Ambiente

a. El sector de Medio Ambiente y de manejo de recursos naturales resulta extremadamente importante para las Funciones Críticas Nacionales. Siendo Colombia uno de los países con mayor biodiversidad del mundo, este sector proporciona una gran riqueza de recursos al desarrollo estatal.

10. **Sector:** Recursos Minero-Energéticos

a. **El sector minero-energético** se compone de diversas industrias productoras de energía como el sector minero y de extracción de metales, y la industria de petróleo y gas. Este sector actúa como multiplicador de la Economía nacional, ya que en el

país para el 2021 se tuvieron exportaciones de petróleo crudo de 26%, de carbón de 12% y de oro de 6.14%.

11. **Sector:** Salud y Protección Social
a. Los sectores de Salud y Protección Social prestan un servicio crítico para proteger el bienestar y la salud de todos los sectores de la economía. Están preparados para apoyar cualquier amenaza natural, humana o terrorista contra la población de Colombia.
b. La pandemia de COVID-19 ilustró cómo la salud y la seguridad de la población de un país son fundamentales para su funcionamiento cotidiano. El sector sanitario depende en gran medida de las relaciones intersectoriales para asegurar mejor sus infraestructuras críticas.

12. **Sector:** Tecnologías de la información y comunicaciones
a. Cada vez son más los países que digitalizan sus numerosos sectores, por lo que nunca ha sido tan importante proteger estas infraestructuras críticas de los malos agentes y las amenazas.
b. La dependencia de las tecnologías de la información es cada vez mayor a medida que nos interconectamos. Las interdependencias inherentes al sector de las tecnologías de la información han creado retos únicos en materia de protección, pero también nuevas oportunidades de colaboración.

13. **Sector:** Transporte
a. El sector del transporte asiste a millones de colombianos que viajan por el país cada día, y a bienes y servicios económicos, como petróleo, productos agrícolas, café y madera.
b. El sector del transporte es una función crítica nacional que, si se interrumpe, tendrá amplias repercusiones en otros sectores interconectados como la salud y la seguridad, el comercio, la tecnología y la defensa.

Ahora bien, de acuerdo con el decreto 338 de 2022, el Ministerio de Tecnologías de la Información y las Comunicaciones convoca a cada uno de los sectores catalogados como titulares de infraestructura crítica cibernética o de servicios esenciales dentro del presente documento, para que designen un representante, quien será presentado como tal, mediante escrito dirigido al Ministerio de tecnologías de la información y las comunicaciones y el Comité Nacional de Seguridad Digital antes del 30 de agosto de 2024, para luego ser convocado en las mesas sectoriales de Infraestructuras Críticas Cibernéticas - ICC que se realizaran con ocasión a la verificación y seguimiento del levantamiento de las ICC.

7. Amenazas y Riesgos a la infraestructura crítica digital

La Cuarta Revolución Industrial, caracterizada por la convergencia de tecnologías digitales, físicas y biológicas, ha traído consigo avances sin precedentes. Sin embargo, esta transformación digital también ha introducido amenazas y riesgos nuevos y complejos que requieren seria atención.

Entre las amenazas y riesgos específicos figuran los relacionados con la Inteligencia Artificial, las comunicaciones 5G, la analítica de datos y el Big Data, y otras tecnologías emergentes. Los sesgos algorítmicos en los sistemas de IA pueden perpetuar y amplificar los sesgos existentes, dando lugar a decisiones injustas y discriminatorias. El desarrollo de sistemas de armas autónomas también plantea graves problemas éticos y de seguridad.

Además, la automatización que permite la IA puede desplazar a un número significativo de trabajadores, alimentando el desempleo y la desigualdad (The Fourth Industrial Revolution, 2017). El auge de los «deepfakes» -contenidos falsos de gran realismo- puede manipular la opinión pública y socavar la confianza en las instituciones (Konina, 2021)(Velarde, 2020)(Agbaji et al., 2023).

El aumento de la conectividad y la dependencia de las redes 5G las hacen más vulnerables a los ciberataques, lo que plantea riesgos para la privacidad y puede interferir con sistemas críticos (Thomaz et al., 2021)(Velarde, 2020)(La Cuarta Revolución Industrial, 2017). La recopilación y el análisis masivos de datos personales a través de Big Data también plantean problemas de privacidad, y la manipulación de los datos puede utilizarse para influir en la opinión pública y en los procesos electorales.

La proliferación de dispositivos del Internet de las Cosas aumenta la superficie de ataque y la probabilidad de ciberataques, mientras que la tecnología blockchain, aunque ofrece ventajas de seguridad y transparencia, también puede ser explotada. Estos son algunas de las amenazas y riesgos que se tratan dentro del MSPI, el cual es la base de este documento.

a. Riesgos a la infraestructura crítica cibernética

La definición de los riesgos a la infraestructura crítica cibernética se da con base en el Modelo de Seguridad y Privacidad de la Información (MSPI) el cual fue actualizado y toma en cuenta los modelos europeos. En ese sentido se plantean los principales riesgos.

b. Amenazas a la infraestructura crítica cibernética

La infraestructura crítica ha estado sujeta durante mucho tiempo a **amenazas físicas y desastres naturales**, y ahora también está cada vez más expuesta a **riesgos cibernéticos**. Estos riesgos se derivan de una creciente integración de las tecnologías de la información y las comunicaciones con la infraestructura crítica y los adversarios centrados en explotar las posibles vulnerabilidades cibernéticas. A medida que la infraestructura física se vuelve más dependiente de sistemas cibernéticos complejos para las operaciones, la infraestructura crítica puede volverse más vulnerable a ciertas amenazas cibernéticas, incluidas las **amenazas transnacionales**.

Las amenazas y los peligros pueden ser específicos de regiones geográficas o de todo un país, e incluso pueden tener ramificaciones globales como:

- **Eventos Climatológicos:** temperaturas extremas, sequía e incendios forestales.

- Eventos Hidrológicos: inundaciones
- **Eventos Meteorológicos**: ciclones tropicales, severas, invierno severo etc.
- **Eventos Geofísicos:** terremotos, tsunamis y erupciones volcánicas
- **Pandemias:** brotes de enfermedades globales.
- **Accidentes Tecnológicos e Industriales:** fallas estructurales, incendios industriales, riesgos emisiones de sustancias y derrames químicos.
- **Interrupciones no programadas**: infraestructura obsoleta, mal funcionamiento del equipo y fallas a gran escala.
- **Incidentes Criminales y Ataques Terroristas:** vandalismo, robo, daños a la propiedad, incidentes de disparos y ataques cinéticos.
- **Incidentes cibernéticos**: ataques de denegación de servicio, malware, phishing, entre otros.
- **Ataques a la cadena de suministro**: explotación de vulnerabilidades para causar fallas en el sistema o la red.
- **Operaciones de influencia extranjera:** para difundir información errónea o socavar procesos
- Inversión no confiable: para dar potencialmente a las potencias extranjeras una influencia indebida sobre la infraestructura critica del país

8. Derechos comprometidos por las ICC.

La seguridad nacional requiere la protección de una serie de infraestructuras que resultan fundamentales para el mantenimiento de servicios esenciales de la comunidad, cuya interrupción tendría graves consecuencias para territorios concretos o para el país en general lo que coyunturalmente generaría una afectación a los derechos de los ciudadanos, entre los cuales prima el Derecho a la vida y sus derechos conexos como el Derecho a la salud, al agua y saneamiento, alimentación, Derecho a la libertad seguridad e integridad personal, Derecho al trabajo, Derecho a los servicios públicos domiciliarios, Derecho a la prestación del servicio público de transporte, entre otros.

De este modo, la implementación de la metodología de identificación de las ICC en conjunto con las guías de activos, gestión de riesgos y gestión de incidentes, facilitan el éxito del levantamiento de las ICC y la generación oportuna de acciones y operaciones según la dinámica de los riesgos que permitan establecer lineamientos en donde prime la seguridad de las ICC y los servicios esenciales para que sean aprovechados activa y correctamente en beneficio de los derechos de los ciudadanos.

Este enfoque basado en la prevención desde la identificación busca fomentar la confianza en el entorno digital, el fortalecimiento en el sector económico y social, lo que permitirá

asegurar la prestación de los servicios esenciales, la innovación, productividad, competitividad, empleo y sobre todo una vida digna en un entorno seguro en el cual se evite la materialización de infracciones a los derechos de los ciudadanos.

Las infraestructuras críticas cibernéticas protegen varios derechos humanos fundamentales, entre ellos:

1. Derecho a la vida y la seguridad: La identificación y protección de sistemas que pueden afectar la prestación esencial de servicios como la energía, el agua y la salud entre otros, asegura que las personas puedan acceder a servicios vitales, previniendo riesgos asociados a la vida e integridad de las personas.

2. Derecho a la privacidad: La identificación de las infraestructuras criticas cibernéticas permite la implementación de controles oportunos para la protección de los datos personales y datos sensibles de los individuos frente accesos no autorizados.

3. Derecho a la libertad de expresión: La protección de las infraestructuras cibernéticas también asegura que las plataformas de comunicación y expresión no sean censuradas o manipuladas, permitiendo el libre flujo de información.

4. Derecho a la información: Mantener la seguridad de las infraestructuras críticas cibernéticas asegura que la información sobre servicios públicos y emergencias esté disponible y sea accesible, a su vez proporciona que las personas puedan recibir la información clara, oportuna y veraz.

5. Derecho a la seguridad: La ciberseguridad protege a las personas y sociedades de amenazas cibernéticas que pueden causar daños físicos o emocionales. La seguridad en el ciberespacio es una extensión del derecho a vivir en un entorno seguro.

6. Igualdad y no discriminación: La identificación de las ICC permiten tomar acciones dentro del estado de manera que no discriminen a ningún grupo, garantizando que todos tengan acceso igualitario a la tecnología, a la información, a la educación digital y a la protección contra ciberamenazas, entre otras situaciones de desarrollo que se generaron dentro de los ecosistemas digitales.

El equilibrio entre la ciberseguridad y la protección de los derechos fundamentales es crucial para garantizar que las medidas de seguridad no se conviertan en herramientas de control o represión; En este sentido, es fundamental la identificación de las ICC y la implementación de los controles para generar medidas proactivas por parte de los administradores y el gobierno.

9. Casos comparados: Metodología Infraestructura Crítica Cibernética

El estudio de casos comparado de metodologías de infraestructura crítica cibernética revela los diversos enfoques para identificar, evaluar y mitigar amenazas y riesgos en los activos críticos. Si bien comparten variables comunes, se debe garantizar la resiliencia y continuidad operativa, cada metodología difieren en su alcance, profundidad y énfasis en aspectos como la evaluación de riesgos, la gestión de incidentes y la gobernanza. El presente análisis y el anexo 3 identifican os enfoques, las variables y los sectores principales en cada Estado, esto vario acorde a cada realidad o entidad.

Actor	Documento	Metodología	Variables	Sectores
ENISA	Methodologies for the identification of Critical Information Infrastructure assets and services	**1. Enfoque no dependiente del servicio crítico:** No implica un análisis de los servicios críticos soportados; en su lugar, solo analiza la infraestructura de la red. **2. Enfoque dependiente de los servicios críticos (CS):** Comienzan con la identificación de los servicios críticos y los servicios que pertecen a estos. Se basa en el impacto que la interrupción de un servicio puede tener en las funciones vitales de la sociedad	**1.** Tamaño de la población afectada **2.** La dependencia intersectorial **3.** El impacto geográfico **4.** La seguridad personal y el impacto en la privacidad	
Laboratorio Nacional de Argonne de los Estados Unidos	Metodología para evaluar las interdependencias y dependencias de la infraestructura critica	**1. Estimación Inicial:** Recopilación de información general de los activos de infraestructura crítica utilizando fuentes abiertas. **2. Actual:** Recopilación y análisis de datos de las dependencias físicas, cibernéticas y geográficas, utilizando herramientas de anticipación y visualización. **3. Avanzada:** Estudio de sistemas de infraestructuras críticas, con nuevos mecanismos de recopilación de datos e integración de herramientas **4. Objetivo Final:** Comprensión integral de todas las dimensiones de dependencia e interdependencia,		

OCDE	Metodología de la OCDE para la identificación de infraestructuras criticas	**1.** Identificar activos y redes críticas con evaluación de criticidad. **2.** Análisis de interdependencias **3.** Realización de análisis de vulnerabilidad para identificar puntos débiles (Uso de metodología CRISRRAM, RAMCAP Plus)		
Canadá	National Estrategy for Critical Infraestructure		Procesos, sistemas, instalaciones, tecnologías, redes, activos y servicios esenciales para: 1.La Salud 2. Bienestar economico 3. Seguridad 4. Efectividad en el funcionamiento del gobierno	Energía y servicios Públicos Finanzas Alimento Transporte Gobierno Tecnología de la información y la comunicación Salud Agua Seguridad Fabricación
Australia	Critical Infraestructure resilence strategy		Impacto en: - El bienestar social - El bienestar económico - La seguridad y defensa nacional	Energía Agua Transporte Comunicaciones Bancos y finanzas Salud Alimento Educación superior e investigación Servicios de emergencia Defensa Espacio
Estados Unidos	Framework for Improving Critical Infrastructure Cybersecurity (NIST)	**1. Gestión de activos:** se identifican los dispositivos, sistemas físicos, datos, software, aplicaciones y sistemas de comunicación dentro del sector. **2. Definición de operadores y proveedores:** se definen los operadores y proveedores del sector y se identifica un socio externo del que depende esa infraestructura. **3. Evaluación de riesgos:** se identifican y documentan las vulnerabilidades de los activos críticos cibernéticos, se identifican y	Impacto en: 1. La seguridad de la nación 2. La Seguridad Económica Nacional 3. La Salud 4. La Seguridad Publica 5. La Seguridad Cibernética y Privacidad 6. La Gobernanza en Ciberseguridad	Tecnología de información TI Sistemas de Control Industrial Sistemas ciberfisicos Internet de las Cosas IoT
Suiza	The Swiss National Strategy for the Protection of Critical Infrastructure	**1.** Realización de una evaluación de riesgos **2.** Análisis de la importancia de cada infraestructura crítica **3.** Evaluación de la vulnerabilidad de cada infraestructura crítica **4.** Elaboración de una lista de infraestructuras críticas prioritarias	Impacto en: 1. El bienestar social 2. La economía 3. La seguridad nacional	Energía Transporte Tecnologías de la información y la comunicación (TIC) Servicios financieros Administración pública Salud pública Seguridad pública Agua Alimentación

Reino Unido	Critical National Infrastructure	1. Mapear funciones esenciales con base a las variables establecidas 2. Determinar los sistemas: Mapear los sistemas que proporcionan la función 3.Evaluar los impactos del sector en el sistema de infraestructurasx 4. Identificar los sistemas, las organizaciones y las relaciones de apoyo 5. Evaluar los impactos intersectoriales	Impacto en: 1. La sociedad 2. Económia 3. Defensa y seguridad nacional 4. Indice demografico	Quimicos Nuclear civil Comunicaciones Defensa Servicios de emergencia Energía Finanzas Alimento Gobierno Salud Espacio Transporte Agua
Portugal	Ranking Critical Infrastructures – The Portuguese Methodology	1. Se identifican las infraestructuras críticas y se clasifican según su sector. 2. Análisis de Interdependencia y efecto cascada por medio del algoritmo ADPA y las construcción de una matriz de dependencias 2. Se evalúa la criticidad de cada infraestructura crítica mediante la identificación y análisis de los impactos potenciales de un evento adverso en la sociedad y la economía. 4. Se priorizan las infraestructuras críticas en función de su importancia relativa	Impacto en: 1. La seguridad pública 2. La economía 3. El medio ambiente 4. La sociedad	Energía Transporte Abastecimiento de agua Salud Comunicaciones Banca y finanzas Administración pública Industria química Industria nuclear Defensa Alimentación

Ilustración 1 Comparativo de metodología de ICC internacional

Fuente: Construcción Propia

10. Metodología para identificación de ICC en Colombia

Según la línea expuesta el presente documento plantea una actualización de la metodología, la cual requiere identificar las infraestructuras críticas cibernéticas a través del paso a paso expuesto a continuación, para así, lograr el levantamiento del inventario de ICC y de servicios esenciales en el ciberespacio. En esta parte se explica cómo se llega a la identificación de las variables y en el capítulo posterior, se explica el paso a paso y los productos a lograr mediante el levantamiento de ICC.

Paso 1. Identificar el problema: identificación del problema donde sectores deben abordar y desarrollar un concepto que puedan ejecutar juntos. Para ello se debe:

1.1. Identificación de la agencia líder: Necesidad de definir qué agencia o departamento gubernamental liderará este esfuerzo. Durante este proceso, debe haber una comprensión de la cantidad de recursos y tiempo necesarios para completar esta tarea. La Agencia/Departamento coordinador también deberá elegir un "Líder del Equipo de Planificación". Una vez hecho esto, deberán revisar cualquier documentación o gobernanza actual existente.

a. Definir los apoyos: Para la identificación de apoyos se debe identificar la dependencia e interdependencia entre los sectores. Como existe un alto nivel de las relaciones físicas

comunes entre los sistemas de infraestructura crítica, se hace necesario definir las dependencias de alto nivel para definir los sectores de interés.

En la siguiente ilustración se relacionan las dependencias en un alto nivel, los puntos rojos indican que el sector de apoyo identificado en la parte superior de la columna proporciona bienes o servicios al sector de interés a lo largo del lado izquierdo de la matriz.

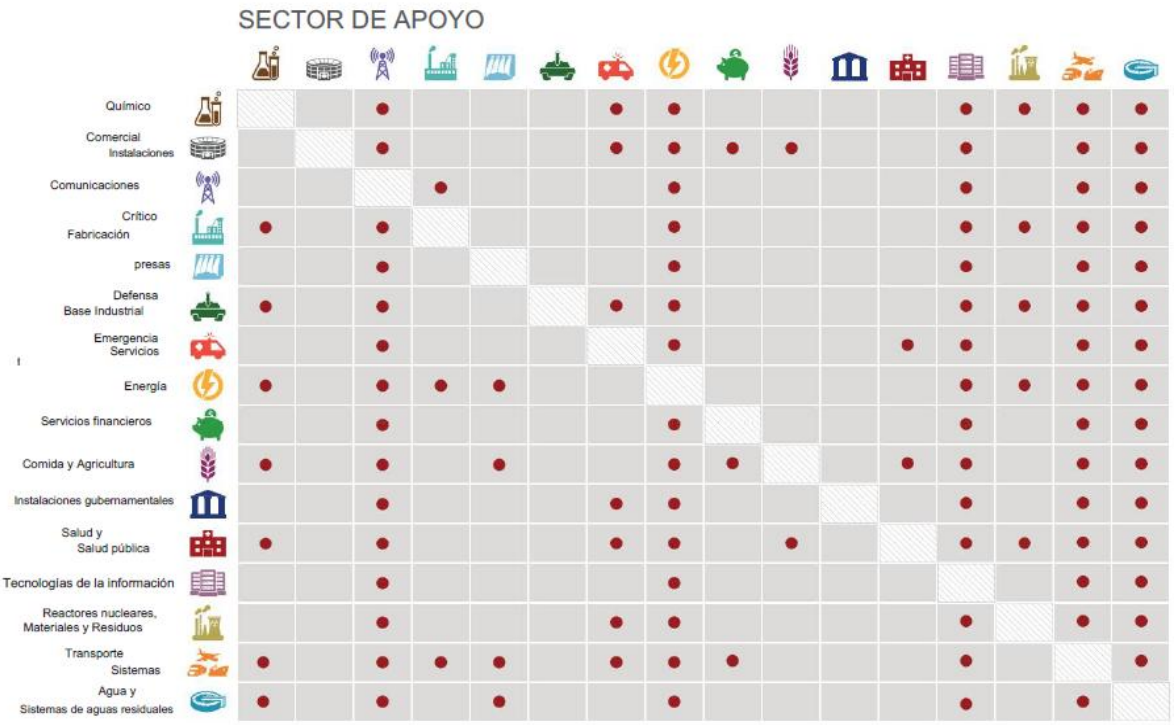


Ilustración 2 Interdependencia de Infraestructura Crítica Cibernética de Estados Unidos

Fuente. CISA.

En el caso de Colombia se propone esta interrelación la cual vario acorde al levantamiento y actualización en el levantamiento de la Infraestructura Crítica cibernética. Este paso se identifican los 13 sectores y acorde al tercer paso del Excel, se explica la interrelación que se pretende lograr a partir del levantamiento de la ICC.

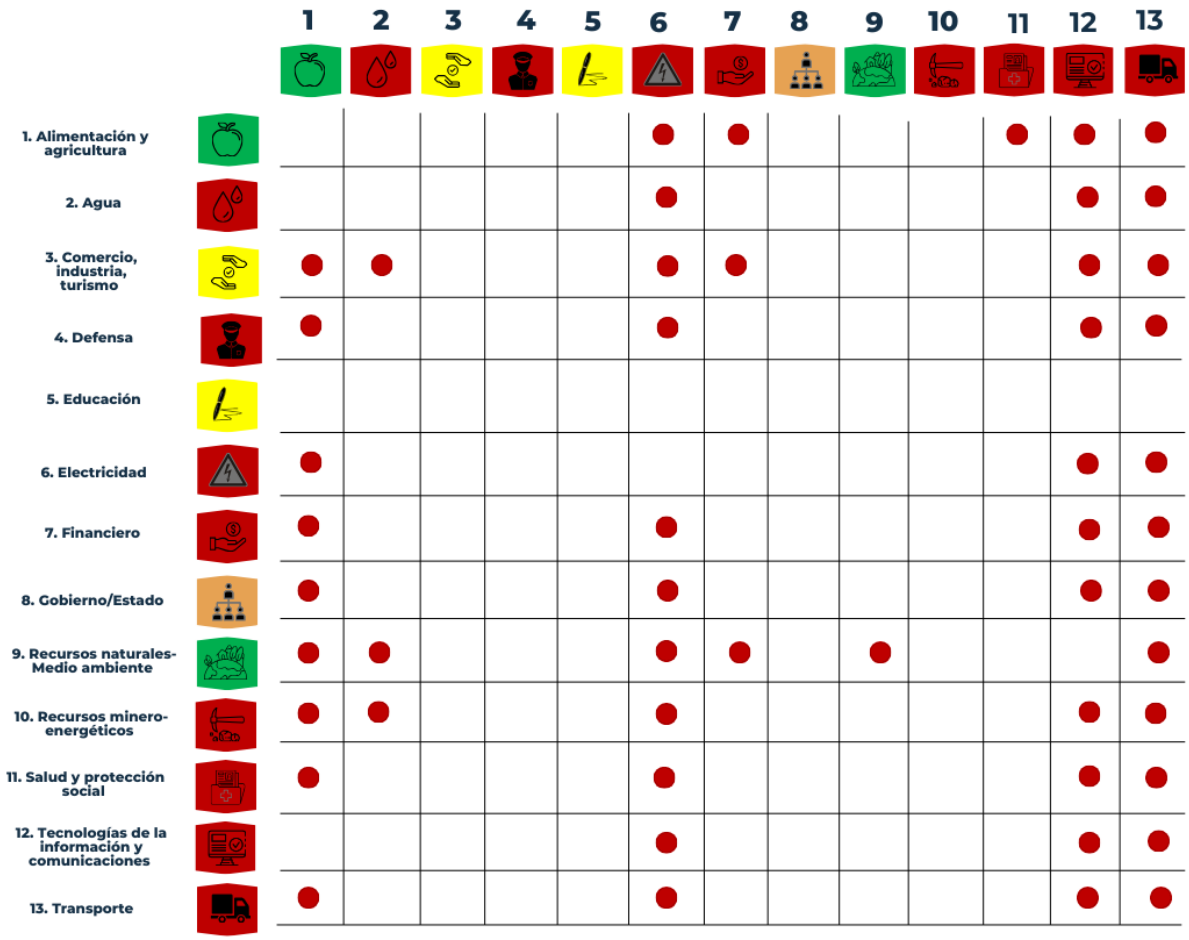


Ilustración 3 Interdependencia de infraestructura Crítica Cibernética de Colombia

Fuente. Construcción propia

b. **Identificar conceptos:** Se deben reflejar un cierto grado de investigación fundamental realizada por las principales partes interesadas para confirmar la necesidad de una evaluación y la viabilidad de los primeros conceptos propuestos.

c. **Experiencia pasada con incidentes del mundo real:** se deben analizar los huracanes, incendios forestales, ataques cibernéticos y demás factores externos que incidan en la infraestructura.

d. **Grupos de trabajo y organizaciones asociadas:** Conformar grupos de trabajo que pueden incluir partes interesadas de una variedad de organizaciones tales como propietarios y operadores de instalaciones del sector privado, organizaciones de recuperación y respuesta a emergencias, proveedores de servicios públicos y autoridades reguladoras, agencias y autoridades de transporte, organizaciones de planificación metropolitana, organismos encargados de hacer cumplir la ley y de seguridad consejos tribales, instituciones académicas y centros de investigación, asociaciones industriales.

e. **Evaluaciones previas, planes, operativos y ejercicios:** Realizar evaluaciones en instalaciones ubicadas dentro del área de enfoque geográfico o la infraestructura de apoyo que tiene el potencial de proporcionar información sobre resiliencia; procesos de planificación colaborativa, lecciones aprendidas de los ejercicios de simulación.

f. **Análisis de peligros estatales y locales y evaluaciones de capacidades:** Se deben identificar las amenazas y evaluar los riegos externos e internos cada año, explorando qué amenazas y peligros pueden afectarlos, cuáles serían los impactos potenciales y qué capacidades deberían existir para gestionar eficazmente ese riesgo.

g. **Identificación de amenazas por parte de socios públicos y privados:** Se debe trabajar con centros de fusión como policía, seguridad pública, servicios de bomberos, respuesta a emergencias, etc, para la identificación de amenazas.

Paso 2. Diseño: En este paso se deben definir las preguntas clave de investigación que los esfuerzos de evaluación regional intentarán abordar, en este paso se establecen las 05 variables planteadas en la metodología acorde los siguientes ítems relevantes de estudio:

- Estableciendo la extensión geográfica del esfuerzo
- Identificando los sistemas de infraestructura que se considerarán en la evaluación
- Articulando los pasos específicos que las partes interesadas tomarán para abordar preguntas clave de investigación.
- Describir las características de la infraestructura existente.
- Definir infraestructura Cyber

Este paso es la base sobre la cual se crean las 05 variables para evaluar la ICC.

Paso 3. Recopilar datos: se aborda la investigación de fuentes, colaboración de varias agencias, entrevistas con expertos, discusiones, evaluaciones del sitio y otros pasos que ayudan a capturar la información necesaria para abordar las preguntas clave de investigación de la evaluación.

a. Métodos de recopilación: La revisión de literatura, investigación de fuentes abiertas -OSINT- (publicaciones en línea, blogs, redes sociales), medios (artículos de periódicos y revistas), datos públicos del gobierno (informes, discursos, sitios web, presentaciones de cumplimiento normativo), datos comerciales (informes de investigación de mercado empresarial, bases de datos), literatura gris (informes técnicos, patentes, libros blancos, trabajos no publicados, boletines, comunicados de prensa, presentaciones).

b. Otros Métodos: Entrevistas individuales, encuestas y evaluaciones estructuradas.

Paso 4. Analizar: En este enfoque se debe aplicar de un enfoque analítico para evaluar los sistemas de infraestructura de interés.

- Identificar las amenazas y peligros para la infraestructura.
- Evaluación de las vulnerabilidades de la infraestructura priorizada

- Evaluar las consecuencias y las interacciones entre los sistemas de infraestructura y priorizar el riesgo para los sistemas de infraestructura.
-

a. **Tipos de análisis que se pueden realizar durante la evaluación:** análisis de amenazas y peligros, análisis de vulnerabilidad, análisis de criticidad, análisis comparativo, análisis de planos, análisis geoespacial, análisis de capacidad, análisis de datos, análisis de red, análisis fallido, análisis de decisión. El análisis incluye la identificación de activos críticos, la cual se evalúa a la luz de las variables propuestas.

Paso 5. Documentar y entregar resultados: Acá se documentan los problemas específicos, retos y oportunidades descubiertas desde la evaluación y definición de potenciales cursos de acción que pueden comenzar a abordar las brechas de resiliencias identificadas.

Aquí, se agregan hallazgos importantes del análisis, se documentan los resultados e identifican cómo presentar la información para abordar con mayor eficacia el propósito original y los objetivos previstos resultados de la evaluación.

Se tiene en cuenta el desarrollo de cursos de acción, en donde se identifican los problemas de resiliencia y se visualizan posibles soluciones. Los cursos de acción bien construidos deben hacer lo siguiente:

- Identificar claramente las organizaciones que deberían liderar o tener un papel en su ejecución;

- Ser soluciones lógicas que sean relevantes para el problema identificado en el hallazgo clave;

- Ser factible de manera realista dentro de las limitaciones conocidas

- Identificar los recursos disponibles que pueden ayudar en su ejecución.

Los hallazgos clave de la evaluación y los cursos de acción, así como el cuerpo de investigación y análisis, deben presentarse a las partes interesadas en un formato convincente y útil (o múltiples formatos) que cumpla con los usos previstos, estos pueden ser:

- Informes narrativos que documentan análisis, hallazgos clave y recomendaciones.

- Listas de verificación que documentan vulnerabilidades a nivel de activos o sistemas y opciones para considerar mitigar esas vulnerabilidades.

- Sesiones informativas y presentaciones para entrega en reuniones interinstitucionales, talleres o industria / conferencias académicas.

- Infografías que representan datos y hallazgos.

- Productos cartográficos estáticos e interactivos que aprovechan los datos y análisis geoespaciales recopilados durante la evaluación para ilustrar hallazgos y

recomendaciones relevantes relacionados con sistemas de infraestructura regional.

- Herramientas de apoyo a la toma de decisiones que ayuda a las partes interesadas a probar posibles cursos de acción para tomar decisiones informadas (listas de verificación sencilla y árboles de decisión dentro de una interfaz de usuario simple u opciones de software más avanzadas que integran modelos y elementos de visualización).

- Los conjuntos de datos compilados como la información geoespacial, los resultados del modelado y los inventarios de activos que se recopilaron, seleccionaron o crearon durante el análisis de resiliencia, que también pueden proporcionar valor a las partes interesadas para una mayor planificación y análisis.

Paso 6. Promover la acción: Colocar el trabajo de base para la acción sobre los hallazgos analíticos y tomar medidas tangibles para mejorar la resiliencia a través de inversiones de capital, esfuerzos de planificación, capacitación y ejercicios.

En este punto es necesario implementar soluciones de resiliencia y medir su eficacia. Así se reconocen los elementos de infraestructura crítica:

a. **Tiene tres elementos:** físico, cibernético y humano.

b. **El intercambio de información entre estos elementos se da a través de los siguientes pasos:** fijar metas y objetivos; identificar la infraestructura; evaluar y analizar los riesgos; implementar riesgos de gestión y actividades; y, medidas de eficacia.

De tal forma, se cuenta con pasos específicos para mejorar la resiliencia regional de la infraestructura:

a. **Planeación:** Necesidad de desarrollar o actualizar planes, incluidos los planes estratégicos, operativos y tácticos.

b. **Inversiones de capital y presentaciones de subvenciones:** Los propietarios y operadores de instalaciones, las organizaciones regionales y las agencias gubernamentales pueden usar los hallazgos del análisis de resiliencia para guiar las inversiones estratégicas en equipo, planificación, capacitación y recursos para mejorar la resiliencia y la protección de las instalaciones, las comunidades circundantes y regiones enteras.

c. **Capacitación:** Estas necesidades de capacitación pueden incluir capacitación general sobre temas centrales (gestión de incidentes) o capacitación específica de la organización vinculada a políticas y procedimientos (garantizar que el personal conozca la continuidad del negocio o el plan de operaciones de emergencia).

d. **Ejercicios:** Medio para explotar más a fondo los riesgos recién identificados, resolver las brechas de coordinación y planificación, y diseñar enfoques para otros problemas de infraestructura identificados durante el curso de una resiliencia de evaluación regional.

- Es de destacar que, uno de los principales desafíos para la resiliencia de la infraestructura es la creciente complejidad de la infraestructura de moderna actual. La infraestructura está conectada a muchos otros activos, sistemas y redes de infraestructura de los que dependen para las operaciones normales del día a día.

6. Conceptos de evaluación o variable para la identificación de infraestructuras críticas cibernética nacional

Colombia con este documento busca actualizar la metodología de identificación de infraestructura crítica cibernética, con base en el decreto 338, el cual insta a identificar infraestructuras críticas y de un sistema unificado de evaluación y seguimiento a esta.

Por lo que la identificación de IC a nivel nacional se ha basado en procedimientos particulares que cada entidad pública y particular ha construido de acuerdo con sus necesidades y funciones. Donde se destacan tres variables fundamentales: a) Sociales, que analizan el impacto de la IC en la calidad de vida de la población; b) Económicas, que analizan el impacto de la IC en la economía nacional y departamental; y c) Medioambientales, que analizan el impacto de la IC en la biodiversidad y los recursos ecosistémicos.

Si bien, estas variables han permitido identificar y evaluar las infraestructuras y activos críticos a nivel nacional, en un contexto cada vez más complejo y cambiante gracias a la interconexión global por el crecimiento acelerado de las TIC, se hace necesario actualizar el enfoque de identificación de infraestructuras críticas para hacer frente a nuevos riesgos y amenazas. Incorporando nuevas variables que permitan una identificación más precisa y completa de las infraestructuras críticas en Colombia para luego, poder pasar a la identificación de una Infraestructura crítica cibernética, la cual se encuentra definida en el Decreto Único 1078 de 2015 adicionado por el Decreto 338 de 2022, como aquellos *"Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía"*.

En esta última sección se propone una metodología para identificar las infraestructuras críticas públicas cibernéticas nacionales y de servicios esenciales, considerando metodologías internacionales y las infraestructuras críticas de países referentes en ciberseguridad. Proponiendo a partir de este estudio comparativo 5 variables nuevas o conceptos de evaluación para la identificación de infraestructuras críticas cibernéticas en Colombia. Estos son los siguientes, los cuales se exponen de manera general y se anexan un archivo en Excel con la definición de cada una de ellas.

1. **Impacto a las funciones críticas nacionales:** Esta variable evalúa el impacto sobre cuantas funciones críticas nacionales se ven afectadas por la afectación de la seguridad del activo de infraestructura crítica cibernética. Lo anterior, con base en las categorías de comunicación, distribución, administración y suministro.

2. **Contexto y/o población afectada:** Esta variable se refiere al contexto y la importancia del sistema, incluyendo la cantidad de personas que se perturba en el servicio de una infraestructura crítica, y a la densidad poblacional en la zona de influencia de dicha infraestructura, lo anterior con un enfoque de Derechos Humanos, por lo que es esencial que en esta variable se evalúa el impacto sobre su afectación. Esta variable es importante para evaluar el grado

de impacto en la población y la necesidad de priorizar la recuperación del servicio.

3. **Impacto operacional:** Esta variable mide el impacto y alcance en el funcionamiento, teniendo en cuenta la salud pública, área geográfica, entre otros, que se vería afectada en caso de interrupción del servicio de una infraestructura crítica. Se consideran aspectos como la cantidad de usuarios y la distribución geográfica de la infraestructura. Evaluar esta variable es importante porque permite identificar las zonas más vulnerables y establecer planes de **contingencia** que aborden específicamente el impacto en cada área geográfica afectada.

   En esta variable es fundamental trabajar de la mano con otros departamentos gubernamentales encargados de estudiar factores que tienen un impacto operacional en la IC. Por ejemplo, en el caso de determinar las dependencias geográficas se deben tener en cuenta los informes de entidades encargadas de estudiar los fenómenos climáticos como lo es el IDEAM y el Banco de la República[19]

4. **Afectación Económica Nacional:** Esta variable mide el impacto que la interrupción del servicio de una infraestructura crítica tendría sobre la economía del país, específicamente sobre el Producto Interno Bruto (PIB). Se consideran aspectos como la disminución en la producción, la pérdida de empleos y la reducción en las exportaciones. Esto es una estimación con base en los datos que provee el DANE.

5. **Impacto Nacional al servicio:** Impacto Nacional del Servicio - Incidentes que podrían afectar al servicio del Estado, esto pensado en términos de seguridad nacional, derechos humanos y la afectación correlacionada otros sectores esenciales o con los que se tenga relación. Impacto de su servicio y la interdependencia con otro sector

11. Definición de las variables y explicación en la metodología:

Las Infraestructuras Críticas Cibernéticas en la metodología se organizan en sectores y se procura por lograr identificar los subsectores y los operadores, de manera escalonada. Lo anterior, ya que pueden representar cada uno una categoría general de servicios y sistemas esenciales.

En ese sentido se propone:

[19] Banco de la República. (2023). Desastres naturales en Colombia: un análisis regional. Señala que, Colombia por su ubicación geográfica es uno de los países en Latinoamérica más propensos a sufrir desastres naturales, siendo los departamentos de Antioquia y Putumayo los que sufrieron un mayor número de pérdidas humanas por desastres naturales.

Paso 1. Teniendo en cuenta la identificación de activos críticos de información de su entidad según el Modelo de Privacidad y Seguridad de la Información (MSPI). El cual debe tener cada entidad.

Paso 2. Con base en el paso 1 desarrolle la matriz en Excel con los factores de evaluación y la delimitación de la infraestructura crítica cibernética (anexo número 1).

Paso 3. Seguimiento y control de las ICC (anexo número 2).

6.1.1 Definición de variables

- Activos - Serían los elementos tangibles o intangibles que son esenciales para que los sistemas funcionen.

- Indicador o Clasificación de Incidentes - Etiquetará los sucesos en función de su gravedad y/o impacto potencial en sus sectores.

En el caso de la metodología en Colombia se utilizará la taxonomía de clasificación de incidentes de COLCERT[20], en esta parte se debe especificar el tipo de clasificación o potencial incidente sobre el activo.

La escala de evaluación se alinea a guía de DAFP (1) Bajo; (2) Moderado; (3) alto ; (4) Extremo.

A. FUNCIONES CRÍTICAS NACIONALES: Se define como LA FUNCIÓN CRÍTICA DEL ESTADO, Esto tendría consecuencias para los roles esenciales de la ICC en un mayor número de las Funciones Críticas Nacionales.

La escala de evaluación se alinea a guía de DAFP se define así:

• Bajo (1) = Impacto una o ninguna función crítica nacional que afecte su servicio.

• Moderado (2) = Supone un impacto potencial en dos funciones críticas Nacionales con impacto en su organización y otros sectores de apoyo.

• Alto (3) = Tendrá un impacto en tres funciones críticas nacionales, es probable que afecte a otras organizaciones.

• Extremo (4) = Tendrá un impacto grave en 04 o más funciones críticas nacionales, lo que se refleja en la capacidad operativa de la organización, impacto conocido o previsto en otras organizaciones.

Estas funciones se dividen en 04 grandes categorías y cada una de ellas incluye cada una de las funciones de la siguiente manera: [21]

Conexión Comunicación	Distribución	Administración	Suministro
1. Operación del Core Network (Núcleo	1. Distribución de electricidad	1. Celebración de elecciones	1. Exploración y extracción de combustibles

[20] https://www.colcert.gov.co/800/articles-198656_taxonomia.pdf

[21] Definición de funciones críticas nacionales adaptadas de https://www.rand.org/pubs/research_reports/RRA1512-1.html

Conexión Comunicación	Distribución	Administración	Suministro
de la red operada)			
2. Prestación de servicios de redes de acceso por cable o redes alámbricas.	2. Mantener las cadenas de suministro	2. Desarrollar y mantener obras y servicios públicos	2. Refinación y procesamiento de combustibles
3. Prestación de servicios de comunicación e información de contenidos basados en Internet	3. Transmisión de electricidad	3. Educación y formación	3. Generación de electricidad
4. Prestación de servicios de enrutamiento, acceso y conexión a Internet	4. Transportar carga y pasajeros por aire	4. Cumplimiento de la ley/normatividad (Law Enforcement)	4. Manufactura de equipos/materiales /insumos
5. Prestación de servicios de posicionamiento, navegación y tiempo.	5. Transportar carga y pasajeros por ferrocarril	5. Mantener el acceso a los historiales médicos	5. Producción y suministro de productos y servicios agrícolas
6. Prestación de servicios de redes de acceso de radiodifusión	6. Transportar carga y pasajeros por carretera	6. Gestionar los materiales peligrosos	6. Producción y suministro de productos y servicios de alimentación humana y animal
7. Prestación de servicios de redes de acceso por satélite	7. Transportar carga y pasajeros por barco	7. Gestionar las aguas residuales	7. Producción de productos químicos
8. Prestación de servicios de redes de acceso inalámbricas	8. Transportar materiales por ductos, oleoductos o gasoductos.	8. Gestionar la administración pública	8. Suministro de metales y materiales

Conexión Comunicación	Distribución	Administración	Suministro
	10. Transporte masivo de pasajeros	9. Disponer de capacidades de gestión de incidentes cibernéticos	9. Suministro de viviendas
		10. Prepararse para las emergencias y gestionarlas	10. Suministro de productos y servicios de tecnología de la información
		11. Preservar los derechos constitucionales	11. Suministro de material y apoyo operativo a la defensa
		12. Proteger la información confidencial	12. Investigación y desarrollo
		13. Proporcionar y mantener infraestructuras (Física)	13. Suministro de agua
		14. Prestar servicios de mercados de capitales y actividades de inversión	
		15. Prestar servicios de banca comercial y de consumo	
		16. Prestar servicios de financiación y liquidez	
		17. Prestar servicios de gestión de identidad y servicios de apoyo fiduciario asociados	
		18. Prestar servicios de seguros	

Conexión Comunicación	Distribución	Administración	Suministro
		19. Prestar asistencia médica	
		20. Prestar servicios de compensación y liquidación de pagos	
		21. Proporcionar seguridad pública	
		22. Proporcionar financiación mayorista	
		23. Almacenar combustible y mantener reservas	
		24. Apoyar la salud de la comunidad	

B. Contexto/Población - Se basaría en la población afectada por la interrupción del sector. En esta variable se tiene en cuenta la afectación a los derechos humanos. La escala de esta se define con base en el método Hanlon, el cual es una herramienta utilizada en el campo de la salud pública para priorizar problemas de salud y asignar recursos de manera efectiva. En ese sentido, se toma el componente de magnitud para entender el número de personas afectadas por el problema en relación con la población total. El cual se basa en una estimación a partir de Hanlon, J.J. y Pickent, George E. Public Health Administration and Practice. Ed 8.

- Bajo (1) = 99.999 o menos personas
- Moderado (2) = de 100.000 a 249.999 personas
- Alto (3) = de 250.000 a 499.999 persona
- Extremo (4) =Impacto potencial a 500. 000 o más personas

C. Impacto Operacional

Esta variable mide el impacto y alcance en el funcionamiento (servicios de la entidad, teniendo en cuenta la salud pública, área geográfica, entre otros, que se vería afectada en caso de interrupción del servicio de una infraestructura crítica. Se consideran aspectos como la cantidad de usuarios y la distribución geográfica de la infraestructura.

Bajo (1) = Nivel menor: El impacto que causa la materialización del riesgo en los objetivos de la entidad es mínimo. El impacto de la operación es pequeño en el territorio o la entidad.

Moderado (2) = Nivel moderado: La materialización del riesgo puede causar una pérdida momentánea. El impacto afecta momentáneamente pero breve la operación de la entidad y/o en los territorios.

Alto (3) = Nivel mayor: Genera retrasos importantes que afectan el cumplimiento de los objetivos. En esta parte se afecta la operación de la entidad y sus acciones en el territorio.

Extremo (4) = Nivel catastrófico: Puede detener la operación de la entidad, incluso, tener consecuencias como el cierre definitivo. Afecta la operación total de la entidad y su despliegue en territorio.

D. Afectación Económica Nacional

La afectación Económica nacional mide el impacto de un incidente económico en términos del PIB, tomando en cuenta lo siguiente:

Bajo (1) =Impacto menor al 0,1% del PIB

Moderado (2) = Impacto inferior del 0,1 al 0,5%

Alto (3) = Impacto del 0,5 al 1% del PIB.

Extremo (4) = Impacto mayor al 1% del PIB.

Lo que se mide de la siguiente manera:

Impacto económico en porcentaje del PIB = (Valor del impacto económico / PIB) * 100

El impacto se mide según los siguientes datos:

- PIB Colombia año 2023: 1,572,459.000.000
- Este valor se debe dividir sobre el valor del impacto[22] económico del sector/PIB *100.

Los datos del PIB enfoque de la producción se toman del DANE, en la tabla que se adjunta.

E. Impacto Nacional del Servicio: Incidentes que podrían afectar al servicio del Estado y otros sectores esenciales o con los que se tenga relación. Impacto de su servicio y la interdependencia con otro sector

Ejemplos:

• Interrupciones

• Tiempo de inactividad

• Averías de equipos

• Problemas de seguridad/catástrofes naturales

• Pérdida de control

• Bajo (1) = Impacto muy bajo en la organización, improbable que afecte a otras organizaciones

[22] El valor del impacto económico se entrega acorde a la proyección del DANE por sectores

• Moderado (2) = Supone un impacto potencial para la organización, posibilidad mínima de impacto para otras organizaciones

• Alto (3) = Tendrá un impacto en la organización, es probable que afecte a otras organizaciones

• Extremo (4) = Tendrá un impacto grave en la capacidad operativa de la organización, impacto conocido o previsto en otras organizaciones.

Estas son las 05 variables que se evalúan junto a esta se establece el tiempo de indisponibilidad y recuperación acorde a la siguiente escala:

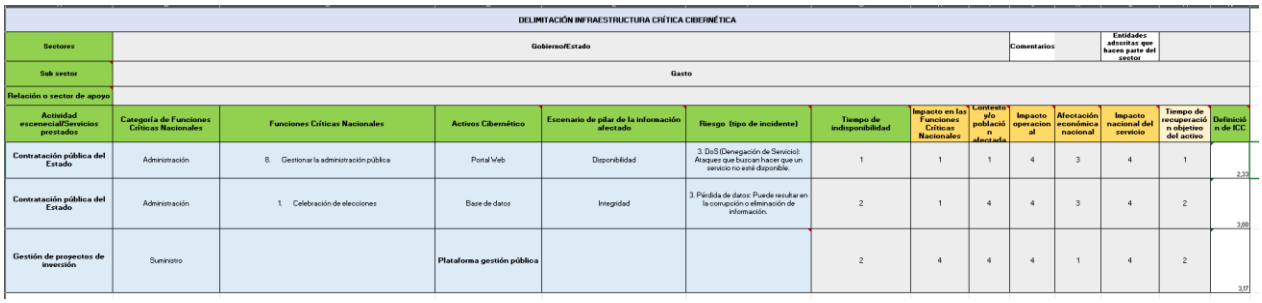
Escala

Bajo (1) =. El tiempo de indisponibilidad del activo es de 24 horas o menos.

Moderado (2) = El tiempo de indisponibilidad del activo es de 24 a 72 horas.

Alto (3) = El tiempo de indisponibilidad del activo es de 72 horas a una semana.

Extremo (4) = El tiempo de indisponibilidad del activo es superior a una semana o no se puede determinar por su alto impacto



DELIMITACIÓN INFRAESTRUCTURA CRÍTICA CIBERNÉTICA													
Sectores	Gobierno/Estado								Comentarios		Entidades adscritas que hacen parte del sector		
Sub sector	Gasto												
Relación o sector de apoyo													
Actividad esencial/Servicios prestados	Categoría de Funciones Críticas Nacionales	Funciones Críticas Nacionales	Activos Cibernético	Escenario de pilar de la información afectado	Riesgo (tipo de incidente)	Tiempo de indisponibilidad	Impacto en las Funciones Críticas Nacionales	Contexto y/o población afectada	Impacto operacional	Afectación económica nacional	Impacto nacional del servicio	Tiempo de recuperación objetivo del activo	Definición de ICC
Contratación pública del Estado	Administración	8. Gestionar la administración pública	Portal Web	Disponibilidad	3. DoS (Denegación de Servicio): Ataques que buscan hacer que un servicio no esté disponible.	1	1	1	4	3	4	1	2,29
Contratación pública del Estado	Administración	1. Celebración de elecciones	Base de datos	Integridad	3. Pérdida de datos: Puede resultar en la corrupción o eliminación de información.	2	1	4	4	3	4	2	3,00
Gestión de proyectos de inversión	Suministro		Plataforma gestión pública			2	4	4	4	1	4	2	3,17

Ilustración 4 Paso 3 identificación de ICC

Resultado de la evaluación se presenta la escala de las categorías y definiciones de Infraestructura crítica cibernética/ Servicios esenciales:

1. La ICC todo lo que en la evaluación de entre 2,45 a 4. (Categoría Crítico) - Extremo

2. Servicio Esencial: todo aquel que en la escala se encuentre entre 1,95 y 2,94. (Categoría Esencial) - Alto

3. Servicio no esencial, pero con impacto a la seguridad: todo entre 0.95 y 1.94. (Categoría importante) - Moderado

4. Activo que se contempla, pero no cumple un impacto a nivel nacional. – (Categoría Secundario) - Bajo

12. Actualización en la metodología:

En la propuesta se menciona modificar las variables de estudio para evaluar sectores y subsectores, en ese sentido, se modifica el punto número 5. En el que se amplía las tres variables y se propone el estudio de impacto a partir de las mencionadas.

A su vez, la propuesta va encaminada a:

- Incluir la sección de etiquetado para ICC (Infraestructura Crítica Cibernética).
- Actualizar la clasificación de activos.
- Establecer un capítulo con la descripción de los criterios de identificación.
- Definir operadores de las infraestructuras Críticas Cibernéticas y las redes de operación.
- Incluir, Interdependencias:

- Internas entre subsectores o servicios de un mismo sector

-Entre sectores críticos

-Entre activos de la red de datos de varios sectores.

- Ajustar el formato de identificación y clasificación de activos para ICC manejando únicamente lo relacionado con seguridad digital (una vez ya se haya identificado los activos de información).
- Identificar los activos de criticidad alta y media e incluir criterios de identificación de ICC para ellos.
- Actualizar anexo 4 Guía para la gestión del riesgo y diseño de controles a través de la identificación de activos de información y el reporte de la gestión del riesgo de seguridad de la información autoridades o entidades especiales asociada al MSPI.

Consideraciones finales

Con estos lineamientos se consolidan los criterios mínimos para el reporte de información por parte de las entidades públicas y se busca servir como referente frente a las entidades privadas.

La metodología para la identificación de las Infraestructuras Críticas Cibernéticas tiene por objeto ayudar a los propietarios y operadores a identificación de Infraestructuras Críticas, evaluar cualquier riesgo relacionado, y desarrollar e implementar soluciones de resiliencia.

Las infraestructuras críticas cibernéticas pueden ser propiedad y estar gestionadas por una amplia gama de entidades de los sectores público y privado. Estos lineamientos ayudarán a dirigir y alinear los diversos esfuerzos relacionados con la seguridad y la resistencia de estos sistemas, aunque no hay dos sistemas iguales, esta estrategia pretende sentar las bases para la identificación de Infraestructuras cibernéticas.

La Infraestructura Crítica incluye servicios tales como activos, sistemas, instalaciones, redes y otros sistemas vitales de los que la sociedad colombiana depende para mantener la economía, la salud pública, la seguridad y varias Funciones Críticas Nacionales para mantener al país "funcionando". La Infraestructura Crítica puede definirse mejor como aquellos sistemas y activos, ya sean físicos o virtuales que son tan vitales que su incapacidad o destrucción puede tener un impacto debilitante en la seguridad, la economía, la salud pública o la seguridad de la nación, la salud pública o la seguridad de la nación.

13. Orientación

1. Identificar la ICC, ser capaz de identificar los problemas que los sectores específicos

deben abordar y desarrollar un concepto que pueda ejecutarse conjuntamente.

2. Diseñar la evaluación con preguntas claves de investigación que permitan realizar una evaluación eficaz en territorio.

3. Recopilación de datos, llevar a cabo la investigación, recopilación multiinstitucional, entrevistas con expertos en la materia, debates facilitados, evaluaciones in situ y otros pasos que ayuden a las partes interesadas a recopilar la información abordar las preguntas clave de investigación de la evaluación.

4. Analizar y utilizar diversas técnicas analíticas para evaluar los sistemas de interés.

5. Documentar y entregar resultados para proporcionar una documentación escrita de los problemas, retos y oportunidades descubiertos a partir de la evaluación y la definición de posibles líneas de acción que puedan empezar a abordar las deficiencias de resiliencia identificadas

6. Promover la acción a realizar sobre los resultados analíticos y tomar medidas tangibles para mejorar resiliencia mediante inversiones de capital, esfuerzos de planificación, formación y ejercicios.

Paso a paso para la identificación de las ICC

En un mundo dinámico e interconectado, donde la privacidad y la seguridad de los datos es fundamental, surge la protección de infraestructuras críticas cibernéticas como un eje esencial para garantizar la continuidad y la seguridad de los servicios fundamentales, teniendo en cuenta la garantía de los derechos humanos y la protección de los derechos fundamentales.

Las infraestructuras Criticas Cibernéticas abarcan los 13 sectores, desde energía y transporte hasta redes de comunicación, son vulnerables a las amenazas cibernéticas que pueden afectar gravemente la seguridad, estabilidad social, económica y política de un país.

Este paso a paso tiene como objetivo guiar el proceso de levantamiento de infraestructuras críticas cibernéticas, el cual se enfoca en tres etapas clave: la **identificación de activos críticos**, la **evaluación mediante una matriz de variables que contempla, evaluar los activos críticos, frente a las actividades y servicios prestados, a la luz de evaluar escenarios frente a:**

1. Impacto en las funciones críticas nacionales
2. Contexto y/o población afectada
3. Impacto operacional
4. Afectación económica nacional
5. Impacto nacional del servicio

- Tiempo de recuperación de activo planteado en la guía de riesgos.

y la implementación de un **control de seguimiento y gestión de riesgos**. A través de este enfoque estructurado, las organizaciones pueden identificar la infraestructura crítica cibernética, los servicios esenciales, las vulnerabilidades, priorizar recursos de protección y establecer mecanismos proactivos y de anticipación para mitigar riesgos, garantizando así la resiliencia y seguridad de sus infraestructuras críticas.

Las Infraestructuras Críticas Cibernéticas se identificarán inicialmente en los 13 sectores establecidos en el documento matriz, paulatinamente se procurará lograr identificar los subsectores y los operadores de manera escalonada. Lo anterior, ya que cada uno puede representar una categoría general de servicios y sistemas esenciales.

En ese sentido se propone:

Paso 1. Identifique los activos críticos de información de su entidad según el Modelo de Privacidad y Seguridad de la Información (MSPI).

Paso 2. Aplique los controles correspondientes según la guía de gestión de riesgos asociada al MSPI.

Paso 3. Con base en el paso 1 y 2 diligencie la matriz en formato Excel con los factores de evaluación y la delimitación de la infraestructura crítica cibernética (anexo número 1).

Paso 4. Seguimiento y control de las ICC (anexo número 2).

Definición de variables

- Activos - Serían los elementos tangibles o intangibles que son esenciales para que los sistemas funcionen.

- Indicador o Clasificación de Incidentes - Etiquetará los sucesos en función de su gravedad y/o impacto potencial en sus sectores.

En el caso de la metodología en Colombia se utilizará la taxonomía de clasificación de incidentes de COLCERT[23], en esta parte se debe especificar el tipo de clasificación o potencial incidente sobre el activo.

La escala de evaluación se alinea a guía de DAFP (1) Bajo; (2) Moderado; (3) alto; (4) Extremo.

A. IMPACTO A LA SEGURIDAD: Se define como LA FUNCIÓN CRÍTICA DEL ESTADO, Esto tendría consecuencias para los roles esenciales de la ICC en un mayor número de las Funciones Críticas Nacionales.

La escala de evaluación se alinea a guía de DAFP se define así:

• Bajo (1) = Impacto una o ninguna función crítica nacional que afecte su servicio.

• Moderado (2) = Supone un impacto potencial en dos funciones críticas Nacionales con impacto en su organización y otros sectores de apoyo.

• Alto (3) = Tendrá un impacto en tres funciones críticas nacionales, es probable que afecte a otras organizaciones.

[23] https://www.colcert.gov.co/800/articles-198656_taxonomia.pdf

• Extremo (4) = Tendrá un impacto grave en 04 o más funciones críticas nacionales, lo que se refleja en la capacidad operativa de la organización, impacto conocido o previsto en otras organizaciones.

Estas funciones se dividen en 04 grandes categorías y cada una de ellas incluye cada una de las funciones de la siguiente manera: [24]

Conexión Comunicación	Distribución	Administración	Suministro
1. Operación del Core Network (Núcleo de la red operada)	1. Distribución de electricidad	1. Celebración de elecciones	1. Exploración y extracción de combustibles
2. Prestación de servicios de redes de acceso por cable o redes alámbricas.	2. Mantener las cadenas de suministro	2. Desarrollar y mantener obras y servicios públicos	2. Refinación y procesamiento de combustibles
3. Prestación de servicios de comunicación e información de contenidos basados en Internet	3. Transmisión de electricidad	3. Educación y formación	3. Generación de electricidad
4. Prestación de servicios de enrutamiento, acceso y conexión a Internet	4. Transportar carga y pasajeros por aire	4. Cumplimiento de la ley/normatividad (Law Enforcement)	4. Manufactura de equipos/materiales /insumos
5. Prestación de servicios de posicionamiento, navegación y tiempo.	5. Transportar carga y pasajeros por ferrocarril	5. Mantener el acceso a los historiales médicos	5. Producción y suministro de productos y servicios agrícolas
6. Prestación de servicios de redes de acceso de radiodifusión	6. Transportar carga y pasajeros por carretera	6. Gestionar los materiales peligrosos	6. Producción y suministro de productos y servicios de

[24] Definición de funciones críticas nacionales adaptadas de https://www.rand.org/pubs/research_reports/RRA1512-1.html

Conexión Comunicación	Distribución	Administración	Suministro
			alimentación humana y animal
7. Prestación de servicios de redes de acceso por satélite	7. Transportar carga y pasajeros por barco	7. Gestionar las aguas residuales	7. Producción de productos químicos
8. Prestación de servicios de redes de acceso inalámbricas	8. Transportar materiales por ductos, oleoductos o gasoductos.	8. Gestionar la administración pública	8. Suministro de metales y materiales
	10. Transporte masivo de pasajeros	9. Disponer de capacidades de gestión de incidentes cibernéticos	9. Suministro de viviendas
		10. Prepararse para las emergencias y gestionarlas	10. Suministro de productos y servicios de tecnología de la información
		11. Preservar los derechos constitucionales	11. Suministro de material y apoyo operativo a la defensa
		12. Proteger la información confidencial	12. Investigación y desarrollo
		13. Proporcionar y mantener infraestructuras (Física)	13. Suministro de agua
		14. Prestar servicios de mercados de capitales y actividades de inversión	
		15. Prestar servicios de banca comercial y de consumo	

Conexión Comunicación	Distribución	Administración	Suministro
		16. Prestar servicios de financiación y liquidez	
		17. Prestar servicios de gestión de identidad y servicios de apoyo fiduciario asociados	
		18. Prestar servicios de seguros	
		19. Prestar asistencia médica	
		20. Prestar servicios de compensación y liquidación de pagos	
		21. Proporcionar seguridad pública	
		22. Proporcionar financiación mayorista	
		23. Almacenar combustible y mantener reservas	
		24. Apoyar la salud de la comunidad	

B. Contexto/Población - Se basaría en la población afectada por la interrupción del sector. La escala de esta se define con base en el método Hanlon, el cual es una herramienta utilizada en el campo de la salud pública para priorizar problemas de salud y asignar recursos de manera efectiva. En ese sentido, se toma el componente de magnitud para entender el número de personas afectadas por el problema en relación con la población total. El cual se basa en una estimación a partir de Hanlon, J.J. y Pickent, George E. Public Health Administration and Practice. Ed 8.

- Bajo (1) = 99.999 o menos personas
- Moderado (2) = de 100.000 a 249.999 personas

- Alto (3) = de 250.000 a 499.999 persona
- Extremo (4) =Impacto potencial a 500. 000 o más personas

C. Impacto Operacional

Esta variable mide el impacto y alcance en el funcionamiento (servicios de la entidad, teniendo en cuenta la salud pública, área geográfica, entre otros, que se vería afectada en caso de interrupción del servicio de una infraestructura crítica. Se consideran aspectos como la cantidad de usuarios y la distribución geográfica de la infraestructura.

Bajo (1) = Nivel menor: El impacto que causa la materialización del riesgo en los objetivos de la entidad es mínimo. El impacto de la operación es pequeño en el territorio o la entidad.

Moderado (2) = Nivel moderado: La materialización del riesgo puede causar una pérdida momentánea. El impacto afecta momentáneamente pero breve la operación de la entidad y/o en los territorios.

Alto (3) = Nivel mayor: Genera retrasos importantes que afectan el cumplimiento de los objetivos. En esta parte se afecta la operación de la entidad y sus acciones en el territorio.

Extremo (4) = Nivel catastrófico: Puede detener la operación de la entidad, incluso, tener consecuencias como el cierre definitivo. Afecta la operación total de la entidad y su despliegue en territorio.

D. Afectación Económica Nacional

La afectación Económica nacional mide el impacto de un incidente económico en términos del PIB, tomando en cuenta lo siguiente:

Bajo (1) =Impacto menor al 0,1% del PIB

Moderado (2) = Impacto inferior del 0,1 al 0,5%

Alto (3) = Impacto del 0,5 al 1% del PIB.

Extremo (4) = Impacto mayor al 1% del PIB.

Lo que se mide de la siguiente manera:

Impacto económico en porcentaje del PIB = (Valor del impacto económico / PIB) * 100

El impacto se mide según los siguientes datos:

- PIB Colombia año 2023: 1,572,459.000.000
- Este valor se debe dividir sobre el valor del impacto[25] económico del sector/PIB *100.

Los datos del PIB enfoque de la producción se toman del DANE, en la tabla que se adjunta.

E. Impacto Nacional del Servicio: Incidentes que podrían afectar al servicio del Estado y otros sectores esenciales o con los que se tenga relación. Impacto de su servicio y la interdependencia con otro sector

[25] El valor del impacto económico se entrega acorde a la proyección del DANE por sectores

Ejemplos:

• Interrupciones

• Tiempo de inactividad

• Averías de equipos

• Problemas de seguridad/catástrofes naturales

• Pérdida de control

• Bajo (1) = Impacto muy bajo en la organización, improbable que afecte a otras organizaciones

• Moderado (2) = Supone un impacto potencial para la organización, posibilidad mínima de impacto para otras organizaciones

• Alto (3) = Tendrá un impacto en la organización, es probable que afecte a otras organizaciones

• Extremo (4) = Tendrá un impacto grave en la capacidad operativa de la organización, impacto conocido o previsto en otras organizaciones.

Estas son las 05 variables que se evalúan junto a esta se establece el tiempo de indisponibilidad y recuperación acorde a la siguiente escala:

Escala

Bajo (1) =. El tiempo de indisponibilidad del activo es de 24 horas o menos.

Moderado (2) = El tiempo de indisponibilidad del activo es de 24 a 72 horas.

Alto (3) = El tiempo de indisponibilidad del activo es de 72 horas a una semana.

Extremo (4) = El tiempo de indisponibilidad del activo es superior a una semana o no se puede determinar por su alto impacto

DELIMITACIÓN INFRAESTRUCTURA CRÍTICA CIBERNÉTICA										
Sectores	Gobierno/Estado					Comentarios		Entidades adscritas que hacen parte del sector		
Sub sector	Gasto									
Relación o sector de apoyo										
Actividad escenecial/Servicios prestados	Activos	Clasificación de incidente (tipo de incidente)	Tiempo de indisponibilidad	Impacto a la seguridad	Contexto y/o población afectada	Impacto operacional	Afectación económica nacional	Impacto nacional del servicio	Tiempo de recuperación objetivo del activo	Definición de ICC
Contratación pública del Estado	Portal Web	DoS (Denegación de Servicio)	1	4	1	4	3	4	1	2.83
Contratación pública del Estado	Base de datos	Phishing	2	4	4	4	3	4	2	3.50
Gestión de proyectos de inversión	Plataforma gestión pública	APT	2	4	4	4	1	4	2	3.17

Ilustración 4 Paso 3 identificación de ICC

Resultado de la evaluación se presenta la escala de las categorías y definiciones de Infraestructura crítica cibernética/ Servicios esenciales:

1. La ICC todo lo que en la evaluación de entre 2,45 a 4. (Categoría Crítico) - Extremo

2. Servicio Esencial: todo aquel que en la escala se encuentre entre 1,95 y 2,94. (Categoría Esencial) - Alto

3. Servicio no esencial, pero con impacto a la seguridad: todo entre 0.95 y 1.94. (Categoría importante) - Moderado

4. Activo que se contempla, pero no cumple un impacto a nivel nacional. – (Categoría Secundario) - Bajo

Importante:

Una vez, se diligencie la matriz en el formato Excel, la entidad representante de cada sector deberá diligenciar el anexo 2. *Estado actual de la infraestructura crítica cibernética de cada organización.* En el siguiente Link: https://forms.office.com/r/bvYF1QCBUF .

Posteriormente, deberá remitir al correo icc@colcert.gov.co la información que se encuentra en color verde, junto con el anexo 2 diligenciado y deberá ocultar la demás información con el fin asegurar su confidencialidad.

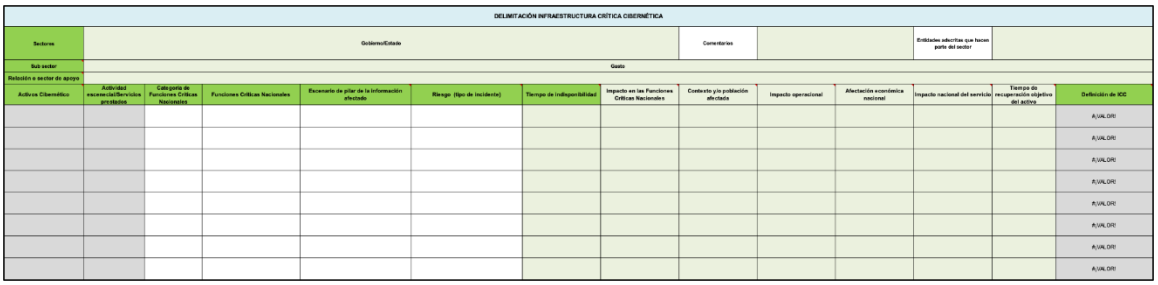
14. Fuentes

1. Catálogo de ICC, 2019, Consejo Privado de Competitividad, https://compite.com.co/wp-content/uploads/2019/06/ICC_2019_V1_VWeb.pdf
2. Cybersecurity and Crítical Infrastructure, 2020, Homeland Security, https://www.dhs.gov/archive/coronavirus/cybersecurity-and-crítical-infrastructure
3. Information Technology Sector-Specific Plan: An Annex to the NIPP 2013, 2016, Homeland Security, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf
4. Public Summary of Sector Security and Resilience Plans, 2018, Cabinet Office, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf
5. Methodologies for the identification of Crítical Information Infrastructure assets and services, 2015, ENISA, https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis
6. National Strategy for Crítical Infrastructure, 2009, Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
7. Artículo 333, 1991, Constitución Política de Colombia, https://www.constitucioncolombia.com/titulo-12/capitulo-1/articulo-333
8. Artículo 365, 1991, Constitución Política de Colombia, https://www.constitucioncolombia.com/titulo-12/capitulo-5/articulo-365
9. Ley 1341, 2009, Congreso de Colombia, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913
10. Decreto 338, 2022, Ministerio de Tecnologías de la Información y las Comunicaciones, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866
11. OECD Reviews of Risk Management Policies, Good Governance for Crítical Infrastructure Resilience, 2019, OECD iLibrary, https://www.oecd-ilibrary.org/sites/b1dac86e-en/index.html?itemId=/content/component/b1dac86e-en
12. Analysis of Crítical Infrastructure Dependencies and Interdependencies, 2015, Argonne National Laboratory, https://publications.anl.gov/anlpubs/2015/06/111906.pdf
13. National Strategy for Crítical Infrastructure, 2009, Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf
14. Framework for Improving Crítical Infrastructure Cybersecurity, 2018, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
15. Crítical Infrastructure Resilience Strategy, 2023, Cyber and Infrastructure Security Centre, https://www.tisn.gov.au/Documents/Australian+Government+s+Crítical+Infrastructure+Resilience+Strategy.pdf
16. Good Governance for Crítical Infrastructure Resilience, 2019, OECD, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/swissbasicstrategyforcríticalinfrastructureprotecti on.htm

17. Information Technology Sector-Specific Plan: An Annex to the NIPP 2013, 2016, Homeland Security, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf
18. Public Summary of Sector and Resilience Plans, 2018, Cabinet Office, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf
19. RAND Corporation. (2023). *Identifying and Prioritizing Systemically Important Entities*. https://www.rand.org/pubs/research_reports/RRA1512-1.html

15. ANEXOS:

Anexo 1. Delimitación de sectores (Matriz en formato Excel).



DELIMITACIÓN INFRAESTRUCTURA CRÍTICA CIBERNÉTICA

Sectores	Gobierno/Estado		Comentarios		Entidades adscritas que hacen parte del sector	
Sub sector	Gasto					
Relación o sector de apoyo						

Activos Cibernético	Actividad escencial/Servicios prestados	Categoría de Funciones Críticas Nacionales	Funciones Críticas Nacionales	Escenario de pilar de la información afectado	Riesgo (tipo de incidente)	Tiempo de indisponibilidad	Impacto en las Funciones Críticas Nacionales	Contexto y/o población afectada	Impacto operacional	Afectación económica nacional	Impacto nacional del servicio	Tiempo de recuperación objetivo del activo	Definición de ICC
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!

Impacto en las Funciones Críticas Nacionales	Contexto y/o población afectada	Impacto operacional	Afectación económica nacional	Impacto nacional del servicio	Tiempo de recuperación objetivo del activo	Definición de ICC
						#¡VALOR!
						#¡VALOR!
						#¡VALOR!
						#¡VALOR!
						#¡VALOR!
						#¡VALOR!

Activos Cibernético	Actividad escenecial/Servicios prestados	Categoría de Funciones Críticas Nacionales	Funciones Críticas Nacionales	Escenario de pilar de la información afectado	Riesgo (tipo de incidente)	Tiempo de indisponibilidad

Anexo 2. Estado actual de la infraestructura crítica cibernética de cada organización. (Actualizable cada año) https://forms.office.com/r/bvYF1QCBUF