El futuro digital es de todos

MinTIC

Relación con Proveedores de Seguridad Digital

MSPI

Modelo de Seguridad y Privacidad de la Información

Ministerio de Tecnologías de la Información y las Comunicaciones

MARZO DE 2022

Carmen Ligia Valderrama Rojas - Ministra de Tecnologías de la Información y las Comunicaciones

Iván Mauricio Durán Pabón - Viceministro de Transformación Digital

Ingrid Tatiana Montealegre Arboleda - Directora de Gobierno Digital

Oscar Eduardo Salazar- Subdirector (E) de Estándares y Arquitectura de TI

Angela J. Cortés H. – Líder del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT)

Danny A. Garzón A.– Asesor del equipo de Seguridad y Privacidad de la Información

Ivan A. Ontibon R.– Asesor del equipo de Seguridad y Privacidad de la Información

Felipe Sarmiento H.- Asesor del viceministerio de Transformación Digital

Ministerio de Tecnologías de la Información y las Comunicaciones

Viceministerio de Transformación Digital

Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 1 10/03/2022	Creación de la propuesta de documento para observaciones de las múltiples partes interesadas.

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

Modelo de Seguridad y Privacidad de la Información

Roles y Responsabilidades V 4.0

Esta guía de la Dirección de Gobierno Digital se encuentra bajo una Licencia Creative Commons Atribución 4.0 Internacional.

Contenido

1. Relación con proveedores de seguridad digital

Las entidades estatales del orden nacional y territorial requieren mantener relaciones con proveedores al adquirir productos o servicios. Ahora bien, cuando los productos y servicios se adquieren para la gestión de la Seguridad Digital dichos proveedores pueden tener acceso directo o indirecto a la información y los sistemas de información de las entidades estatales, o proporcionarán elementos (software, hardware, procesos o recursos humanos) que estarán involucrados en el procesamiento de la información. Asimismo, Las Entidades también pueden tener acceso físico o lógico a la información de los proveedores cuando controlan o monitorean los procesos de producción y entrega de los bienes y servicios adquiridos.

Por lo tanto, las entidades y los proveedores pueden causar riesgos de Seguridad Digital mutuos. Estos riesgos deben ser evaluados y tratados tanto por las entidades como por las organizaciones proveedoras mediante una gestión adecuada de la seguridad de la información y la implementación de los controles pertinentes.

Así las cosas, este anexo proporciona una guía sobre los aspectos más relevantes a tener en cuenta en las relaciones con proveedores de productos y servicios de seguridad digital para las entidades del estado.

La información puede estar en riesgo cuando los proveedores tienen una gestión de seguridad de la información inadecuada en especial porque los proveedores de seguridad informática tienen acceso a información crítica respecto a: vulnerabilidades, registros de auditoría (logs), direccionamiento interno, información tecnología y versiones de la infraestructura de TI que soporta los procesos misionales de las entidades, por esta razón se debe identificar la información a la que pueden tener acceso estos proveedores y los permisos de las operaciones que pueden realizar sobre esta información, así mismo se deben identificar los controles y aplicarlos para mantener los niveles de seguridad adecuados para la información que tratan estos proveedores. Por ejemplo, si hay una necesidad especial de confidencialidad de la información, se pueden usar los acuerdos de no divulgación.

Otro ejemplo son los riesgos de protección de datos, cuando el acuerdo con los proveedores incluye la transferencia o acceso de información a través de fronteras (fuera del país), en este sentido tanto los proveedores nacionales, como internacionales deben cumplir las normas y directrices establecidas en materia de seguridad digital en sus relaciones con entidades del Estado.

La entidad estatal necesita tener conciencia de que la responsabilidad legal o contractual respecto a la protección de datos sigue siendo de esta, aunque la información este siendo tratada por un proveedor. Por ello debe verificar la implementación de los controles establecidos para mitigar los riesgos en los activos de información de los terceros que participen en el tratamiento de información de la entidad y que estos sean acordes a su criticidad y a los planes de tratamiento establecidos en el análisis de riesgos, incluyendo los riesgos asociados a posibles migraciones consecuencia de cambio de proveedores, así como el uso de herramientas y servicios de seguridad de diferentes fabricantes.

El responsable de seguridad de la información de la entidad debe participar activamente en el análisis y ejecución de cada uno de los puntos que se indican en la presente guía.

El presente anexo fue realizado tomando como referencia la norma ISO 27036, la cual brinda elementos detallados para tener en cuenta en la Seguridad de la información para las relaciones con proveedores.

2. Planificación de las relaciones con Proveedores

Para gestionar adecuadamente la seguridad de la información en las relaciones con proveedores, las entidades estatales deben establecer un plan de relación con proveedores que documente la decisión adoptada por el nivel directivo de adquirir 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 adquirir un producto o servicio relacionado con activos de información, así como las consideraciones de seguridad de la información relacionadas con esta contratación.
Propósito:	Gestionar con la debida diligencia 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

- 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:
    - Documentación existente de gestión de relaciones con proveedores, como planes y acuerdos de relaciones con proveedores.

Salidas

- Plan de evaluación y tratamiento de riesgos de seguridad de la información asociados al producto o servicio que se contrate;
- 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;
- 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.
- Plan de relación con proveedores.

Actividades para 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 Modelo de Seguridad y Privacidad de la Información (MSPI) y en la estrategia de relación con proveedores.

- La entidad deberá garantiza que esta evaluación de riesgos de seguridad de la información:

  1) Sea proporcional a la criticidad del producto o servicio que se planea adquirir;

  2) Tenga 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.

  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.

  Deberá 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.
- Definir el plan de evaluación y tratamiento de riesgos de seguridad de la información para el cumplimiento del objetivo, alineado con la metodología aplicable para la entidad 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 citado plan 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. 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.
II. Propiedad intelectual de terceros; y
III. 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 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.

3. Selección de proveedores

Para gestionar con la debida diligencia 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 informática 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 la debida diligencia 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.	• Nuevos criterios de seguridad para la selección de proveedores específicos para los productos o servicios a adquirir. • Acuerdos de confidencialidad específicos para los productos o servicios a adquirir. • Permisos que tendrá el proveedor sobre la información y los activos identificados. • 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. • Resultados de la evaluación del cumplimiento de los requisitos de seguridad de la información de los proveedores.

	• 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 para realizar por parte de la entidad estatal contratante:

- Definir e implementar criterios de selección de proveedores que contengan especificaciones del producto o servicio que se puede contratar y en el marco de los 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;
  - Madurez del proveedor en seguridad de la información. Esta madurez se puede definir verificando, de cualquier manera, que el proveedor implemente controles en Seguridad de la Información, a partir del cumplimiento de estándares internacionalmente reconocidos, o que proporcione documentación de su sistema de gestión de seguridad de la información, como planes de continuidad de negocio documentados y probados, o planes para garantizar su capacidad de admitir activaciones simultáneas por parte de diferentes clientes de planes de recuperación y gestión de incidentes.
  - 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;
  - Se realizará una aceptación transitoria de la política de seguridad de la información por parte del proveedor, incluyendo los acuerdos de confidencialidad de la entidad, cuando el producto o servicio a contratar haya sido previamente explotado, por la entidad o por otro proveedor; Establecer los lineamientos en el contrato para la terminación contractual, cuando se evidencie una falta a las políticas de seguridad de la información que ponga en riesgo los activos de información de la entidad según lo establecido en el análisis de riesgo existente.
- 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.

- Los documentos que hagan parte del proceso contractual deberán contener información suficiente para que el proveedor pueda preparar su propuesta con fundamento a criterios jurídicos, técnicos y financieros. En particular, 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; y

  4) 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 debe contener contenido público o desclasificado. Dicho documento debe contener la información necesaria para permitir que el proveedor responda justificativamente.

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.

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.

4. 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 velar por 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 de negociación de acuerdos con proveedores.
Propósito:	Gestionar con la debida diligencia 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

- Decisión sobre quién llevará a cabo las actividades de supervisión del proveedor;
- Resultados anteriores de las actividades de seguimiento y cumplimiento de los proveedores.

Salidas

- Evaluación de riesgos de seguridad de la información e informes de auditoría relacionados con las actividades de supervisión y ejecución del cumplimiento.

Cuando aplique:

- 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;
- Informe de ejecución del plan de migración;
- Historial de cambios de seguridad de la información e informes asociados;

	• Historial de incidentes de seguridad de la información e informes asociados; • Acuerdo de relación con proveedores actualizado; • 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;
- 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;
- Capacitar periódicamente al personal que pueda estar involucrado en la ejecución del plan de terminación de contratos;
- 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, entre ellos :
    - 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;
    - 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:

    1) identificar y evaluar los impactos en la seguridad de la información resultantes de estos cambios o auditar las no conformidades;

2) Determinar si se deben reconsiderar los aspectos de seguridad de la información definidos en el contrato con el proveedor;

3) 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.

5. 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 la debida diligencia 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.	• Informes periódicos de los servicios o productos que evidencie el cumplimiento de los indicadores establecidos. • Evidencias de reuniones periódicas de seguimiento acorde a lo establecido en las cláusulas y según requerimiento del supervisor del contrato. • Resultados de revisiones técnicas, administrativas o auditorias de cumplimiento en búsqueda de acciones de mejora o verificación del cumplimiento requerido

Actividades para 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 (modelo de responsabilidad compartida), por lo cual se recomienda:

a) Asegurar que los documentos y pólizas se encuentren vigentes durante el periodo de ejecución, en caso de prórrogas estar atentos a las actualizaciones contractuales pertinentes.

b) Realizar revisiones periódicas a los documentos, planes y procedimientos entregados por el proveedor, sobre los cuales basen 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 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) El proveedor debe adoptar los procedimientos de la entidad contratante o adaptar sus procesos existentes según corresponda, 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 a las capacitaciones.

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 de terminación del contrato que incluya: 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

6. 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 esté funcional según corresponda, para así evitar impactos operacionales, legales o económicos.

Es preciso tener presente los tiempos, documentos y elementos requeridos para el cierre del contrato, 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 la debida diligencia 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. • Activación del plan de continuidad del negocio, verificación de controles existentes y respaldo de información o dispositivos según corresponda.	• Acta de finalización del contrato avalada y firmada por el supervisor, en el cual certifica el cierre de la relación contractual. • Informe de lecciones aprendidas durante el tiempo del servicio y en el cierre del contrato.

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) Conformar 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 llegaren a presentarse, la forma de mitigarlos y las desviaciones que puedan reflejarse en el cronograma por la materialización de las amenazas.

   Nota: en el evento tal que el servicio deba ser entregado de un proveedor a otro, deberá conformarse 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: El proveedor 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 la cual certifique el cierre del proceso contractual.

h) Verificar el cambio de credenciales de acceso, eliminación de usuarios y cierre de conexiones remotas al proveedor saliente.