INFORME DE AUDITORÍA INTERNA DE SISTEMAS DE GESTIÓN

FECHA	DÍA	MES	AÑO
Apertura	25	8	2021
Cierre	31	8	2021
Emisión del Informe	6	9	2021

SISTEMA DE GESTIÓN AUDITADO
Sistema de Gestión de Seguridad de la Información
Ciclo de Auditoría (Periodo a Auditar)
2020 -2021

Líder Sistema de Gestión Auditado **Andrés Diaz Molina** **Correo electrónico** adiazm@mintic.gov.co

EQUIPO AUDITOR QUE REALIZÓ LA AUDITORÍA INTERNA			
Nombre	**Rol**	**Nombre**	**Rol**
Harley Roldán Silva hroldan@mintic.gov.co	Auditor Líder	Rafael Hernando Calle Cabezas (rcalle@mintic.gov.co)	Auditor
Danny Alejandro Garzón Aristizabal dgarzon@mintic.gov.co	Auditor	Iván Alexis Ontibon Rojas (iontibon@mintic.gov.co)	Auditor
Hasblady González Engativá (hgonzaleze@mintic.gov.co) En formación	Auditor	Fredy Alfonso De la Ossa Rojas (fdelaossa@mintic.gov.co)	Auditor

INTRODUCCIÓN

El ejercicio de auditoria interna al Sistema de Gestión de Seguridad de la Información en MinTIC, se concentró en determinar la conformidad del mismo frente la Norma NTC-ISO/IEC 27001:2013, en cuanto a su implementación, ejecución, eficiencia, fortalezas y mejora, a partir de unos criterios definidos y desarrollados mediante un concreto plan de auditoría.

Con un equipo auditor bien formado, de suficiente experiencia y cuyo ánimo de buen trabajo destaca su independencia y objetividad, este informe detalla las diez (10) no conformidades que corresponden a situaciones menores no repetitivas y que pueden y debe subsanarse en los términos establecidos en los procedimientos correspondientes del sistema; así mismo se muestran las ocho (8) observaciones realizadas al sistema y que se recomienda sean evaluadas y si se requiere inmersas en planes de mejoramiento para evitar que terminen convirtiéndose en no conformidades para el sistema; también se hacen recomendaciones que pueden redundar en la mejora del sistema y en el fortalecimiento de la operación de la seguridad de la información.

En términos generales el Ministerio refleja una correcta implementación de su Sistema de Gestión de Seguridad de la Información respecto al cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables, por lo que se identifica el compromiso a nivel general de la entidad y en los procesos; esto sin que se deba limitar la socialización e implementación de controles adicionales y fortalecer la parte documental enfocada en el ciclo de vida PHVA para llegar a un nivel de adaptabilidad y concienciación mayor.

Finalmente, es importante destacar que los controles seleccionados para cumplir con la conformidad respecto a la norma ISO/IEC 27001:2013, cumplen con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de la información tratada en el ministerio.

Claiificación del Hallazgo

NC-ME (No Conformidad Menor)**:** Incumplimiento de un requisito de la ISO o de un apartado del standar o de un criterio de la auditoria.

NC-MA (No Conformidad Mayor): Incumplimiento grave o reiterativo de un de un requisito completo o apartado completode un criterio.

OBS (Observación): Evidencias encontadas que pueden generar en un futuro una No Conformidad. a la fecha no se ha incumplido ningún requisito, apartado o criterio, sin embargo, si no se hace un tratamiento adecuado, en la siguiente auditoría puede dejarse como no conformidad.

Alcance de la Auditoría Interna

La Auditoría al SGSI MinTIC tiene alcance a los procesos del Ministerio/Fondo Único de TIC, a todos los niveles funcionales y organizacionales del Ministerio/Fondo Único de TIC, a los funcionarios, contratistas y aquellas personas que dentro de la entidad que utilicen, recolecten, procesen e intercambien información; se incluye en este alcance las Bases de Datos, redes y aplicaciones críticas de negocio, así como las instalaciones de Ministerio/Fondo Único de TIC que se ubica en el Edificio Murillo Toro Carrera 8a entre calles 12A y 12B Bogotá, Colombia, y en los data-center o centros de replicación de datos propios o contratados. La vigencia que se evalúa comprende desde el 01/01/2020 al 01/08/2021.

Objetivos de la Auditoría Interna

General	Específicos
Determinar la conformidad del sistema de gestión de Seguridad de la Información del MinTIC, con los criterios de la norma NTC ISO/IEC 27001:2013; evaluando la capacidad del sistema de gestión para asegurar que la entidad cumple los requisitos legales, reglamentarios y contractuales aplicables; así como evalúar su eficacia e identificar las áreas de mejora.	1. Establecer la conformidad del Sistema de Gestión de Seguridad de la Información de acuerdo con la implementación de las cláusulas y controles de la norma NTC ISO/IEC 27001:2013. 2. Valorar la capacidad del Sistema de Gestión para asegurar que la entidad cumple los requisitos legales, reglamentarios y contractuales aplicables. 3. Determinar el nivel de eficacia del sistema de gestión e identificar los procesos que requieran implementar otros controles adicionales.

Criterios de la Auditoria Interna

NTC -ISO/IEC 27001:2013
Ley 1273 DE 2009
LEY 1581 DE 2012
DECRETO 1377 2013
SISTEMA DE GESTIÓN DOCUMENTAL
Guía de auditoría interna basada en riesgos para entidades públicas - Versión 4 - Julio de 2020
SPITICMA-001 MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
SPITICPR-001 GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
GDO-TIC-MA-014 MANUAL DE ACTIVOS DE INFORMACIÓN v 3.0
RESOLUCIÓN NÚMERO 000924 DEL 4 JUN 2020 "Por la cual se actualiza la Política de Tratamiento de Datos Personales del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 2007 de 2018"
RESOLUCIÓN NÚMERO 002256 DE 06 DE NOVIEMBRE DE 2020
Demás normas o documentos que apliquen.

RESULTADOS DE LA AUDITORÍA INTERNA

1. Fortalezas

1. Se identifica un cumplimiento muy alto en el cumplimiento de la norma, incluyendo la identificación de riesgos y controles ejecutados.
2. La definición de los roles y las responsabilidades respecto a la seguridad de la información y las competencias del personal designado cumple con las necesidades de la entidad para definir los lineamientos pertinentes garantizando la confidencialidad, integridad y disponibilidad de la información tratada por el Ministerio.
3. Se destaca el compromiso de los procesos en su disposición y argumentación de los controles, frente al ejercicio realizado de la auditoría interna.
4. Se denota una dedicación por parte de los procesos y de la entidad para dar cumplimiento a la Política General de Seguridad y Privacidad de la Información reflejado en un avance significativo de implementación al cumplimiento de la norma.
5. La definición de los roles y las responsabilidades respecto a la seguridad de la información y las competencias del personal designado cumplen con las necesidades de la entidad para definir los lineamientos pertinentes, garantizando la confidencialidad, integridad y disponibilidad de la información tratada por el ministerio.
6. Se destaca el interés de la entidad en la continuidad del negocio, ejerciendo de manera constante las actividades generales y relacionadas con la seguridad de la información.

2. Hallazgos de la Auditoría Interna

Requisito Incump.	Describe Requisito / Objetivo Control	Clasificación	#	Descripción Hallazgo	Recomendación
5.1	LIDERAZGO Y COMPROMISO Literal b. asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización.	NC-ME	1	MIG-TIC-CD-001 FORTALECIMIENTO ORGANIZACIONAL Revisadas las Cartas descriptivas de todos los procesos del MIG, se observa que en el apartado que corresponde a "Normas técnicas aplicables", no se enuncian las normas y requisitos puntuales que debe cumplir cada proceso en relación con la NTC-ISO/IEC 27001:2013.	Modificar las cartas descriptivas de manera que se indique explicitamente, cuáles requistos de seguridad de la información descritos en la NTC-ISO/IEC 27001:2013 se deben cumplir cada proceso.
9.1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información. Capítulo 5. Elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado, artículo 17, del Decreto 648 de 2017 que modifica el artículo	NC-ME	2	EAC-TIC-CD-001 EVALUACIÓN Y APOYO AL CONTROL DE LA GESTIÓN A pesar de estar definido en la carta descriptiva del proceso como objetico “realizar evaluación independiente y objetiva del Sistema de Gestión Integral”, la OCI no la lleva a cabo, debido a que su responsabilidad es diferente y se encuentra enmarcada en la ley 87/93 y en la Guía de auditoría interna basada en riesgos para entidades públicas, donde indica que se enfoca en una evaluación independiente y objetiva del sistema de control interno y su relación con otras políticas aplicables al Sector Público; funciones que tampoco están descritas ni en el objetivo ni en el y alcance del documento (EAC-TIC-CD-001 EVALUACIÓN Y APOYO AL CONTROL DE LA GESTIÓN).	Modificar la carta descriptiva del proceso de manera que su objetivo sea coherente con las funciones que le corresponden, según la LEY 87 DE 1993 noviembre 29 “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado" y las demás disposiciones que le sean aplicables.

6.1.3	Tratamiento de riesgos de la seguridad de la información Literal d) producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A;	NC-ME	3	SPI-TIC-CD-001 – SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Se ha producido la Declaración de Aplicabilidad con los controles necesarios para operar el SGSI y su justificación, sin embargo, en el sistema no se han documentado o excluido formalmente procedimientos que no fueron presentados en la auditoria para: 1. Gestión de medios removibles 2. Disposición de los medios 3. Procedimiento de ingreso seguro 4. Trabajo en áreas seguras (GTI-TIC-FM-016 Control de acceso áreas seguras de tecnologías) 5. Instalación de software en sistemas operativos 6. Políticas y procedimientos de transferencia de información – (SPI-TIC-FM-005 TRANSFERENCIA DE BASES DE DATOS CON DATOS PERSONALES A ENTIDADES EXTERNAS) 7. Procedimientos de control de cambios 8. Recolección de evidencia 9. Derechos de propiedad intelectual 10. Gestión con proveedores	Implementar y/o exluir mediante la Declaración de Aplicabildiad los procedimientos que demandan los controles del Anexo A. Establecer la relación de los controles con los procesos del Sistema.
A.18.11	Identificación de la legislación aplicable y de los requisitos contractuales.	NC-ME	4	SPI-TIC-CD-001 – SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN No se identifica en la matriz de requsitos legales los sistemas de información a los que aplican estos requisitos. Dado que los sistemas de información pueden ser diferentes y las normas que lo aplican también, se genera el riesgo de no poder identificar todos los requisitos legales necesarios para cumplir con la seguridad de la información.	Se recomienda incluir dentro de la matriz de requisitos legales los sistemas de información a los que les aplica. El control establece que los requisitos estatutarios, reglamentarios y contractuales pertinentes se deberían identificar y documentar explícitamente y mantenerlos actualizados para "cada sistema de información

A.6.1.5	Seguridad de la información en la gestión de proyectos.	NC-ME	5	ACT-TIC-CD-001 ACCESO A LAS TIC Ni en el manual de la metodología de Gerencia de Proyectos (DES-TIC-MA-008), ni en la gestión de proyectos se identifica incluida la seguridad de la información. El proceso de Acceso a las TIC presentó varias alternativas y estrategias para soportar el cumplimiento de la seguridad de la información en los proyectos, sin embargo, dado que existe una metodología definida por la entidad, se debe incluir en la misma la seguridad de la información de los proyectos.	Se recomienda, en cabeza del líder del sistema y del responsable de la metodología, incluir la seguridad de la información en este documento.
A.11.2.8	Equipos de usuario desatendido.	NC-ME	6	ACT-TIC-CD-001 ACCESO A LAS TIC El control establece que los equipos desatendidos se les debe dar una protección apropiada, para lo cual se identifica que en el Manual de políticas de seguridad y privacidad de la información (PI-TIC-MA-001, Código: SI-A.9.4 – Control de Acceso a Sistemas y Aplicaciones. Ítem d), se estableció que las sesiones inactivas deben cerrarse después de un período de inactividad de 3 minutos y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo. Pese a lo anterior, se realizó la validación en los Sistemas de Información: SIMIG, ASPA, INTEGRATIC (tanto en el MinTIC como en trabajo en casa con VPN conectada) y posterior a los 5 minutos, no se identificó un bloqueo o sesiones inactivas en los SI.	Se recomienda configurar todos los sistemas de información para que después del tiempo de inactividad definido, se cierren o bloqueen de acuerdo con el control y la directriz de manual de políticas de seguridad de la información.

A.11.2.9	Politica de escritorio limpio y pantalla despejada.	NC-ME	7	ACT-TIC-CD-001 ACCESO A LAS TIC El control indica que se debería adoptar un política de escitorio limpio, para lo cual se identifica que en el Manual de políticas de seguridad y privacidad de la información (PI-TIC-MA-001, Código: SI-A.11.2 – Equipos, ítem x) que define que la Oficina de Tecnologías de la Información debe configurar como política general que todos los equipos de cómputo que se encuentren en los dominios del Ministerio/Fondo Único de TIC oculten de manera automáticas los iconos, accesos directos o documentos que se encuentren en el escritorio, para lo cual se identificó que esta configuración no se encuentra aplicada o configurada.	Se recomienda configurar y aplicar el control definido en el Manual de políticas de seguridad y privacidad de la información con respecto al ocultamiento de los íconos del escritorio.
A.12.1.2	Gestión de cambios.	NC-ME	8	GTI-TIC-CD-001 GESTIÓN DE TI El control establece que se deben gestionar los cambios en los sistemas de procesamiento de la información que afectan la seguridad de la información, sin embargo, se identifica que el procedimiento de "Gestión de cambios normales" (GTI-TIC-PR-011) establece en su objetivo que aplica solo para el ambiente de producción, por lo cual no se identifica cuál es la gestión del cambio que se realizan en los ambientes de pruebas y desarrollo y cómo se garantiza la seguridad de la información.	Se recomienda actualizar la documentación existente para garantizar que la gestión de cambios aplica a todos los ambientes garantizando la seguridad de la información.
A.10.1.2	Gestión de llaves	NC-ME	9	GTI-TIC-CD-001 GESTIÓN DE TI No se evidencia la existencia de una política de gestión de llaves criptográficas en el cual se evidencie el ciclo desde su creación hasta el retiro y destrucción de llaves criptográficas.	Se debería contar con una política de gestión de llaves criptográficas, que indique el ciclo de vida y los roles responsables del desarrollo de la actividad

A.11.2.3	Seguridad del cableado	NC-ME	10	No se evidencia el cumplimiento del control "A.11.2.3: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño", toda vez que no se entregó a la auditoría evidencia fotográfica de la protección existente para cableado, cajas de conexión y dispositivos de interconexión y la respectiva política de control de acceso.	Se insta a la implementación de los controles y a conservar las evidencias de su operación para cuando sean requeridos por auditorías internas o entidades de control.

3. OBS (Observación)

GTI-TIC-CD-001 GESTIÓN DE TI
Se evidencia que aunque el manual SPI-TIC-MA-001 MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN en su numeral 6.8. LINEAMIENTOS DE SEGURIDAD DE LAS COMUNICACIONES define que La Oficina de Tecnologías de la Información debe establecer los procedimientos para el direccionamiento y transporte correctos del mensaje, así como la confiabilidad y disponibilidad del servicio, estos procedimientos no se encuentran documentados.
7.5 INFORMACIÓN DOCUMENTADA
7.5.1 Generalidades.
Se recomienda Crear la documentación necesaria para la eficacia del sistema de gestión de la seguridad de la información de acuerdo a la categoria establecida en el manual de politicas de seguridad y privacidad de la información. (Procedimientos, guias, manuales, etc.)

SPI-TIC-CD-001 – SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Pese a que se tienen adecuadamente identificados los objetivos, que son coherentes con lo definido en la política de seguridad de la información y que se hace seguimiento a los mismos, estos objetivos no son medidos a través de indicadores, no se cuenta con línea base, metas y ni resultados de ese tipo de mediciones.
6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS, Literal b, Los objetivos de seguridad de la información deben ser medibles (si es posible).
Se recomienda Iniciar la medición de los objetivos a través de planes individuales que permitan conocer el avance cuantitativo de cada uno de los mismos y establecer indicadores, línea base, y metas.

CES-TIC-CD-001 COMUNICACIÓN ESTRATÉGICA
En virtud de las necesidades que en materia de comunicación presentan los diferentes Sistemas de Gestión, en el Plan de comunicación estratégicas, se debe definir explícitamente los sistemas que serán apoyados o beneficiados en materia de estrategia de comunicaciones internas y externas, durante una vigencia o periodo.
7.4 COMUNICACIÓN

SPI-TIC-CD-001 – SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Los listados de contactos con autoridades y grupos de interés no describen la forma, el medio o canal de comunicación (correo electrónico, dirección física, sede electrónica o números telefónicos), ni los procedimientos establecidos que especifiquen cuándo y a través de quienes se debería intercambiar información.
A.6.1.3 Contacto con las autoridades
A.6.1.4 Contacto con las autoridades Contacto con grupos de interés especial

SPI-TIC-CD-001 – SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
La política para dispositivos móviles no se encuentra actualizda, ni cuenta con las medidas de seguridad y de soporte, que sean consecuentes con la realidad que vive el MInTIC para gestionar los riesgos introducidos por el uso de éstos dispositivos.
A.6.2.1 Política para dispositivos móviles.
GTI-TIC-MA-012 Manual de Política Trae tu Propio Dispositivo
Se deben actualizar y aplicar la política para dispositivos móviles y unas medidas de seguridad y de soporte, que sean consecuentes con la realidad que vive el MInTIC para gestionar los riesgos introducidos por el uso de éstos dispositivos.

GTH-TIC-CD-001 GESTIÓN DEL TALENTO HUMANO
Aunque se realizó una capacitación a los gerentes públicos sobre temas de corrupción y derecho disciplinario, es requerido que a todos los empleados se les realice la comunicación o socialización del proceso disciplinario de acuerdo con el control.
A.7.2.3 Proceso disciplinario.

GRA-TIC-CD-001 GESTION DE RECURSOS ADMINISTRATIVOS
Durante la entrevista, se evidencia que los colaboradores desconocen los lineamientos que se relacionan con la ubicación de los equipos para reducir los riesgos de seguridad de la información y acceso no deseado a información privilegiada.
A.11.2.1 Ubicación y protección de los equipos
Se recomienda implementar lineamientos para garantizar que los equipos a cargo del MinTIC, cumplan con los criterios de seguridad de la información.

SPI-TIC-CD-001 – SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Es necesario modificar la Declaración de aplicabilidad de manera que se indique explícitamente que se trata de la justificación de la inclusión o no de uno o varios controles y establecer la relación de los controles con los procesos del Sistema.
6.1.3 Tratamiento de riesgos de la seguridad de la información
La organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de
la información, Literal d) producir una declaración de aplicabilidad que contenga los controles necesarios
(véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A.

Cantidad de No Conformidades encontradas	10

Cantidad de Observaciones encontradas	8

4. Oportunidades de Mejora

DES-TIC-CD-001 DIRECCIONAMIENTO ESTRATÉGICO
El documento "Partes Interesadas SPI-TIC-DI-010" se identifica información como "Logros y resultados esperados" que se puede utilizar para complementar el Plan de Comunicaciones y/o a análisis DOFA, con el objetivo de ver referenciados los mismos en los mapas de riesgos de la entidad o de sus procesos.
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO.

DES-TIC-CD-001 DIRECCIONAMIENTO ESTRATÉGICO
La auditoría realizada fue dirigida a un proceso específico, sin embargo, algunas preguntas fueron atendidas por otros funcionarios de otros procesos como del GIT de Transformacion Organizacional o seguridad de la información. Aunque es un gran apoyo tranversal a la entidad, se sugiere para alcanzar la mejora, permitir que el proceso sea quien realice las intervenciones correspondientes .

5.2 POLÍTICA
La política de la seguridad de la información debe: f) comunicarse dentro de la organización.

GTH-TIC-CD-001 GESTIÓN DEL TALENTO HUMANO
Incluir en el proceso disciplinario, cuáles son las situaciones que pueden impactar la seguridad de la información como por ejemplo: Violaciones a la Privacidad y confidencialidad de la Información, Incidentes de Seguridad de la información, Piratería informática, Fraude y espionaje, entre otros.
ISO/IEC 27002. 7.2.3 Proceso disciplinario. "El proceso disciplinario formal debería proveer una respuesta gradual que tenga en cuenta factores tales como la naturaleza y la gravedad de la violación y su impacto sobre el
negocio; si es o no su primera infracción"

ACT-TIC-CD-001 ACCESO A LAS TIC
Aunque se identifican documentos independientes para gestionar los cambios en la organización para algunos procesos con relación a necesidades particulares (Gestión de Compras y Contratación, Actualización en el ASPA, entre otros), se observa como oportunidad, implementar un procedimiento formal de aprobación de cambios transversal en la entidad que facilite la mejora continua en todos los procesos.
ISO/IEC 27002. A.12.1.2 ítem d) El procedimiento de aprobación formal para los cambios propuestos.

GRA-TIC-CD-001 GESTION DE RECURSOS ADMINISTRATIVOS
Se visualizan 35 áreas seguras, los auditados manifiestan que faltan otras áreas que no se encuentran en el manual. Adicional a esto, presuntamente no hay un control de acceso a través de las escaleras, de esta manera personal no autorizado puede acceder a áreas seguras; por esta razón se considera relevante mejorar la aplicación de controles de seguridad a través de ampliar el perímetro de seguridad física a esos espacios o áreas seguras.
A.11.1.1. Perímetro de seguridad física

AGI-TIC-CD-001 GESTIÓN DE ATENCIÓN A GRUPOS DE INTERÉS
Transcurrieron mas de 3 años para realizar la primera actualización de la caraterización de grupos de interes por área. Se debe realizar con una periodicidad menor, debido a que el conexto interno y externo puede cambiar.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

AGI-TIC-CD-001 GESTIÓN DE ATENCIÓN A GRUPOS DE INTERÉS
Socialización de campañas de sensibilización sobre Seguridad de la Información
Es necesario para alcanzar la mejora, delegar al menos a un funcionario para asistir a las sensibilizaciones de Seguridad de la Información, y este deberá realizar las transferencia en el área.
5.2 POLÍTICA
La política de la seguridad de la información debe: f) comunicarse dentro de la organización.

GDO-TIC-CV-001 GESTIÓN DOCUMENTAL
Se hace necersario realizar socialización y transferencia recurrente de los temas y tips de seguridad de la información a proveedores y contratista. En este caso, ARKADOCS, proveedor encargado de la gestión y administración del archivo físico.
A.15.1.1
Política de seguridad de la información para las relaciones con proveedores

GDO-TIC-CV-001 GESTIÓN DOCUMENTAL
En coordinación con Seguridad de la Información y Fortalecimiento organizacional; el procedso de gestión documental, tiene los elementos necesarios para generar aquellos procedimientos que demandan los controles y que se convierten en obligatorios para el SGSI.

IDI-TIC-CD-001 INVESTIGACIÓN DESARROLLO E INNOVACIÓN Al inicio del contrato o durante la ejecución de los contratos, se deben dar charlas de sensibilización de las políticas o recomendaciones internas sobre segruridad de la información y entregar aquellos documentos de seguridad de la información que son de interés para las partes. A.15.1.1 Política de seguridad de la información para las relaciones con proveedores
IDI-TIC-CD-001 INVESTIGACIÓN DESARROLLO E INNOVACIÓN Además de la obligación general en los contratos, es importante y necesario dejar explicitamente en cada contrato o convenio una cláusula u obligación relacionada con el cumplimiento de la política de seguridad de la entidad. A.15.1.1 Política de seguridad de la información para las relaciones con proveedores.
IDI-TIC-CD-001 INVESTIGACIÓN DESARROLLO E INNOVACIÓN Debido a la claridad de los contratos, existe la posibilidad de evidenciar el seguimiento y monitoreo de los requisitos de seguridad en proveedores de servicios externos, así como acciones rutinarias y auditorias para cumplir con los requisitos de seguridad. A.15.1.1 Política de seguridad de la información para las relaciones con proveedores
GTH-TIC-CD-001 GESTIÓN DEL TALENTO HUMANO Implementar estrategias adecuadas para la comunicación y apropiación de las politicas de seguridad de la información a los colaboradores del ministerio, tales como chralas, talleres, inducciones y realizar peiodicamente mediciones que permitan evaluar y verificar el grado de aporpiación de las politicas de seguridad de la información A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información
GTI-TIC-CD-001 GESTIÓN DE TI Establecer a intervalos planificados y documentar las revisiones de los logs (registros de auditoria) de las actividades de los usuarios con accesos privilegiados (administradores) con el objetivo de verificar las acciones realizadas por estos usuarios. A.9.2.5 Revisión de los derechos de acceso de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado
UAT-TIC-CD-001 USO Y APROPIACIÓN EN TIC En intervalos planificados se debe evaluar el nivel de apropiación del equipo de trabajo de los proveedores sobre la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios en el Ministerio de Tecnologías de la Información y las Comunicaciones. A.15.1.1 Política de seguridad de la información para las relaciones con proveedores

UAT-TIC-CD-001 USO Y APROPIACIÓN EN TIC
Al presentar formatos adicionales que no se encuentren contemplados, registrados y avalados en el sistema de gestión, en el procedimietno específico; es necesario indicarlo (Documento no controlado o instrumento de gestión y hacerlo conocer del auditor antes de iniciar la evaluación delregistro)
7.5 INFORMACIÓN DOCUMENTADA
7.5.1 Generalidades
El sistema de gestión de la seguridad de la información de la organización debe incluir:
b) la información documentada que la organización ha determinado que es necesaria para
la eficacia del sistema de gestión de la seguridad de la información.

5. Conclusiones

1. Una vez realizado el ejercicio de auditoría interna al Sistema de Gestión de Seguridad de la Información en MinTIC, se establece conformidad con la Norma NTC-ISO/IEC 27001:2013, en cuanto a su implementación, ejecución, eficiencia, fortalezas y mejora, toda vez que las no conformidades detectadas corresponden a situaciones menores no repetitivas y que pueden y debe subsanarse en los términos establecidos en los procedimientos correspondientes del sistema.

2. El Ministerio refleja una correcta implementación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 en cuanto al cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables, y se identifica el compromiso a nivel general de la entidad y de cada uno de los procesos; es importante continuar con la socialización e implementación de más controles y fortalecer la parte documental enfocada en el ciclo de vida PHVA para llegar a un nivel de adaptabilidad y concienciación mayor.

3. Se evidenció que la implementación de los controles seleccionados para cumplir con la conformidad respecto a la norma ISO/IEC 27001:2013, cumplen con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de la información tratada en el ministerio y se identificaron puntos de mejora respecto a algunos controles específicos y la difusión y apropiación de los lineamientos en seguridad de la información establecidos al interior del ministerio para todos los colaboradores del ministerio.

PLAN DE MEJORAMIENTO

Conforme a lo establecido en el procedimiento "MIG-TIC-PR-003 -formulación, seguimiento y cierre de acciones de mejora", todos los hallazgos deben ser contemplados en un plan de mejoramiento MIG-TIC-FM-011, y debe ser entregado al Auditor Líder, en un plazo máximo de diez (10) días hábiles a partir de la entrega del presente informe.

Dicho plan de mejoramiento será verificado por el Equipo Auditor de este ciclo de auditoría interna, previo al cargue en la herramienta SIMIG, así como, será dicho equipo quien efectuará el cierre en la herramienta SIMIG.

Anexos que forman parte del presente informe

Anexo 1	EAC-TIC-FM-003	Acta de Reunión de Auditoría Interna	SI
Anexo 2	EAC-TIC-FM-020	Carta de Representación	SI
Anexo 3	EAC-TIC-FM-002	Plan de Auditoría Interna de Sistemas de Gestión	SI
Anexo 4	EAC-TIC-FM-014	Lista de Chequeo Auditoria Interna SG	NO
Anexo 5	MIG-TIC-FM-012	Listado de Asistencia o Soporte de reunión virtual	SI
Anexo 6	EAC-TIC-FM005	Informe de Auditoría Interna	SI
Anexo 7	EAC-TIC-FM08	Formato de evaluación de auditores Internos	SI
Anexo 8	MIG-TIC-FM-011	Formato Plan de mejoramiento	SI
Anexo 9		Presentación Apertura de Auditoria	SI
Anexo 10		Presentación Cierrde de Auditoria	SI

Anexo 11	Carpetas de Planeación, Ejecución, Informe y Cierre de Auditoria	NO

Flujo Aprobaciones (Equipo Auditor) Informe de Auditoría Interna

Elaboró	Revisó	Aprobó
Auditor(es): Hasblady González Engativá (En Formación) Danny Alejandro Garzón Aristizabal Rafael Hernando Calle Cabezas Fredy Alfonso De la Ossa Rojas Iván Alexis Ontibon Rojas Fecha: 06/09/2021	Auditor(es): Harley Roldán Silva Hasblady González Engativá (En Formación) Danny Alejandro Garzón Aristizabal Rafael Hernando Calle Cabezas Fredy Alfonso De la Ossa Rojas Iván Alexis Ontibon Rojas Fecha: 06/09/2021	Auditor Líder: Harley Roldan Silva Fecha: 06/09/2021

Firmado digitalmente por HARLEY ROLDAN SILVA
Fecha: 2021.09.06 13:27:20 -05'00'

Harley Roldán Silva
Nombre y Firma Auditor Líder

Andrés Díaz Molina
Nombre y Firma Líder del SG o del SIG

REGISTRO DE FIRMAS ELECTRONICAS

EAC-TIC-FM-005_INFORME_AUDITORIA_INTERNA_SGSI_06092021

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20210906-142549-ee1613-69483552 Creación: 2021-09-06 14:25:49

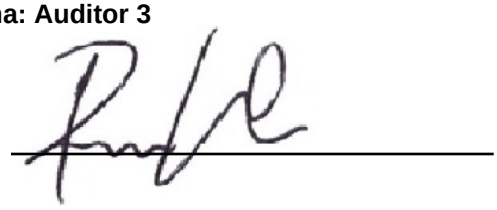
Estado: Finalizado Finalización: 2021-09-06 16:03:32

Escanee el código para verificación

Firma: Auditor 4

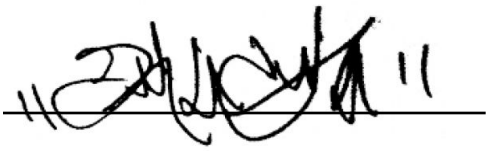
Ivan Alexis Ontibon Rojas
80204785
iontibon@mintic.gov.co

Firma: Auditor 3



rcalle@mintic.gov.co

Firma: Auditor 2



dgarzon@mintic.gov.co

Firma: Auditor 1

Hasblady González Engativá
1032374059
hgonzaleze@mintic.gov.co
Contratista – Dirección de Gobierno Digital - (Observador y en entrenamiento)
Dirección de Gobierno Digital MINTIC

REGISTRO DE FIRMAS ELECTRONICAS

EAC-TIC-FM-005_INFORME_AUDITORIA_INTERNA_SGSI_06092021

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20210906-142549-ee1613-69483552 Creación: 2021-09-06 14:25:49

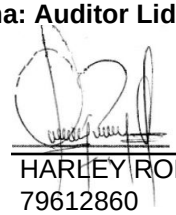
Estado: Finalizado Finalización: 2021-09-06 16:03:32

Escanee el código para verificación

Firma: Líder del SG o del SIG

Andrés Díaz Molina
92192112
adiazm@mintic.gov.co
Asesor - Oficial de Seguridad y Privacidad de la Información
Ministerio de TIC

Firma: Auditor Lider



HARLEY ROLDAN SILVA
79612860
hroldan@mintic.gov.co
Contratista
Dirección de Gobierno Digital - MinTIC

Firma: Auditor 5

fdelaossa@mintic.gov.co

REPORTE DE TRAZABILIDAD

EAC-TIC-FM-005_INFORME_AUDITORIA_INTERNA_SGSI_06092021

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Escanee el código para verificación

Id Acuerdo: 20210906-142549-ee1613-69483552 Creación: 2021-09-06 14:25:49

Estado: Finalizado Finalización: 2021-09-06 16:03:32

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Firma	Hasblady González Engativá hgonzaleze@mintic.gov.co Contratista – Dirección de Gobierno Digital - (Obser Dirección de Gobierno Digital MINTIC	Aprobado	Env.: 2021-09-06 14:25:50 Lec.: 2021-09-06 15:27:35 Res.: 2021-09-06 15:28:09 IP Res.: 181.53.13.78
Firma	Danny Alejandro Garzon Aristizabal dgarzon@mintic.gov.co	Aprobado	Env.: 2021-09-06 15:28:09 Lec.: 2021-09-06 15:28:47 Res.: 2021-09-06 15:28:54 IP Res.: 190.60.254.239
Firma	Rafael Hernando Calle Cabezas rcalle@mintic.gov.co	Aprobado	Env.: 2021-09-06 15:28:54 Lec.: 2021-09-06 15:29:02 Res.: 2021-09-06 15:29:13 IP Res.: 190.156.160.99
Firma	Ivan Alexis Ontibon Rojas iontibon@mintic.gov.co	Aprobado	Env.: 2021-09-06 15:29:13 Lec.: 2021-09-06 15:29:36 Res.: 2021-09-06 15:30:13 IP Res.: 181.50.16.12
Firma	Fredy Alfonso De la Ossa Rojas fdelaossa@mintic.gov.co	Aprobado	Env.: 2021-09-06 15:30:13 Lec.: 2021-09-06 15:31:02 Res.: 2021-09-06 15:31:25 IP Res.: 190.27.90.29
Firma	HARLEY ROLDAN SILVA hroldan@mintic.gov.co Contratista Dirección de Gobierno Digital - MinTIC	Aprobado	Env.: 2021-09-06 15:31:25 Lec.: 2021-09-06 15:32:02 Res.: 2021-09-06 15:32:14 IP Res.: 181.58.63.124
Firma	Andrés Díaz Molina adiazm@mintic.gov.co Asesor - Oficial de Seguridad y Privacidad de la Inf Ministerio de TIC	Aprobado	Env.: 2021-09-06 15:32:14 Lec.: 2021-09-06 16:03:25 Res.: 2021-09-06 16:03:32 IP Res.: 191.95.40.123