INFORME DE AUDITORIA INTERNA DE SISTEMAS DE GESTIÓN

FECHA	DIA	MES	AÑO
Apertura	3	8	22
Cierre	9	8	22
Emsión del Informe	12	8	22

SISTEMA DE GESTIÓN AUDITADO
NTC ISO 27001:2013
Ciclo de Auditoria (Periodo a Auditar)
2021-2022

Líder Sistemas de Gestión Auditado ANDRES DIAZ MOLINA **Correo electrónico** adiazm@mintic.gov.co

EQUIPO AUDITOR QUE REALIZÓ LA AUDITORÍA INTERNA			
Nombre	**Rol**	**Nombre**	**Rol**
Juan Carlos Márquez Flórez	Auditor Líder		

INTRODUCCIÓN

Hoy se ha presentado un gran reto para Ministerio, no sólo la auditoria de la NTC ISO 27001:2013, sino que al mismo tiempo por ser una entidad oficial debe cumplir a cabalidad con la constitución, leyes, decretos, resoluciones que se expiden las entidades (congreso, presidencia, ministerios, entes de control, entre otros) y que al mismo tiempo los organos de control están atentos para validar su cumplimiento. El reto consiste en articular no sólo la norma sino lograr al mismo tiempo, armonizar, sincronizar y evidenciar la adherencia de los procesos a la norma NTC ISO 27001:2013, y a la normatividad actual de obligatorio cumplimiento.

Las auditorias a los sistemas de gestión debe enforcarse en la prevención, más que al hallazgo propiamente; realizando el ejercicio de auditorias de la NTC ISO 27001:2013, de esta manera se concientiza a los auditados del Ministerio de las TIC´s a entender el por qué se debe de atender un numeral de la norma o un control, dicho de esta forma se logra que los auditados expresaran abiertamente y describieran el proceso de una manera natural, de cómo llevan a cabo mosttando la realidad.

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 Auditoria Interna

La Auditoría al SGSI MinTIC tiene como alcance Asegurar la confidencialidad, integridad y disponibilidad de la información en la gestión y control de la prestación del Servicio Público de las Tecnologías de la Información y las Comunicaciones

Objetivos de la Auditoria Interna

General	Específicos
Determinar la conformidad del sistema de gestión del Ministrio/Fondo Ünico de TIC, con los criterios de la norma NTC ISO/IEC 27001:2013; evaluando la capacidad del sistema de gestión para asegurar que la organización cumple los requisitos legales, reglamentarios y contractuales aplicables; evalúa su eficacia e identifica las áreas de mejora.	

Criterios de la Auditoria Interna

Requisitos de las normas ISO 27001:2013, procedimientos documentados del Miinisterio/Fondo Único de TIC, requisitos legales establecidos y vigentes y normatividad aplicable a cada proceso.

RESULTADOS DE LA AUDITORIA INTERNA

1. Fortalezas

1.En primer lugar, el compromiso de la Alta Gerencia: Despacho de la Ministra, Viceministerios, Secretaria General, no sólo al proporcionar los recursos humanos, técnicos y financieros, sino que además participan activamente en todo el proceso y que culmina con la Revisión por la Dirección donde se toman decisiones para el mejoramiento del sistema de gestión de seguridad y privacidad de la información.
2.Desde la Secretaría General se delegó al señor Cristhian Ramírez Pérez, como una muestra del compromiso de la Alta Gerencia, con el fin de validar la transparencia y conocer de primera mano la forma en que se lleva a cabo el cumplimiento de los procesos y de las normas legales.
3.La designación de forma directa del Oficial de Seguridad y Privacidad de la Información desde la Oficina del despacho de la Ministra, ya que los resultados logrados en la implementación de la Norma NTC ISO 27001:2013 se deben en gran parte al nivel de autoridad con que se cuenta, al depender directamente de este despacho.
4.Acompañando al Oficial de Seguridad y Privacidad de la Información se encuentra un Equipo de profesionales calificados y que se convierten en garantes de todo el proceso, no sólo de la implementación, sino también del mantenimiento del sistema de seguridad y privacidad de la información al ayudar, acompañar y gestionar con la articulación de todos los procesos.
5.Todo el personal que participó en la auditoría: Directores, Jefes de Oficina, Subdirectores, Coordinadores, Líderes y Gestores de Procesos, Proveedores, Contratistas y Funcionarios, cumpliendo con la cita, "y con la camiseta puesta", dispuestos a mostrar con hechos el cumplimiento de su proceso pero al mismo tiempo, de una manera transparente cumpliendo con la norma NTC ISO 27001:2013 y también dispuestos a aceptar sugerencias y recomendaciones para lograr un mejor desempeño del sistema de gestión de seguridad y privacidad de la información.
6.Para la auditoría se contó con un equipo de Auditores en formación: Jairo Torres, Cristian Montaño, Paola Walteros, Sandra Arteaga, Erika Quintero y Nelson Pardo, a los cuales se le permitió asistir para que observaran de manera directa la auditoria con el fin de obtener experiencia y al mismo tiempo acumular horas de vuelo, lo que le permitirá al Ministerio, contar con auditores más idóneos y listos para afrontar retos como el de las auditorias.
7.El Ministerio cuenta con herramientas de última generación que, sin lugar a dudas, llevan a robustecer y garantizar la confidencialidad, disponibilidad e integridad de la información, puede parecer sólo un software pero detrás de ellos hay fuertes inversiones financieras y el empleo de recursos técnicos y humanos para mantener una eficiencia y operatividad. Se destacan entre muchas herramientas los Servidores Azure, Firewall de última generación, software: Simig, Iri, Integratic, Veeam Backup, Service Desk, ASPA, DRP AWS, BI Analítica, Kactus, Office 365, Directorio Activo.
8.La política "Trae tu propio dispositivo", es un ejemplo de cómo se puede llevar a cabo el cumplimiento de las normas de seguridad y privacidad de la información sin perder la confidencialidad, disponibilidad e integridad de la información, sin ser intrusivos, respetando la privacidad de las personas en sus dispositivos móviles.
9.Se destaca el proceso de Gestión de Fortalecimiento Organizacional, quien tiene la responsabilidad de los diferentes sistemas de gestión y que hoy puede recoger los frutos de trabajo en equipo y de meses de esfuerzo.
10.La definición de los procesos cuenta con una estructura definida que apunta a cumplir con el ciclo PHVA.
11.La auditoría del SGSI se llevó a cabo sin ningún inconveniente, y se contó con la colaboración de todos los procesos y personas citadas. Esto permitió que el plan de auditoría se cumpliera en su totalidad.

2. Hallazgos de la Auditoría Interna

Requisito Incump.	Describe Requisito / Objetivo Control	Clasificación	#	Descripción Hallazgo	Recomendación
			1	**Para la presente Auditoría NO SE ENCONTRARON HALLAZGOS**	
			2		
			3		

			4		
			5		
			6		
			7		
			8		
			9		
			10		

3. OBS (Observación)

•El instrumento que se utiliza para la gestión de riesgos y gestión de activos es el Excel, si bien es una herramienta poderosa y la norma no estipula en qué tipo de herramienta se debe llevar a cabo, por ser Excel vulnerable o susceptible para modificar, de no tomarse las medidas necesarias los registros que allí se llevan se pueden ver afectados en un integridad, debido a quela herramienta permite modificar los registros.

Cantidad de No Conformidades encontradas	0

Cantidad de Observaciones encontradas	1

4. Oportunidades de Mejora

1.Se cuenta con la certificación de NTC ISO 27001:2013, ahora lo que sigue es la evolución hacia la mejora continua, se invita para que todos participen de forma proactiva y puedan seguir nutriendo el sistema de gestión seguridad y privacidad de la información, de acuerdo con el proceso establecido.
2.Debido a disponibilidad por labores propias de cada rol y a la rotación de personal, se invita a continuar fortaleciendo al equipo auditor, invitando a las áreas para que aporten candidatos para el proceso de selección de auditores con el fin de contar con un grupo suficiente para cubrir las auditorías internas.
3.Se bien se cuenta con un plan de cultura organizacional, se deben seguir incluyendo ejercicios de apropiación en temas de seguridad de la información a todos los niveles, incluyendo personal de vigilancia, servicios generales, funcionarios, contratistas, entre otros.

5. Conclusiones

1. El Sistema de Gestion de Seguridad y Privacidad de la Informacion del Ministerio/Fondo Unico de TIC CUMPLE con los requisitos que establece la Norma NTC ISO 27001:2013.

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	
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	SI
Anexo 5	MIG-TIC-FM-012	Listado de Asistencia o Soporte de reunión virtual	SI
Anexo 6			
Anexo 7			
Anexo 8			
Anexo 9			
Anexo 10			

Flujo Aprobaciones (Equipo Auditor) Informe de Auditoría Interna

Elaboró	Revisó	Aprobó
Auditor(es): **Fecha:**	**Auditor(es):** Gisela E. López López **Fecha**: 16/08/2022	**Auditor Líder**: **Juan Carlos Márquez F.** **Fecha:** 12/08/2022

Nombre y Firma Auditor Líder

Nombre y Firma Líder del SG o del SIG

REGISTRO DE FIRMAS ELECTRONICAS

EACTICFM005V7InformedeAISistemasGestin

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

Id Acuerdo: 20220817-142508-27f6b3-27950305
Creación: 2022-08-17 14:25:08
Estado: Finalizado
Finalización: 2022-08-17 15:21:02

Escanee el código para verificación

Aprobación: Aprobador

Andrés Díaz Molina
92192112
adiazm@mintic.gov.co
Coordinador del GIT de Seguridad y Privacidad de la Información
Ministerio de TIC

REPORTE DE TRAZABILIDAD

EACTICFM005V7InformedeAISistemasGestin

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

Id Acuerdo: 20220817-142508-27f6b3-27950305 Creación: 2022-08-17 14:25:08

Estado: Finalizado Finalización: 2022-08-17 15:21:02

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Aprobación	Andrés Díaz Molina adiazm@mintic.gov.co Coordinador del GIT de Seguridad y Privacidad de la Ministerio de TIC	Aprobado	Env.: 2022-08-17 14:25:09 Lec.: 2022-08-17 15:20:54 Res.: 2022-08-17 15:21:02 IP Res.: 190.109.20.169