OFICINA DE CONTROL INTERNO

INFORME DE AUDITORÍA

TIPO DE INFORME

Preliminar [ ] **Definitivo** [X]

AUDITORÍA AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BAJO LOS REQUISITOS DE NORMA ISO/IEC 27001/2013

AÑO	AUDITORÍA	PROCESO, PROCEDIMIENTO O ACTIVIDAD	ÁREA RESPONSABLE
2023	A09	Aplica a los procesos definidos en el Mapa de Procesos de Minciencias dentro del marco operativo del Modelo de Seguridad y Privacidad de la información implementado	Líderes de los procesos evaluados

PERIODO AUDITADO O EVALUADO	FECHA INFORME PRELIMINAR	FECHA INFORME DEFINITIVO
05 de octubre de 2022 a julio 31 de 2023	08/09/2023	15/09/2023

Informe elaborado por:
LUZ MARLENNY CANO ROMERO
Oficina de Control Interno

Contenido

INTRODUCCION

La Oficina de Control Interno en ejecución del plan anual de auditoría para la vigencia 2023, y dentro de su rol de enfoquehacia la Prevención efectuó el diagnóstico del estado de madurez sobre la implementación del Sistema de Gestión de Seguridad de la Información.

1. OBJETIVOS

Auditar el cumplimiento de los requisitos de la Norma ISO/IEC 27001:2013, verificando el cumplimiento de las disposiciones planificadas y comprobando que se mantienen de manera eficaz los controles, en el Modelo de Seguridad y Privacidad de la información implementado en MINCIENCIAS.

2. ALCANCE

La Auditoría Interna aplica a los procesos definidos en el en Mapa de procesos de Minciencias dentro del marco operativo del Modelo de Seguridad y Privacidad de la información implementado.

3. METODOLOGÍA

La Metodología empleada para desarrollar la presente Auditoria se soporta en la verificación y análisis de documentos y/o registros físicos y virtuales, la consulta en http://gina.minciencias.gov.co/, página web, revisión de respuestas a solicitudes de información escrita y verbal, pruebas selectivas, pruebas de observación, visitas de inspección, entrevistas, encuestas, mesas de trabajo con los servidores públicos y contratistas que lideran y apoyan los proceso de Gestión de Tecnología de la Información, Gestión Contractual, Gestión Jurídica, Gestión de Administrativa - Bienes y Servicios, Gestión Documental, Gestión Financiera- Direccionamiento General e Informes, Gestión de Evaluación y Control y sus Procedimientos, con el fin de valorar su estado y nivel de cumplimiento frente a los requisitos técnicos, de oportunidad y legales que le aplican.

4. MUESTRA

La Muestra empleada para desarrollar la presente Auditoria, se fundamenta en muestreo aleatorio simple revisando la información relevante del proceso y con la que se puede demostrar cumplimiento.

5. RIESGOS EVALUADOS

Se Identificaron los riesgos de Tecnología con el Mapa de Riesgos de la Entidad, verificando que están alineados y que se aplican los controles necesarios para gestionar oportunidades o amenazas asociadas.

En el marco de los objetivos y el alcance establecido para esta Auditoria, se evalúan los riesgos actuales establecidos en el Mapa de Riesgos identificados, que pueden afectar los resultados institucionales.

Al respecto se encontró que actualmente existen 03 (tres) riesgos de corrupción identificados en el Proceso Tecnología, los cuales se relacionan en la siguiente tabla:

PROCESO	RIESGOS ACTUALES DEL PROCEDIMIENTO
Tecnología	R 88-2023 Posibilidad de afectación reputacional y económica en la que puede incurrir laentidad, por el favorecimiento a terceros al manipular la información y direccionar indebidamente las respuestas de PQRDS.
	R 4-2023 Posibilidad de afectar la reputación del Ministerio por otorgar a nombre propio ode terceros cualquier dádiva o beneficio derivado de omisiones en el proceso de Gestión para la ejecución de política para la CTeI
	R8-2023 Posibilidad de afectación económica por registrar en la contabilidad las actas deliquidación, incapacidades o resoluciones de condonación y demás actos administrativos que generen una cuenta por cobrar de forma indebida debido a que no se recibe el insumo por parte de la dependencia o se omite su registro.

En la matriz se observa qué después de controles de los Riesgos de corrupción, dos (2) se encuentran en zona de riesgoInherente extremo y uno (1) en zona de riesgo mayor.

Actualmente en el Ministerio se cuentan con 04 (cuatro) riesgos de seguridad de la información, y se realizan seguimiento trimestralmente y son de conformidad con lo estipulado en la Guía de administración de Riesgos y Diseño de Controles establecida por el DAFP. Se puede visualizar en: https://minciencias.gov.co/quienes_somos/planeacion_y_gestion/tratamiento

R68-2023 Posibilidad de acceso indebido o mal intencionado a las plataformas tecnológicas del Ministerio, generando perdida o alteración de información, debido a las vulnerabilidades de las plataformas tecnológicas del Ministerio

R69-2023 Posibilidad de indisponibilidad de la información, debido a interrupciones del servicio por cortes de electricidad, fallos de hardware, daño de los sistemas de climatización del datacenter y daño y/o descarga de las baterías del equipo UPS, daños provocados por mal funcionamiento de los equipos tecnológicos, ataques cibernéticos. etc.

R70-2023 Posibilidad de Daño o modificación en la Información del Ministerio, debido a interrupciones del servicio por cortes de electricidad, fallos de hardware, daño de los sistemas de climatización del datacenter y daño y/o descarga de las baterías del equipo UPS, daños provocados por mal funcionamiento de los equipos tecnológicos, ataques cibernéticos, etc.

R74-2023 Posibilidad de daños o fallas en la infraestructura del Datacenter del Ministerio por eventos relacionados con la infraestructura física como: derrumbes, incendios, inundaciones, entre otros, afectando la disponibilidad, confidencialidad e integridad de la información del Ministerio, debido a daños o fallas en la infraestructura tecnológica y física del Datacenter .

Dada la importancia de la correcta definición de los riesgos, causas y controles como mecanismos de gestión para el logro de los objetivos estratégicos y de proceso, desde control interno se sugiere tener en cuenta las

observaciones documentadas en cada informe de los diferentes procesos, con la finalidad de que se hagan los ajustes necesarios (periodicidad, evidencia, descripción, coherencia riesgo-causa-control), de conformidad con lo estipulado en la Guía de administración de Riesgos y Diseño de Controles establecida por el DAFP.

así mismo se evidencia que se cuenta con los lineamientos para la gestión y control de los riesgos de gestión, corrupción y seguridad digital de la Entidad partiendo desde la política de administración del riesgo, la construcción del mapa de riesgos, la comunicación, consulta y divulgación de los riesgos existentes, su priorización, seguimiento, monitoreo, revisión y actualización para la gestión integral de los riesgos Mediante la Guía para la Gestión del Riesgo y las Oportunidades D102PR03G01.

6. RESULTADOS DE AUDITORIA

6.1 Fortalezas

Se realizó un análisis permitiendo evaluar el estado de contexto de la organización, liderazgo, planificación, soporte, operación, evaluación de desempeño y mejoras, los cuales se convierten en elementos esenciales en el proceso de mejoramiento continuo, para la Entidad desde la pertinencia del subsistema de gestión de seguridad de la información.

El apoyo y disposición brindados por la jefe de Tecnología de la información junto con su equipo de trabajo, así como laentrega oportuna de la información solicitada.

La concientización y/o empeño por parte del contratista líder para el desarrollo e implementación del Sistema de Gestión de Seguridad (SGSI) en la entidad, en cuanto al desarrollo de los procedimientos mejorando y corrigiendo los que están presentes en Gestión Contractual, Gestión Jurídica, Gestión de Administrativa - Bienes y Servicios, Gestión Documental, Gestión Financiera- Direccionamiento General e Informes, Gestión de Evaluación y Control.

6.2. Descripción del Trabajo Realizado, Cumplimiento De La Norma, Opciones De Mejora

6.2.1 Cumplimiento de los requisitos de la Norma Técnica ISO/IEC 27001:2013

Durante el desarrollo de la Auditoria, se evaluaron los siguientes requisitos de la norma Técnica ISO/IEC 27001:2013 a los procesos establecidos en las áreas Gestión contractual, Jurídica, Bienes y servicios, Financiera, Documental, Talento Humano y Tecnologías de la Información**.**

5. Liderazgo

5.1 Liderazgo y compromiso

El documento D103M01 Manual de Política de seguridad de la información define el compromiso, sin embargo, se debeajustar a la versión 2.0 a lo exigido por la ISO 27000: 2013 y ser comunicado a todos los servidores públicos de la Entidad. La Alta dirección debe demostrar liderazgo y compromiso, asegurando que se establezcan la política, los objetivos, asegurar los recursos, promoviendo la mejora continua, dirigiendo y apoyan a las personas para contribuir a la eficacia del SGSI.

5.2 Política

El Manual de políticas de seguridad de la información están acorde a lo exigido por la ISO 27001:2013, lo que está pendiente es presentar los ajustes al comité de Gestión de desempeño institucional e innovación de acuerdo con la dinámica del Ministerio, es decir versión 2, pero la versión 1 está acorde a la normatividad vigente y comunicada

5.3 Roles, responsabilidades y autoridades en la organización

Se tiene definidos unos roles y responsabilidades en generales en los diferentes documentos elaborados del proceso de gestión de TI, como:
Política de seguridad y privacidad de la información
Políticas específicas de segundo nivel de la seguridad y privacidad de a información Gestión de riesgo de seguridad de la información.

A nivel del Ministerio se tiene documentado y aprobado los roles, responsabilidades y autoridades principales del SGSI, para gestionar la seguridad y privacidad de la información dentro de los lineamientos establecidos para tal fin, fortaleciendo la estructura organizacional del sistema de gestión de seguridad de la información, se puede visualizar el documento en GINA como D103M07 Manual de roles y responsabilidades del Sistema de Gestión de Seguridad de la Información SGSI

7.5 Información documentada

Dentro del Proceso de Gestión de tecnología de la Información se ha definido más de 20 documentos, los cuales hacenparte del Manual de la política de seguridad de la información y en cumplimiento de la política de digital y protección de datos. Esta documentación requiere ser ajustada y articulada con los requisitos de la ISO 27001:2013 y complementar los que hacen falta, también debe estar integrado al sistema de gestión la entidad.

Se realizó un análisis permitiendo evaluar el estado de contexto de la organización, liderazgo, planificación, soporte, operación, evaluación de desempeño y mejoras, los cuales se convierten en elementos esenciales en el proceso de mejoramiento continuo, para la Entidad desde la pertinencia del subsistema de gestión de seguridad de la información.

En el anexo A “Diagnóstico inicial…..”, se aplica la encuesta (Objetivos de Control y controles de referencia) a la Gestión de Tecnología de la Información, Talento Humano, Contractual, Jurídica, de Administrativa - Bienes y Servicios, Documental, Recursos Financieros - Direccionamiento General e Informes, Gestión de Evaluación y Control lo cual fue realizada con los funcionarios líderes de cada proceso y el Líder del MPSI SEGURIDAD DE LA INFORMACIÓN, sobre el cumplimiento relacionado con los 14 dominios y 114 controles de seguridad que establece la norma ISO/IEC 27001:2013.

Las respuestas posibles están dadas por: NC, NP, CS, NA. De acuerdo con la información que se presenta en la siguientetabla:

Sigla	Estado de Evaluación	Descripción
NC	NO CUMPLE	No existe y/o no se está haciendo

CP	CUMPLE PARCIALMENTE	Lo que la norma requiere (ISO/IEC 27001 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó, pero no se gestiona
CS	CUMPLE SATISFACTORIAMENTE	Existe, es gestionado, se está cumpliendo con lo que la norma ISO/IEC 27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI cumple 100%
NA	NO APLICA	No se aplica en la Entidad

Anexo A "Diagnóstico inicial encuesta aplicada"

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
A.5	**POLITICA DE LA SEGUIRDAD DE LA INFORMACION**				
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información				
A.5.1.1	Política para la Seguridad de la Información	X			
A.5.1.2	Revisión de políticas para la seguridad de la Información se considera parcial, debido a que falta pasarlo para aprobar versión 02		X		
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**				
A.6.1	**Organización Interna**				
A.6.1.1	Roles y responsabilidades para la seguridad de la información	x			
A.6.1.2	Separación de deberes		X		
A.6.1.3	contacto con las Autoridades (se tiene documentado en procedimiento de incidentes de seguridad D103M01 el contacto de autoridades, hasta la fecha no se ha presenta un incidente que se deba reportar a estas autoridades)		X		
A.6.1.4	Contacto con los grupos de Interés especial		x		
A.6.1.5	Seguridad de la información en la gestión de proyectos	x			
A.6.2	**Dispositivos móviles y de teletrabajo**				
A.6.2.1	Políticas para dispositivos móviles	x			
A.6.2.2	Teletrabajo (Como objeto de auditoría se presentó el proyecto de política de teletrabajo alineado al Manual de políticas de seguridad de la información, pendiente en ese momento de aprobación.		X		
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**				

A.7.1	**Antes de asumir el empleo**				
A.7.1.1	Selección		x		

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
A.7.1.2	Términos y condiciones del empleo		x		
A.7.2	**Durante la ejecución del empleo**				
A.7.2.1	Responsabilidades de la dirección	x			
A.7.2.2	Toma de conciencia educación y formación de la seguridad de la información	x			
A.7.2.3	Proceso disciplinario		x		
A.7.3	Terminación y cambio de empleo				
A.7.3.1	Terminación o cambio de responsabilidades de empleo		x		
A.8	**GESTION DE ACTIVOS**				
A.8.1	**Responsabilidades de los activos**				
A.8.1.1	Inventario de Activos		x		
A.8.1.2	Propiedad de los Activos		x		
A.8.1.3	Uso aceptable de los activos		x		
A.8.1.4	Devolución de Activos		x		
A.8.2	**Clasificación de la información**				
A.8.2.1	Clasificación de la información		x		
A.8.2.2	Etiquetado de la información		x		
A.8.2.3	Manejo de activos		x		
A.8.3	**Manejo de medios**				
A.8.3.1	Gestión de medios removibles		x		
A.8.3.2	Disposición de los medios		x		
A.8.3.3	Transferencia de medios físicos	x			
A.9	**CONTROL DE ACCESO**				
A.9.1	**Requisitos del negocio para el control de acceso**				
A.9.1.1	Política de control de acceso	x			
A.9.1.2	Acceso a redes y a servicios en red	x			
A.9.2	**Gestión de acceso a Usuarios**				
A.9.2.1	Registro y cancelación del registro de usuarios		x		
A.9.2.2	Suministro de acceso de usuarios	x			
A.9.2.3	Gestión de derechos de acceso privilegiado		x		
A.9.2.4	Gestión de información de autenticación secreta de usuarios	x			
A.9.2.5	Revisión de los derechos de acceso de usuarios	x			
A.9.2.6	Retiro a ajuste de los derechos de acceso		x		
A.9.3	**Responsabilidades de los usuarios**				
A.9.3.1	Uso de Información de autenticación secreta	x			
A.9.4	**Control de Acceso a sistemas y aplicaciones**				
A.9.4.1	Restricción de acceso a la información	x			

A.9.4.2	Procedimiento de Ingreso seguro		x		
A.9.4.3	Sistema de gestión de contraseñas		x		

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
A.9.4.4	Uso de programas utilitarios privilegiados		x		
A.9.4.5	Control de acceso a códigos fuentes de programas		x		
A.10	**CRIPTOGRAFIA**				
A.10.1	**Controles Criptográficos**				
A.10.1.1	Política sobre el uso de los controles criptográficos		x		
A.10.1.2	Gestión de llaves		x		
A.11	**SEGURIDAD FISICA Y DEL ENTORNO**				
A.11.1	Áreas seguras				
A.11.1.1	Perímetro de seguridad física	x			
A.11.1.2	Controles de acceso físicos	x			
A.11.1.3	Seguridad de oficinas recintos e instalaciones	x			
A.11.1.4	Protección contra amenazas externas y ambientales	x			
A.11.1.5	Trabajo en las áreas seguras	x			
A.11.1.6	Áreas de despacho y carga				x
A.11.2	**Equipos**				
A.11.2.1	Ubicación y protección de equipos	x			
A.11.2.2	Servicios de suministro	x			
A.11.2.3	Seguridad del cableado		x		
A.11.2.4	Mantenimiento de equipos	x			
A.11.2.5	Retiro de activos		x		
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones			x	
A.11.2.7	Disposición seguro reutilización de equipos		x		
A.11.2.8	Equipos de usuario desatentado		x		
A.11.2.9	Política de escritorio limpio y pantalla limpia		x		
A.12	**SEGURIDAD DE LAS OPERACIONES**				
A.12.1	Procedimientos operaciones y responsabilidades				
A.12.1.1	Procedimientos de operación documentados		x		
A.12.1.2	Gestión de cambios	x			
A.12.1.3	Gestión de la capacidad (Se cumple parcialmente, pendiente de normalizar documento, se adjunta como soporte		x		
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		x		
A.12.2	**Protección contra código maliciosos**				
A.12.2.1	controles contra códigos maliciosos	x			
A.12.3	**copias de Respaldo**				
A.12.3.1	Respaldo de información	x			
A.12.4	**Registro y seguimiento**				
A.12.4.1	Registro de eventos		x		
A.12.4.2	Protección de la información de registro		x		
A.12.4.3	Registros del administrador y del operador	x			
A.12.4.4	Sincronización de relojes	x			

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
A.12.5	**Control de software operacional**				
A.12.5.1	Instalación de software en sistemas operativos	x			
A.12.6	**Gestión de la vulnerabilidad técnica**				
A.12.6.1	Gestión de las vulnerabilidades técnicas	x			
A.12.6.2	Restricciones sobre la Instalación de software		x		
A.12.7	**Consideraciones sobre auditorias de sistemas de información**				
A.12.7.1	controles de auditorías de sistemas de información	x			
A.13	**SEGURIDAD DE LAS COMUNICACIONES**				
A.13.1	**Gestión de la seguridad de las redes**				
A.13.1.1	Controles de redes	x			
A.13.1.2	Seguridad de los servicios de red	x			
A.13.1.3	Separación en las redes	x			
A.13.2	**Transferencia de la información**				
A.13.2.1	Políticas y procedimientos de transferencia de información	x			
A.13.2.2	Acuerdos sobre transferencia de información		x		
A.13.2.3	Mensajería electrónica	x			
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	x			
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**				
A.14.1	**Requisitos de seguridad de los sistemas de información**				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	x			
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	x			
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	x			
A.14.2	**Seguridad en los procesos de desarrollo y soporte**				
A.14.2.1	Política de desarrollo seguro	x			
A.14.2.2	Procedimiento de control de cambio de Sistemas		x		
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de la operación		x		
A.14.2.4	Restricciones en los cambios a los paquetes de software	x			
A.14.2.5	principios de construcción de los sistemas seguros Se considera que cumple parcial, debido a que se construyo el documento, pendiente de normalizar en GINA. Se adjunta documento como soporte		x		
A.14.2.6	Ambiente de desarrollo seguro (Se considera que se cumple parcial, si bien no somos una empresa de sw, se realizan desarrollos , pendiente de normalizar en GINA. Se adjunta documento como soporte		X		

A.14.2.7	Desarrollo contratado externamente		x		
A.14.2.8	Pruebas de seguridad de sistemas			x	
A.14.2.9	Pruebas de aceptación de sistemas			x	

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
A.14.3	Datos de Prueba				
A.14.3.1	Protección de datos de prueba. Se considera de cumple realizan pruebas a través del formato normalizado D103PR02F02	X			
A.15	**RELACIONES CON LOS PROVEEDORES**				
A.15.1	**Seguridad de la información en las relaciones con los proveedores**				
A.15.1.1	Políticas de seguridad de la información para las relaciones con los proveedores		x		
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		x		
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		x		
A.15.2	**Gestión de la prestación de servicios de proveedores**				
A.15.2.1	Seguimiento y revisión de los servicios de los Proveedores		x		
A.15.2.2	Gestión de cambios en los servicios de los proveedores		x		
A.16	**Gestión de Incidentes**				
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**				
A.16.1.1	Responsabilidades y procedimientos		x		
A.16.1.2	Reporte de eventos de seguridad de la información		x		
A.16.1.3	Reporte de debilidades de seguridad de la Información		x		
A.16.1.4	Evaluación de los eventos de seguridad de la información y decisiones sobre ellos		x		
A.16.1.5	Respuesta a incidentes de seguridad de la Información		x		
A.16.1.6	Aprendizaje obtenido de los incidentes de SI		x		
A.16.1.7	Recolección de evidencia		x		
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO**				
A.17.1	continuidad de seguridad de la información				
A.17.1.1	Planificación de la continuidad de la SI			x	
A.17.1.2	Implementación de la continuidad de la SI			x	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la SI			x	
A.17.2	Redundancias			x	

A.17.2.1	Disponibilidad de las Instalaciones de procesamiento de la información			x	
A.18	**CUMPLIMIENTO**				
A.18.1	Cumplimiento de los requisitos legales y contractuales				
Objetivos de Control y Controles de Referencia					
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	x			
A.18.1.2	Derechos de propiedad intelectual		x		
A.18.1.3	Protección de registros		x		
A.18.1.4	Privacidad y protección de información de datos personales	x			
A.18.1.5	Reglamentación de controles criptográficos				x
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	x			
A.18.1.2	Derechos de propiedad intelectual		x		
A.18.1.3	Protección de registros		x		
A.18.1.4	Privacidad y protección de información de datos personales	x			
A.18.1.5	Reglamentación de controles criptográficos				x
A.18.2	Revisiones de seguridad de la información				
A.18.2.1	Revisiones independientes de la seguridad de la información		x		
A.18.2.2	cumplimiento de las políticas y normas de seguridad		x		
A.18.2.3	Revisión del cumplimento técnico		x		

Como resultado de la encuesta anterior, se describe dominio a dominio el estado de madurez obtenido por medio de la información entregad de la líder del MSPI.

A.5 Política de Seguridad 100%

Se evidencia que todos los procesos auditados Tecnología de la Información, Evaluación y control, Contractual, Jurídica, Administración de Bienes y Servicios, gestión financiera, Documental y Talento Humano. tiene claro el Manal de políticas de Seguridad de la Información, sin embargo, se sugiere más sensibilización con respecto a alinear el Manual a todos los controles que se tengan establecidos en cada proceso.

Se evidencia la definición de un conjunto de políticas de seguridad de la información a través del Manual de Políticas de Seguridad y Privacidad de la Información versión 01 aprobado el 30 de septiembre de 2020 publicado en GINA el 02 de octubre de 2020, así mismo se evidencian procesos continuos de sensibilización y apropiación de estas al interior de la Entidad.

✓ **Ejercicio de Phishing**

Fwd: Minciencias y Bancolombia se unen en favor de tu economía... ¡descubre este beneficio para ti!
2 mensajes

Mesa de Servicios Minciencias <mesadeservicios@minciencias.gov.co>
Para: Erika Viviana Chacón Gamba <evchacon@minciencias.gov.co>

fyi
Cordialmente

MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN
Mesa de Servicios Minciencias
mesadeservicios@minciencias.gov.co
Tel: 6016258480 Ext: 2151
AV. Calle 26 No. 57-83 Torre 8. Piso 2 al 6
Bogotá, Colombia
www.minciencias.gov.co

---------- Forwarded message ---------
De: **Jenny Katheryn Martínez Nocove** <jkmartinez@minciencias.gov.co>
Date: lun, 15 may 2023 a las 12:17
Subject: Fwd: Minciencias y Bancolombia se unen en favor de tu economía... ¡descubre este beneficio para ti!
To: Mesa de Servicios Minciencias <mesadeservicios@minciencias.gov.co>, Mesa de Ayuda <mesadeayuda@confecamaras.org.co>

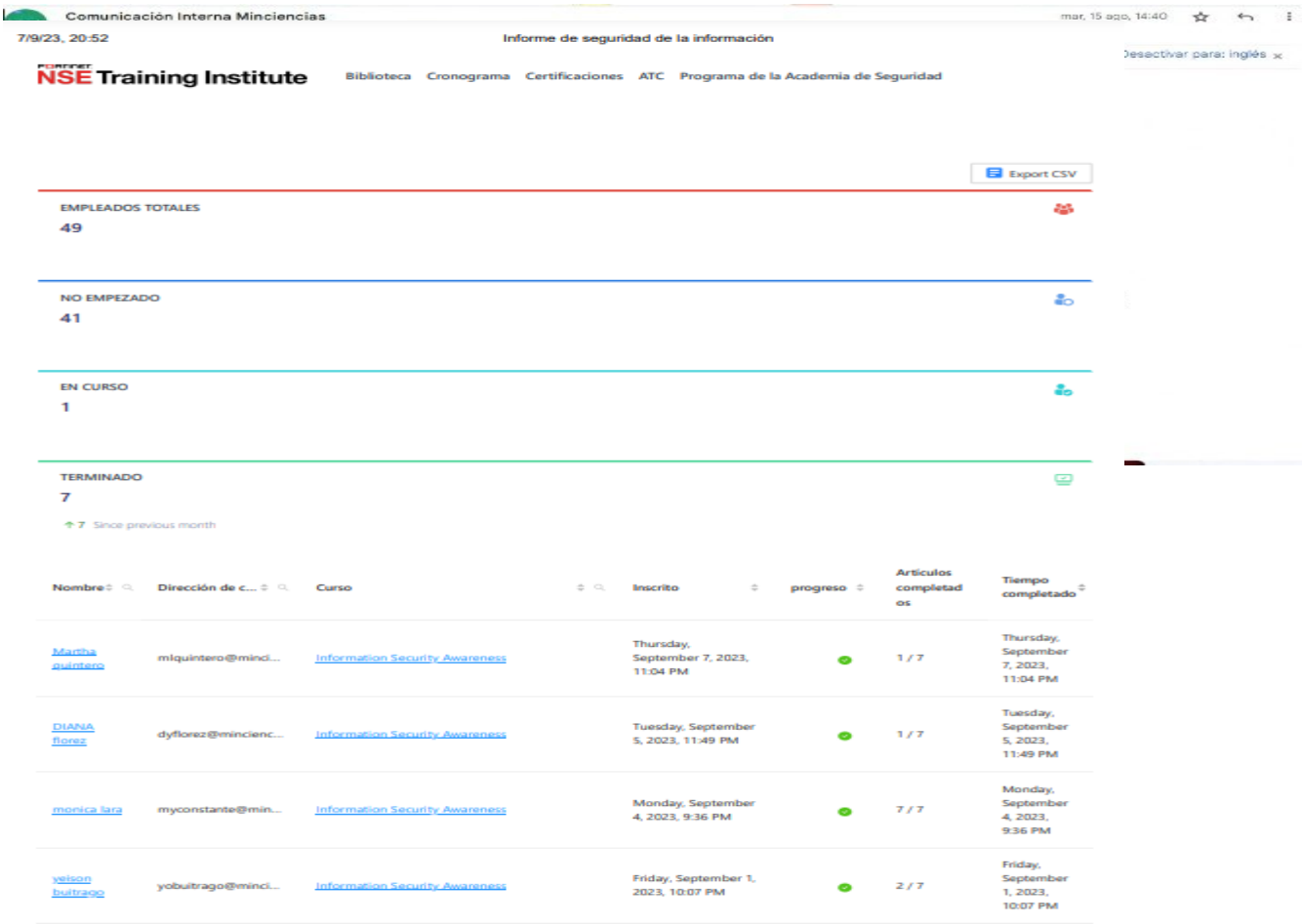
Cordial Saludo,

Remito para su conocimiento y fines pertinentes correo allegado, ya que la dirección no me parece confiable.

Quedo atenta a los comentarios y paso a seguir. Gracias!

Atentamente,

✓ **Carteleras Seguridad de la información**



Sin embargo, continuamos evidenciando que la versión V2 está en desarrollo desde el año 2022 y no se ha logra su terminación y aprobación dado a las faltas de continuidad en los contratos de prestación de servicio del personal y a lasdinámicas que tiene MIN Ciencias con la nueva administración y cambio de ministro.

Las Resolución 1205 2021 fue aprobada por parte de la ministra doctora Mabel Torres el día 16 de junio de 2021 y el fechado por parte de la secretaria general mediante la resolución 1205 de 2021, ARTÍCULO PRIMERO. Adoptar el Manual de Políticas de Seguridad y Privacidad de la Información del Ministerio de Ciencia, Tecnología e innovación y el Manual de políticas de Seguridad y Privacidad de la Información fue aprobada mediante el comité de Gestión de desempeño Institucional y Sectorial mediante el acta No 20.

Para los planes de acción se apoya desde la Alta Dirección a través de las iniciativas que se establece en el plan de acción Institucional PAI, se incluye en gestión de seguridad de la Información y de acuerdo de este PAI se genera el plan de Gestión y seguridad y la privacidad, se puede consultar en https://minciencias.gov.co/quienes_somos/planeacion_y_gestion/seguridad-informacion Y de aquí es el avance que se presenta en revisión por la dirección de la implementación del MSPI

A.6 Organización de la seguridad de la información. 80%

El control A.12.1.2 Gestión de Cambios se tiene incluido en el procedimiento de gestión de cambios en GINA como D103PR02, el cual detalla las actividades necesarias para gestionar los cambios, solicitados por los responsables de los diferentes procesos de Minciencias, con el fin de controlar los cambios realizados a las aplicaciones de software.

Incluir el control A.6.2.2

La entidad cuanta con la auditoría la política de teletrabajo alineada al Manual de política de seguridad de la información y a lo establecido Ley 1221 del 2008, quedando pendiente de ser aprobada.

No se encuentra establecido el cargo Líder de Seguridad de la Información en la entidad, pero se cuenta con un contratista de la oficina de Tecnología y Sistemas de Información para “apoyar, hacer seguimiento y contribuir con el desarrollo e implementación del Sistema de Gestión de Seguridad (SGSI) en la entidad, de conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC, la norma ISO 27001 y lo estipulado en la política de gobierno digital”

No se evidencia la identificación de responsabilidades para la protección de activos individuales y realización de procesos de seguridad de la información específicos en el equipo interno de Sistemas de Información, algunas responsabilidades de SI se plasman de manera muy básica en los perfiles específicos de funcionarios en la siguiente manera: Para los servidores públicos Acuerdo de confidencialidad A201PR01F03 “y para los contratistas Estudios previos A206PR01MO1

Si bien se cuenta con estudios previos y acuerdos de confidencialidad para los niveles de responsabilidad de los colaboradores de MINCIENCIAS frente al SGSI, no se evidencia adecuada distribución o segregación, entre las funciones y las áreas de responsabilidad para reducir las oportunidades de la modificación no autorizada o uso inadecuado de los activos de información.

Se encuentra oficializado y/o normalizado el documento relacionado con contacto con las autoridades (Procedimiento de incidentes) y el documento gestión de proyectos. D103PR03, el cual contiene el contacto con autoridades

Así mismo se evidencia el día de la auditoría la guía en GINA D102PR03G01 Guía para la gestión del riesgo y las oportunidades, donde se evidencio en el numeral 10. Gestión de riesgos de TI, los lineamientos desarrollados para la gestión de los proyectos del Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI alineado a

la seguridad de la información.

10. GESTIÓN DE RIESGOS DE TI

Los lineamientos desarrollados en este ítem aplican para los proyectos del Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI.

El proceso de identificación y gestión de los Riesgos de TI debe asegurar que no exceden el apetito ni la tolerancia al riesgo institucional de acuerdo con lo definido en el numeral 7.2 Apetito del Riesgo, del presente documento, y deben tratarse los riesgos residuales priorizados, con el fin de optimizar los recursos disponibles y enfocar los esfuerzos institucionales, según lo definido en el numeral 10.3 Tratamiento del Riesgo (medidas de respuesta).

Un escenario de riesgo describe un evento relacionado con TI que puede llevar a un impacto en la Entidad. Para que los escenarios de riesgo sean completos y se puedan utilizar en análisis de riesgos, deben contener los siguientes componentes, que se muestran en la tabla a continuación.

Tabla 2. Componentes del Escenario de Riesgos de TI

Escenario del Riesgo	**Actor**	• Interno (funcionarios, contratistas) • Externo (aliado estratégico o proveedor de TI)
	Tipo de amenaza	• Malicioso • Accidental • Fracaso • Natural
	Acción	• Divulgación • Interrupción • Modificación • Robo • Destrucción • Diseño ineficaz

en el marco de la Administración de proyectos. Se propone elaborar un documento de recomendaciones para incluir elementos de Seguridad de la Información en Proyectos Institucionales

A.7 Seguridad de los RRHH. 80%

Hacer seguimiento a las jornadas de sensibilización (asistencia del personal), debido a que algunos funcionarios aseguran no poder asistir a las capacitaciones y por lo tanto desconocen el Manual de Políticas de Seguridad de la Información

Debido a que existe una definición parcial de responsabilidades y roles de seguridad, como se mencionó en el anterior dominio, la aplicación de la seguridad de la información de acuerdo con las políticas establecidas por la Entidad también se lleva a cabo de forma parcial sobre empleados y contratistas.

Se evidencia exigencia de la dirección para que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.

No hay un procedimiento contemple los procesos disciplinarios en caso de que se requiera para el incumplimiento de contratista

A.8 Gestión de activos. 80%

En la Ministerio existen dos matrices de activos de información, una es la que se encuentra publicada en la página web y es administrada por el grupo interno de gestión documental https://minciencias.gov.co/registro-activos-informacion-documental Y la segunda matriz es de carácter clasificado y la administra la oficina de tecnologías y sistemas de información D103M02F01 Matriz de inventarios de activos de información de TI. La Entidad lleva a cabo un inventario de activos de información, que se encuentra en proceso de actualización razón por la cual existe un criterio de riesgo de desactualización de estos.

Sin embargo, dentro del alcance de la implementación de plan de seguridad de la información, se establece que los activos se deben actualizar el 31-12-2023, plan que fue aprobado en comité de gestión desempeño institucional e innovación en enero 2023 y por tal razón a la fecha no se encuentran desactualizado, esta en proceso de actualización.
El plan de seguridad de la información se puede evidenciar en: https://www.minciencias.gov.co/quienes_somos/planeacion_y_gestion/seguridad-informacion

Se evidencia procedimientos para el manejo de los activos de acuerdo con el esquema de clasificación de información adoptado por la organización D103M02.

Al existir como ya se mencionó una definición parcial de responsabilidades en cuanto a seguridad de la información, existen falencias en la concepción del término y la función de propiedad de los activos en lo que a los usuarios se refiere, razón por la cual algunos de los controles implementados no son efectivos, tal es el caso de la devolución de activos.
El Formato Traslados o devolución de bienes y elementos informáticos A203PR01F07 contempla la revisión del área de tecnología a través de la firma de mesa de servicio, la cual pertenece a la oficina de tecnologías y sistemas de información.

Ciencias

COLOMBIA POTENCIA DE LA VIDA	TRASLADO O DEVOLUCIÓN DE BIENES Y ELEMENTOS INFORMÁTICOS	**CÓDIGO:** A203PR01F0 **VERSIÓN:** 02 **FECHA:** 2022-07-28	Ciencias

Nombre de funcionario/contratista que e		Dependencia	
Número de identificación			
Nombre de funcionario/contratista que re		Dependencia	
Número de identificación			
Fecha (DD/MM/AA)		No. de ticket	

PLACA No.	SERIAL	DESCRIPCIÓN	OBSERVACIONES

Concepto Técnico (Mesa de servicios):

Firma funcionario/contratista que entrega	**Firma funcionario/contratista que recibe**
Nombre y firma del Analista que realiza el traslado	**V.º B.º Almacenista / Coordinador(a)**
Mesa de servicios	Grupo de Apoyo Logístico y Documental

A.9 Control de accesos. 90%

Es de gran importancia limitar el acceso a información y a instalaciones de procesamiento de información asegurando el acceso de los usuarios autorizados y evitando el acceso no autorizado a sistemas y servicios. Se observa que en la Entidad hace uso de contraseñas como medida para restringir el acceso a sus sistemas y se tiene conocimiento de la necesidad de desarrollar políticas de control de accesos, gestión de contraseñas y gestionar correctamente escenarios como el teletrabajo, por lo cual han tomado medidas basadas en las buenas prácticas. Sin embargo, existe documentación parcial y se encuentran en construcción nuevos documentos procedimiento de Ingreso seguro y Sistema de gestión de contraseñas.

Es necesario aclarar que la responsabilidad en la gestión de accesos es compartida entre Gestión de Tecnologías de Información y Gestión de Administración de Bienes y Servicios, ya que ésta última tiene a su cargo la gestión y monitoreo de los dispositivos de acceso físico, política que se actualizo.

El documento actualizado de la responsabilidad compartida del acceso físico a través de las tarjetas de proximidad es Reglamento Interno del Ingreso Peatonal y Vehicular A203PR02AN01.

2.2.1. ROLES Y RESPONSABILIDADES EN LA CUSTODIA DE LOS ELEMENTOS Y LA ADMINISTRACIÓN DEL SISTEMA DE ACCESOS:

RESPONSABLE	RESPONSABILIDADES
OTSI*	Garantizar el servicio: acceso al aplicativo (software) mantener operativos los servidores de la solución de control de acceso.
GITALyD**	Garantizar el acceso: mediante el usuario asignado al área y reportar novedades en el servicio.
OTSI	Configuración del aplicativo: gestionar grupos y permisos definidos según los grupos establecidos.
GITALyD	Asignar tarjetas de proximidad: tramitar la asignación de tarjetas de proximidad a servidores públicos y contratistas y asignar los permisos según sea el caso.
OTSI	Actualizar base de datos: una vez al año, en el 2 trimestre de cada vigencia, descargar la base de datos de usuarios y enviar al Grupo Interno de Trabajo de Apoyo Logístico y Documental junto con el registro de grupos y configuraciones existentes en el aplicativo para revisión, depuración y/o ajuste.
GITALyD	Actualizar base de datos: con la base de datos de usuarios, revisar, depurar y/o ajustar la información que sea necesaria y remitir a la OTSI para actualizar el aplicativo.
OTSI	Actualizar base de datos: actualizar el aplicativo con la información remitida por Logística.
GITALyD	Decepcionar tarjetas de proximidad: recibir las tarjetas de proximidad de servidores públicos y contratistas por desvinculación con la Entidad.
GITALyD	Mantener stock tarjetas de proximidad: custodiar las tarjetas de proximidad que no han sido asignadas y que se encuentran en buen estado.

(*): Oficina de Tecnología y Sistemas de Información.
(**): Grupo Interno de Trabajo de Apoyo Logístico y Documental

A.10 Criptografía 50%

Con la criptografía se busca asegurar el uso apropiado y eficaz de esta para proteger la entre otras, confidencialidad de la información. Se evidencia la mención de forma general a las políticas de controles criptográficos en el Manual de políticas de Seguridad de la Información, pero no existen procedimientos escritos sobre el uso protección y tiempo de vida de lasllaves criptográficas. Se evidencia el uso de controles criptográficos por ejemplo en el uso de conexiones VPN a través de los firewalls de la Entidad, sin embargo, como ya se mencionó no se han determinado de forma oficial criterios para establecer tiempos de vida o políticas de gestión de las llaves criptográficas.

Se recomienda sacar la V.2 del Manual de políticas de seguridad de la información contemplando certificado seguro y firma
Digital, así mismo se recomienda la instalación de programa criptográfico para control de información clasificada y reservada.

Se recomienda validar la configuración de control criptográfico en correo electrónico de usuarios que envían información clasificada y/o reservada

Seguridad física y del entorno. 90%

Se observa que la entidad ha tomado medidas para controlar el acceso físico no autorizado, el daño y la interferencia a la información.
Se actualizó el documento de A203PR02AN01 reglamento interno del ingreso peatonal y vehicular, donde se incluyó las

responsabilidades de Gestión de administración de bienes y servicios y oficina de tecnologías y sistemas de información.

2.2.1. ROLES Y RESPONSABILIDADES EN LA CUSTODIA DE LOS ELEMENTOS Y LA ADMINISTRACIÓN DEL SISTEMA DE ACCESOS:

RESPONSABLE	RESPONSABILIDADES
OTSI*	Garantizar el servicio: acceso al aplicativo (software) mantener operativos los servidores de la solución de control de acceso.
GITALyD**	Garantizar el acceso: mediante el usuario asignado al área y reportar novedades en el servicio.
OTSI	Configuración del aplicativo: gestionar grupos y permisos definidos según los grupos establecidos.
GITALyD	Asignar tarjetas de proximidad: tramitar la asignación de tarjetas de proximidad a servidores públicos y contratistas y asignar los permisos según sea el caso.
OTSI	Actualizar base de datos: una vez al año, en el 2 trimestre de cada vigencia, descargar la base de datos de usuarios y enviar al Grupo Interno de Trabajo de Apoyo Logístico y Documental junto con el registro de grupos y configuraciones existentes en el aplicativo para revisión, depuración y/o ajuste.
GITALyD	Actualizar base de datos: con la base de datos de usuarios, revisar, depurar y/o ajustar la información que sea necesaria y remitir a la OTSI para actualizar el aplicativo.
OTSI	Actualizar base de datos: actualizar el aplicativo con la información remitida por Logística.
GITALyD	Decepcionar tarjetas de proximidad: recibir las tarjetas de proximidad de servidores públicos y contratistas por desvinculación con la Entidad.
GITALyD	Mantener stock tarjetas de proximidad: custodiar las tarjetas de proximidad que no han sido asignadas y que se encuentran en buen estado.

(*): Oficina de Tecnología y Sistemas de Información.
(**): Grupo Interno de Trabajo de Apoyo Logístico y Documental

A.11 Seguridad en las operaciones 80%.

Con la seguridad en las operaciones se busca obtener operaciones correctas y seguras de las instalaciones de procesamiento de información. Aquí, se incluyen controles contra códigos maliciosos, respaldo de la información, separación de los ambientes de desarrollo, pruebas y operación, registro de eventos.

Se evidencia que la Entidad ha gestionado a través de la implementación de controles efectivos la seguridad en las operaciones a través de los mecanismos ya descritos. Se hace necesario sin embargo continuar con el proceso de documentar y actualizar los procedimientos que permitan evidenciar al proceso de mejoramiento continuo con énfasis en los siguientes aspectos:

- ✓ Implementación de los para la detección y seguimiento a fallos.
- ✓ Control parcial de cambios en los sistemas de procesamiento de información.
- ✓ Procedimiento de Gestión de la capacidad
- ✓ Se cuenta catalogo se componentes de información

Catálogo de Sistemas de Información / Aplicaciones

Código	ID	ID_B	Tipo de Sist	Sistema de información - Aplicación	ID	Módulo	URL	Certificado actualiza	ID	Dependencia Líder Iniciativa - Area Técnica	Responsable Area Técnica (Nombre y correo)	Usuarios del Sistem	ResponsableTecnología	Entidad Proveedor	Contacto Proveedor	Correo elec
2101001	01	01	Misional	ScienTI	001	CvLAC	https://scienti.minciencias.gov.co/cvlac/Login/pre_s_login.do	ok - Balanceador	21	Dirección de Ciencia	Claudia Liliana Castro Vargas - lcastro@minciencias.gov.co	Ciudadanos y funcionarios del Ministerio	Nidia Janneth León Cabeza	MIC System SAS	[illegible]	dlbarr meryhel
2101002	01	01	Misional	ScienTI	002	GrupLAC	https://scienti.minciencias.gov.co/gruplac/	ok - Balanceador	21	Dirección de Ciencia	Claudia Liliana Castro Vargas - lcastro@minciencias.gov.co	Ciudadanos y funcionarios del Ministerio	Nidia Janneth León Cabeza	MIC System SAS	[illegible]	dlbarr meryhel
2101003	01	01	Misional	ScienTI	003	InstituLAC	https://scienti.minciencias.gov.co/institulac2-war/	ok - Balanceador	21	Dirección de Ciencia	Claudia Liliana Castro Vargas - lcastro@minciencias.gov.co	Ciudadanos y funcionarios del Ministerio	Nidia Janneth León Cabeza	MIC System SAS	[illegible]	dlbarr meryhel
2101004	01	01	Misional	ScienTI	004	Créditos condonables	https://scienti.minciencias.gov.co/dirrechum/becarios/index.jsp	ok - Balanceador	21	Dirección de Ciencia	Claudia Liliana Castro Vargas - lcastro@minciencias.gov.co	Ciudadanos y funcionarios del Ministerio	Nidia Janneth León Cabeza	MIC System SAS	[illegible]	dlbarr meryhel
2101005	01	01	Misional	ScienTI	005	Publindex	https://scienti.minciencias.gov.co/publindex/	ok - Balanceador	21	Dirección de Ciencia	Claudia Liliana Castro Vargas - lcastro@minciencias.gov.co	Ciudadanos y funcionarios del Ministerio	Nidia Janneth León Cabeza	MIC System SAS	[illegible]	dlbarr meryhel
2101006	01	01	Misional	ScienTI	006	Ciencia y Tecnología para todos	https://scienti.minciencias.gov.co/ciencia-war/	ok - Balanceador	21	Dirección de Ciencia	Claudia Liliana Castro Vargas - lcastro@minciencias.gov.co	Ciudadanos y funcionarios del Ministerio	Nidia Janneth León Cabeza	MIC System SAS	[illegible]	dlbarr meryhel
2101008	01	01	Misional	ScienTI	008	Pares evaluadores	https://scienti.minciencias.gov.co/paresEvaluadores/	ok - Balanceador	21	Dirección de Ciencia	Claudia Liliana Castro Vargas - lcastro@minciencias.gov.co	Ciudadanos y funcionarios del Ministerio	Nidia Janneth León Cabeza	MIC System SAS	[illegible]	dlbarr meryhel
2102001	02	47	Misional	Moodle Educación virtual minciencias (Currículo del editor)	001	Programa de Formación a Equipos Editoriales de Revistas Científicas Nacionales	https://educacionvirtual.minciencias.gov.co/login/signup.php https://renata.zoom.us/signin	ok - Balanceador	21	Dirección de Ciencia	Jean Rogelio Linero Cueto jrlinero@minciencias.gov.co	Ciudadanos y funcionarios del Ministerio	Diego Andrés Molina Estrea	In-House [Minciencias]	[illegible]	dmolina@
2103001	03	45	Informativos Digitales	Desempeño Evaluadores	001	Desempeño Evaluadores	https://goo.gl/BRjf6A	No aplica	21	Dirección de Ciencia	Jean Rogelio Linero Cueto jrlinero@minciencias.gov.co	Todo el Ministerio	Diego Andrés Molina Estrea	In-House [Minciencias]	[illegible]	dmolina@
210400	04	46	Informativos	Formulario de Prelascripción al	001	Formulario de Prelascripción al	https://goo.gl/wVFnBh	No aplica	21	Dirección de Ciencia	Jean Rogelio Linero Cueto	Todo el Ministerio	Diego Andrés Molina	In-House	[illegible]	dmolina@

A.12 Seguridad en las Comunicaciones. 90%

El objetivo de la Entidad de asegurar la protección de la información en las redes y la transferencia de información se ha enfocado en la implementación de controles para proteger la confidencialidad, integridad y disponibilidad de la información publicada y transferida en los escenarios LAN y WAN de la Entidad. Se hace necesario ajustar y actualizar los procedimientos publicados con respecto a los acuerdos sobre transferencia segura de información para asegurar criterios de trazabilidad y no repudio.

A.13 Adquisición de sistemas, desarrollo y mantenimiento. 40%

Esta la política de desarrollo Seguro, pero no existen procedimientos que establecen directrices sobre actividades relacionadas con la adquisición de sistemas, desarrollo y mantenimiento basados en las mejores prácticas para el caso específico de MINCIENCIAS.
Es necesario aclarar que el desarrollo de sistemas de información no está contemplado en el alcance de ejecución de actividades de Gestión de Tecnologías de Información puesto que no se dispone de la infraestructura que permita llevar a cabo procesos de desarrollo de aplicaciones.

Sin embargo se evidencio en la auditoria que la entidad tiene proyectado los documentos de lineamientos de desarrollo seguro y plan maestro de operaciones para sistemas de información, donde se establece las directrices de la adquisición, desarrollo y mantenimiento de sistemas. Pendiente de normalizar en el sistema de gestión de calidad

A.14 Relación con proveedores. 70%

En la Entidad la relación con los proveedores se establece contractualmente. Dichos contratos incluyen acuerdos de confidencialidad.
Sin embargo, dichos acuerdos contemplan requisitos muy básicos de seguridad de la información, situación que genera un criterio de riesgo en el establecimiento de las relaciones con proveedores que puedan tener acceso, procesar, almacenar,

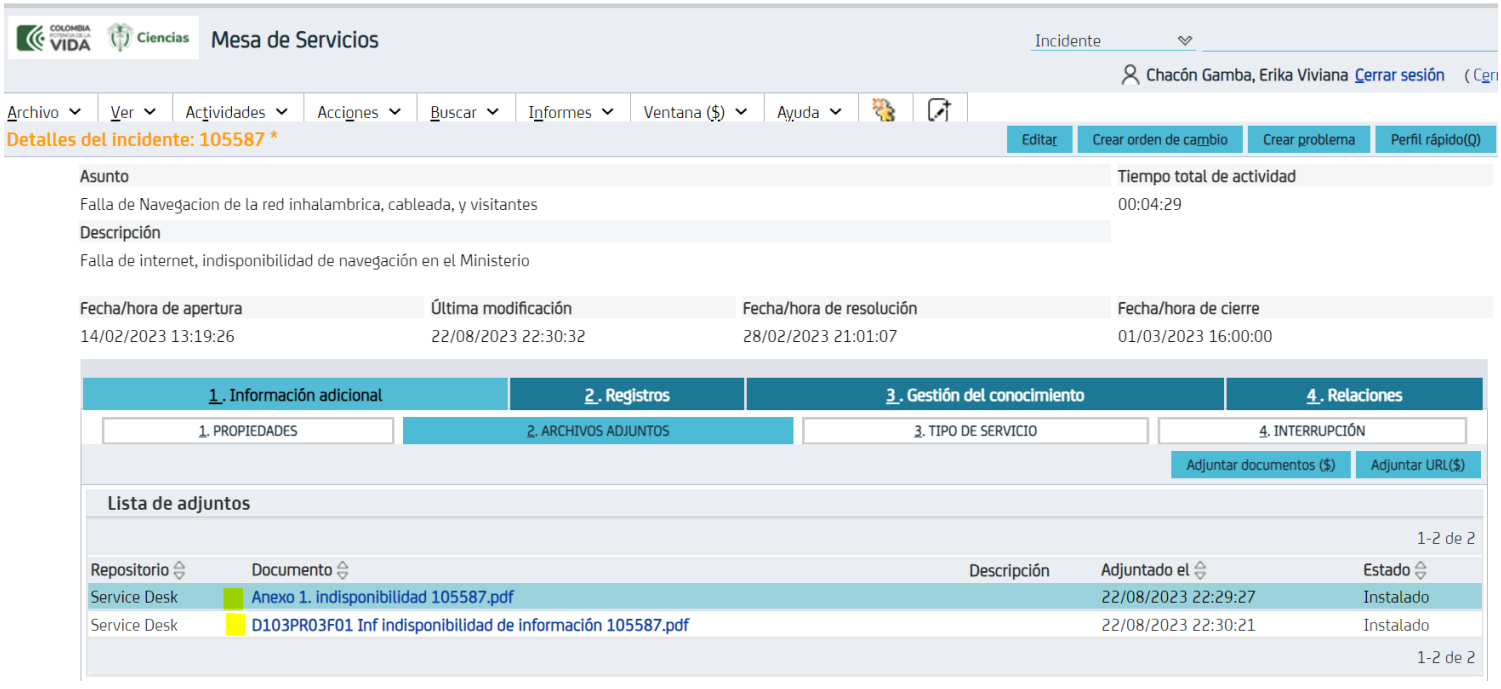
comunicar o suministrar componentes de infraestructura de TI y que se pudiesen materializar en escenarios de incumplimiento ante la inexistencia de controles efectivos.

Adicional de las cláusulas de los contratos, se tiene un acuerdo se seguridad de la información para terceros incluido en GINA como D10M01F01, Documento que contiene las características de confidencialidad y seguridad de la información que terceros deben cumplir al momento de poseer información entregada por Minciencias.

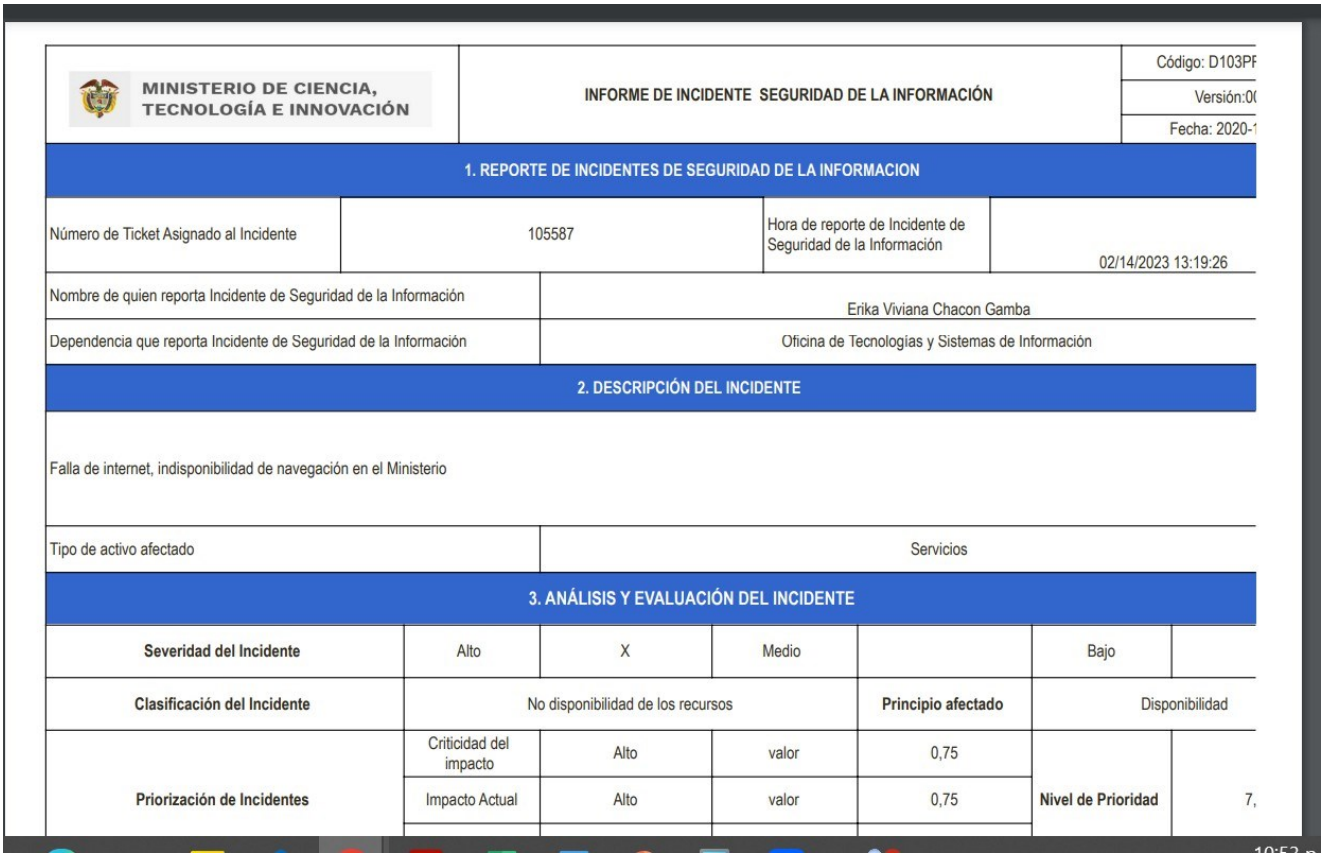
A.15 Gestión de los incidentes de seguridad. 65%

La Gestión de Incidentes propende por asegurar un enfoque coherente y eficaz para el manejo de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
Se evidencia que al interior de MINCIENCIAS., existen canales formales de comunicación (mesa de servicios) se informe acerca de eventos e incidentes de seguridad al grupo de trabajo (soporte) con el fin de generar los correspondientes planes de acción.
Existen sin embargo debilidades en cuanto a la apropiación por parte de los usuarios finales de la cultura de reportar incidentes de seguridad, lo que a su vez determina que la base de conocimiento no crezca en el espectro de casos que permita disminuir tiempos de respuesta y generación de planes de acción efectivos.

En los tickets de mesa de servicios se adjunta el informe de incidentes de seguridad de la información D103PR03F01 y adicionalmente se adjunta el anexo donde incluye las lecciones aprendidas, tal como lo describe el procedimiento de incidentes de seguridad de la información D103PR03



Del informe de incidentes de seguridad solo se evidencia 2 reportes.



MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN

INFORME DE INCIDENTE SEGURIDAD DE LA INFORMACIÓN

Código: D103PF
Versión:0(
Fecha: 2020-1

1. REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Número de Ticket Asignado al Incidente	105587	Hora de reporte de Incidente de Seguridad de la Información	02/14/2023 13:19:26
Nombre de quien reporta Incidente de Seguridad de la Información	Erika Viviana Chacon Gamba		
Dependencia que reporta Incidente de Seguridad de la Información	Oficina de Tecnologías y Sistemas de Información		

2. DESCRIPCIÓN DEL INCIDENTE

Falla de internet, indisponibilidad de navegación en el Ministerio

Tipo de activo afectado	Servicios

3. ANÁLISIS Y EVALUACIÓN DEL INCIDENTE

Severidad del Incidente	Alto	X	Medio		Bajo	
Clasificación del Incidente	No disponibilidad de los recursos			**Principio afectado**	Disponibilidad	
Priorización de Incidentes	Criticidad del impacto	Alto	valor	0,75		
	Impacto Actual	Alto	valor	0,75	**Nivel de Prioridad**	7,

A.16 Continuidad del negocio. 0%

En este se hace necesario planificar, implementar, verificar, revisar y evaluar la continuidad de la seguridad de la información. MINCIENCIAS debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa, situación que se ha evidenciado en el caso de las bases de datos corporativas, cubiertas por el concepto de continuidad del negocio con un proveedor externo.
Se evidencia de igual forma que el concepto de continuidad del negocio no se aplica y no se encuentra documentado el concepto de Recuperación de desastres ni de matriz BIA.

A.17 Cumplimiento con requerimientos legales y contractuales. 80%

La entidad ha referenciado normativas y disposiciones legales vigentes relacionadas con el resguardo de la propiedad intelectual y las demás concordantes de aplicabilidad identificadas en leyes y decretos de MINCIENCIAS. Sin embargo, en el formato de Unificación Normativa no se hace referencia a documentos que soporten el SGSI como es el caso de la ISO/IEC 27001:2013, gestión de riesgos de seguridad de la información ISO 27005 entre otras.

PROCESOS CONTRACTUALES 2020/2021 EJECUTADOS - ASOCIADOS AL SGSI

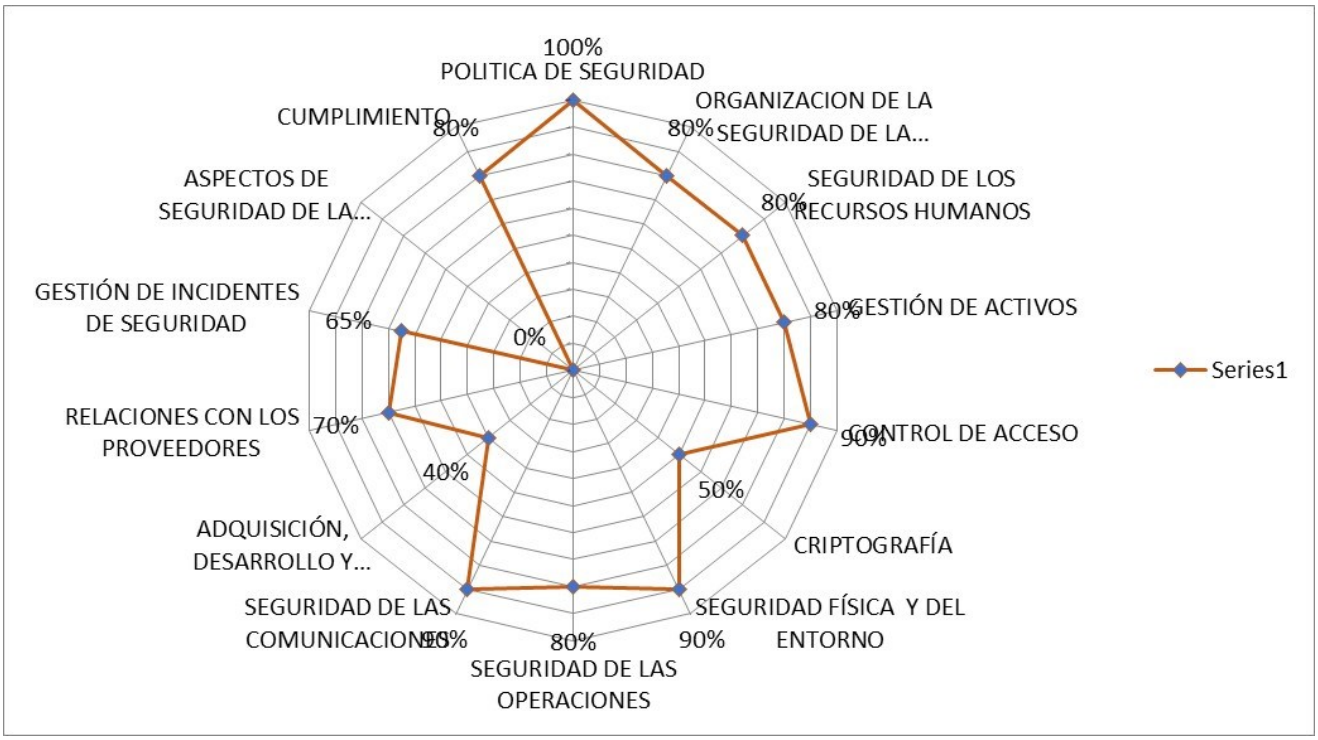
Objeto	Valor estimado	No Contrato
Renovar el licenciamiento de RedHat que incluye soporte, actualizaciones y registro para las máquinas virtuales Linux del Ministerio de Ciencia, Tecnología e Innovación - MINCIENCIAS	34.709.920	414-2023
Realizar la renovación del registro ante LACNIC para el direccionamiento público IPv4 e IPv6 del Ministerio de Ciencia, Tecnología e Innovación - MINCIENCIAS	$3.884.000	415-2023
Realizar la adquisición de cintas LTO 7 para el Ministerio de Ciencia, Tecnología e Innovación - MinCiencias.	$41.890.380	699-2032
dquisición, instalación, configuración y migración de la solución de seguridad perimetral (Firewall de próxima generación) en alta disponibilidad, que incluya soporte, mantenimiento, garantía y servicios especializados, para el Ministerio de Ciencia, tecnología e Innovación – Minciencias	$645.000.000	604-2022

Tabla de resultados por dominio:

Esta tabla, recoge y resume los porcentajes de avance del resultado de Nivel de Implementación de Controles, y muestra el grado de cumplimiento para el total de dominios, tal y como se muestra a continuación:

Item	Dominios	Cumplimiento
5	POLITICA DE SEGURIDAD	100%
6	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN	80%
7	SEGURIDAD DE LOS RECURSOS HUMANOS	80%
8	GESTIÓN DE ACTIVOS	80%
9	CONTROL DE ACCESO	90%
10	CRIPTOGRAFÍA	50%
11	SEGURIDAD FÍSICA Y DEL ENTORNO	90%
12	SEGURIDAD DE LAS OPERACIONES	80%
13	SEGURIDAD DE LAS COMUNICACIONES	90%
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	40%
15	RELACIONES CON LOS PROVEEDORES	70%
16	GESTIÓN DE INCIDENTES DE SEGURIDAD	65%
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	0%
18	CUMPLIMIENTO	80%
TOTAL		71%

Los porcentajes de avances para cada uno de los dominios y subdominios, fueron evaluados mediante los procesos de Gestión de Tecnología de la Información, Gestión Contractual, Gestión Jurídica, Gestión de Administrativa - Bienes y Servicios, Gestión Documental, Gestión Financiera- Direccionamiento General e Informes, Gestión de Evaluación y Control y por la documentación existente en la intranet de la entidad en el micrositio designado para los (Manuales, Formatos, Procedimientos, instructivos, protocolos etc.



De acuerdo con la gráfica, se observa que los dominios con mayor nivel de madurez son política de seguridad (100%), Control de acceso (90%), Seguridad física y del entorno (90), Seguridad de las Comunicaciones (90) lo cual resulta del respaldo de la Alta Dirección y de la gestión adelantada por la Oficina de Gestión de Tecnología de Información para la implementación del Sistema de Seguridad de la Información.

Sin embargo y aunque se muestra un avance significativo en los aspectos mencionados, el nivel de madurez al corte de Agosto de 2023 del SGSI fue del 71% que significa de acuerdo a la escala de cumplimiento definida en el análisis GAP, que la Entidad está levemente por debajo del nivel “Definido” (70%) y por encima del nivel “repetible (40%) es decir, que los procesos se encuentran documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.

Dichos avances no se han desarrollado en similares porcentajes en todos los frentes, prueba de ello son los relativos bajos, avances en lo que tiene que ver con: Adquisición desarrollo y Mantenimiento de los sistemas (40%)Criptografía (50%), Continuidad del Negocio (0%), los cuales muestran muy bajos avances comparados con los otros dominios de la Norma. No obstante, se considera importante precisar que, dado que la Entidad no cuenta con un plan de continuidad del negocio, se incrementan los riesgos de interrupciones no planificadas en TI y telecomunicaciones, ciberataques, brechas de datos, interrupciones del suministro de red, incidentes de seguridad. Riesgos que no fueron identificados, analizados, valorados en el mapa de riesgos de los procesos: Gestión de Recursos tecnológicos y Gestión de Tecnologías de la Información, publicados en la intranet al corte de la presente evaluación.

6.2.3 OPORTUNIDADES DE MEJORA

Publicar oportunamente la versión No 2 del Manual de políticas de Seguridad de la información, lo anterior dado a que si bien, está contemplado como fecha máxima de publicación, en diciembre de 2023, su verificación al cumplimiento de las disposiciones planificadas y comprobando que se mantienen de manera eficaz los controles, en el modelo de Seguridad y Privacidad de la información implementado en MINCIENCIAS solo aumento en un 3 % de avances en un año.

Después de realizar las entrevistas y revisar si hay s planes de contingencia de la plataforma de TIC del año respectivamente, puede afirmarse que se incumple con el control ID: A.17.1.3 verificación, revisión y evaluación de la continuidad de la seguridad de la información, toda vez que plan no ha sido probado en su totalidad, las evidencias suministradas no son suficientes para respaldar un ejercicio adecuado que garantice la continuidad de las operaciones y servicios que provee la entidad, es necesario poner en práctica y realizar el simulacro del plan de contingencia para los sistemas críticos de la entidad y determinar su eficacia.

La entidad cuenta con algunos elementos redundantes lo cual es soportado mediante la evidencia aportada del datacenter, pero no se encuentra documentado en el Plan de contingencia de la plataforma TIC, lo que incumple el control id: A.17.2.1 toda vez que no se cuenta con las "redundancias suficientes" para cumplir con la disponibilidad de los servicios y sistemas críticos de entidad que pudieran verse afectados o comprometidos por un evento o incidente de alto impacto.

Se cuenta con una Política sobre el uso de controles Criptográficos sin embargo se requiere fortalecer los mecanismos que permitan realizar *los controles Criptográficos y gestión de claves* para determinar patrones o comportamientos similares o reincidencia y generar las acciones correctivas que eliminen la no conformidad por cuanto no se tiene evidencia actual que demuestre el cumplimiento al requisito del numeral 10.1 de la norma ISO27001:2013.

Se pudo identificar que no se cuenta con un soporte de los planos del Data Center y de un inventario de los materiales utilizados para su construcción, por lo cual se registra esta situación como una debilidad dentro de la sección de observaciones del presente informe, teniendo en cuenta el riesgo que en algún momento puede llegar a ocasionar afectaciones sobre la planificación e implementación de mejoras a la infraestructura del lugar y con ello afectar su desempeño y operación.

De la misma manera fue posible conocer que no se han realizado simulacros para verificar la efectividad de los controles que se tienen implementados en el Data Center para la protección de los equipos y la información, por lo cual se registra esta situación dentro de la sección Oportunidades de Mejora del presente informe, con el fin que a través de pruebas se pueda asegurar el correcto funcionamiento y la efectividad de los controles.

No se cuenta con la aplicación de una normatividad que se deba cumplir para el diseño e implantación del Data Center en la entidad, por ejemplo la ANSI / TIA-942 que es el estándar de calidad que especifica los requisitos para centros de datos. La topología presentada en la norma es aplicable a cualquier centro de datos de cualquier tamaño y cubre toda la infraestructura física, incluidos, entre otros requisitos: ubicación del sitio, sistema eléctrico, mecánico, seguridad contra incendios, telecomunicaciones, seguridad y entre otros, por lo que requiere que se cuente con un proceso de mejora para cumplir en su totalidad con la norma anteriormente mencionada y así cumplir con las adecuaciones.

Luego de realizar la visita in situ al Data Center, se pudo evidenciar que es un lugar un poco pequeño que dificulta el transitar dentro del mismo, evidenciando que, al encontrarse más de una persona al tiempo dentro del mismo, puede llegarse a tropezar y/o desconectar algún dispositivo de comunicación, por lo cual se recomienda revisar dicha situación y tomar las medidas que se requieran de manera oportuna. Adicionalmente no cuenta con señalización en caso de

emergencia.

Por parte de la Oficina de Control Interno, teniendo en cuenta lo evidenciado en la visita efectuada al Data Center y tal cual como fue registrado anteriormente, se considera que el lugar alcanza niveles de Componentes Redundantes, de acuerdo al estándar TIA 942, sin embargo, se deja registrado dentro de las oportunidades de mejora del presente informe, la recomendación para que la Oficina Asesora de Planeación y gestión de Tecnologías de la Información solicite la certificación del centro de cómputo, a través de las entidades especializadas que se encargan de verificar los centros de datos y entregar las correspondientes certificaciones que confirman el diseño, la construcción y la sostenibilidad del lugar

Protección de la información del Data Center es a través del directorio activo de la entidad se controlan los permisos para que los usuarios ejecuten acciones como la instalación de software no autorizado, así como también a través del aplicativo, el cual se encuentra debidamente licenciado. De igual manera, por medio del antivirus que se tiene licenciado y de la plataforma de seguridad del Firewall, se protege la información contra virus, spyware y demás ataques cibernéticos.
Las contraseñas de acceso a las bases de datos son gestionadas por los administradores de las bases de datos, para lo cual se lleva un control de claves con el apoyo del software de adquisición, que básicamente es una herramienta que facilita la administración de contraseñas.

Se evidencia inoportunidad al inicio de la implementación de los contratos y/o proyectos asociados al SGSI, dado a que los mencionados en la Auditorias anteriores, su ejecución fue mucho después de las fechas planeadas para su ejecución como es el caos de :

Objeto	Valor estimado	Rubro	No. Contrato
Renovación del soporte, garantía y licenciamiento para la solución de seguridad perimetral Checkpoint y EndPoints para el Ministerio de Ciencia, Tecnología e Innovación – MINCIENCIAS.	$380.926.000	Operación y Control	CTO-887
Contratar el soporte y mantenimiento de las plataformas tecnológicas que soportan la infraestructura de la Entidad y una bolsa de repuestos e instalación bajo demanda para el Ministerio de Ciencia Tecnología e Innovación.	$140.059.500		CTO 549-20
Adquirir el licenciamiento, soporte y garantía para la solución de protección de tráfico web que posee la entidad (Blue Coat Proxy SG200) para el Ministerio de Ciencia, Tecnología e Innovación – MINCIENCIAS.	$208.202.000		CTO-390

Renovar el Licenciamiento para la Solución Integral de Seguridad para Servidores, Redes y Usuario Final – Trendmicro del Ministerio de Ciencia Tecnología e Innovación.	$285.799.504,80		802-2020
Adquirir la suscripción de la solución de seguridad WAF CLOUD en modalidad SaaS, para el Ministerio de Ciencia Tecnología e Innovación - MINCIENCIAS.	$84.996.000		885-2020

6.3 Conclusiones y Recomendaciones

La entidad muestra una correcta gestión de los marcos normativos basados en la norma ISO 27001:2013, dando un cumplimiento a algunos de los numerales de la norma, por lo cual se debe trabajar en las observaciones, oportunidades de mejora y No conformidades evidenciadas durante la auditoria, se deben cerrar en un lapso muy corto de tiempo o si es posible, de inmediato, por lo cual el riesgo de pérdida de información se podría materializar aprovechando la vulnerabilidad evidenciada y la probabilidad que existe

Con el fin de asegurar que todos los recursos presentes en el Data Center apoyan directamente las necesidades de la entidad, se recomienda solicitar la certificación, en relación con la clasificación Tier para el centro de cómputo, otorgada por el Uptime Institute, donde se refrende la disponibilidad y efectividad de todos sus componentes y se determine oportunamente aquellos aspectos susceptibles de mejoramiento.

Se realiza la revisión por la Dirección anual para seguridad de la información, el último comité realizado fue sesión 32 Comité Ministerial 21/12/2022 Se adjunta correo, agenda y presentación

Fwd: Solicitud de adicionar tema al comité ministerial sesión No. 32 (21/12/2022)
1 mensaje

Carlos Eduardo Orjuela Oliveros <ceorjuela@minciencias.gov.co> 16 de diciembre de 2022, 19:12
Para: Erika Viviana Chacón Gamba <evchacon@minciencias.gov.co>

Para tu conocimiento. Gracias.

---------- Forwarded message ---------
De: **Carlos Eduardo Orjuela Oliveros** <ceorjuela@minciencias.gov.co>
Date: vie., 16 de diciembre de 2022 8:18 a. m.
Subject: Solicitud de adicionar tema al comité ministerial sesión No. 32 (21/12/2022)
To: Sandra Liliana Martínez León <slmartinez@minciencias.gov.co>
Cc: Angie Paola Molina Vargas <apmolina@minciencias.gov.co>

Cordial saludo Dra. Sandra Liliana,

Agradezco por favor adicionar la "Revisión por la Dirección Sistema de Seguridad y Privacidad de Información -SGSI" dentro de la agenda del comité ministerial sesión No. 32 (21/12/2022), para tal efecto adjunto la respectiva presentación y agradezco se permita a nuestro apoyo de seguridad de la información en lo posible de forma presencial, Erika Chacón, apoyarme durante dicha presentación.

Cordialmente,

--
MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN
Carlos Eduardo Orjuela Oliveros
Jefe Oficina de Tecnologías y Sistemas de Inforamcion
ceorjuela@minciencias.gov.co
Tel: 6258480 Ext: 3500
AV. Calle 26 No. 57-83 Torre 8. Piso 2 al 6
Bogotá, Colombia
www.minciencias.gov.co

No imprimas si no es necesario. Seamos responsables con la protección del medio ambiente.

Declinación de Responsabilidades - Disclaimer

14-12-22 Revisión por la Dirección SGSI.pptx
4101K

Se tiene oficializada el Manual de políticas de seguridad de la información D103M01, y contiene la política de copia de respaldos en el numeral 6.8.3 y actualmente se tiene una acción de mejora AI-0219 relacionado con documentar toda la gestión de backup y vence el 31 de diciembre 2023.

Se tiene oficializada el Manual de políticas de seguridad de la información D103M01, y contiene la política de copia de respaldos en el numeral 6.8.3, por tal razón se generó oportunidad de mejora en documentar los lineamientos de backup

Dar efectivo cumplimiento a lo enunciado en la NTC-ISO 27001:2013, específicamente en realizar y evidenciar resúmenes de los análisis de incidentes y vulnerabilidades de seguridad de la información, así como su respectiva presentación a la Alta Dirección para que se cuente con información necesaria para la toma de decisiones que encaminen al SGSI hacia la mejora continua. Lo anterior en razón a que durante la realización del diagnóstico se evidenció que en la Entidad no se realizan y tampoco son presentados ante la gerencia de la Entidad, incumpliendo lo definido en la norma mencionada.

Contar con el equipo necesario la implementación de la NTC-ISO 27001 en la Entidad, ya que se evidenció que no existe un equipo de trabajo completo, generando así incumplimiento en el numeral 5.1 de la norma enunciada.

Todos los cambios a sistemas de información son controlados por medio de los formatos: Formato Solicitud requerimiento para cambios a Sistemas de Información D103PR02F01 y de Pruebas funcionales de aceptación D103PR02F02, alineados al procedimiento de gestión cambios D103PR02 - Identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección, Todo lo consignado en el catálogo de sistemas de información y aplicaciones es susceptible de cambios. Se cuenta con un catálogo de sistemas información - revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios; se realiza por medio del formato de pruebas de aceptación donde los usuarios finales verifican directamente sobre un ambiente de pruebas lo solicitado y lo formalizan en el mismo para poder pasar a despliegue - mantener un rastro de auditoría de todas las solicitudes de cambio, se ejecuta el procedimiento de Gestión de cambios, el cual deja su rastro a partir de la asignación de un número de caso con su respectivo diligenciamiento, formatos y evidencias - asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados. Se realiza, hace parte del procedimiento para poder cerrar cada solicitud - asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados contratado externamente, se ejecuta el procedimiento de Gestión de cambios, donde se realiza un comité al cuál se presenta el cambio, se evalúan los riesgos y oportunidad para finalmente definir el momento adecuado para su ejecución - Definir los acuerdos de licenciamiento, propiedad de los

códigos y derechos de propiedad intelectual relacionados con el contenido contratado. Para los contratos se incluyen cláusulas que específicas que los derechos patrimoniales son propiedad del Ministerio

Fortalecer las campañas de sensibilización para asegurar que los empleados y contratistas tomen conciencia y den cumplimiento a sus responsabilidades en materia de seguridad de la información.
Implementar un canal de reporte anónimo de incumplimiento de políticas o procedimientos de seguridad de la información ("Denuncias internas") de modo que los clientes internos de la Entidad, puedan participar y aportar propuesta de mejora en lo que respecta a la gestión de la seguridad de la información. Lo anterior ya que no se evidenció dicho mecanismo, tal y como lo establece el numeral 7.2.1, de la GTC-ISO/IEC 27001:2013.

Fortalecer e implementar estrategias para el cumplimiento adecuado de la política de puesto de trabajo despejado y bloqueo de pantalla asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades y la cumplan. Lo anterior con el fin de implementar correctamente el SGSI y garantizar la adecuada seguridad de la información que es responsabilidad de los colaboradores de minciencias.

Fortalecer los procedimientos de operación documentándolos y poniéndolos a disposición de todos los usuarios que los necesitan, con el fin de que todos los colaboradores tengan acceso a la documentación del SGSI y se fomente la cultura de la mejora continua en lo que respecta al SGSI, tal como lo define la NTC-ISO-IEC 27001:2013.

Fortalecer las políticas de desarrollo seguro, así como los respectivos controles para establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la Entidad y los cambios de los sistemas dentro del ciclo de vida de desarrollo de software, de modo que se dé adecuado cumplimiento a lo definido en la NTC-IEC-ISO 27001:2013.

Fortalecer la política para el reporte y tratamiento de incidentes de seguridad mediante controles que permitan asegurar una respuesta rápida eficaz y ordenada a los incidentes de Seguridad de la Información.

no se protege adecuadamente los ambientes de trabajo seguro para las actividades de desarrollo e integración de los sistemas que comprenden todo el ciclo de vida de desarrollo de sistemas.

Establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Entidad.

Lo anterior, a que en la Entidad no se han establecido y acordado todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

Definir acuerdos con los proveedores y estos incluyen requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

Lo anterior en razón a que en la entidad no se han definido los acuerdos con los proveedores y estos incluyen requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

Controlar y revisar los servicios, reportes y registros suministrados por terceras partes. Lo anterior en razón a que se controlan de forma parcial y revisan los servicios, reportes y registros suministrados por terceras partes y se llevan a cabo auditorías a intervalos regulares a los servicios suministrados por terceros.

Diseñar e implementar mecanismos para cuantificar y monitorear los tipos, los volúmenes y los costos del incidente de la Seguridad de la Información. Lo anterior en razón a que, en la entidad, no existen implementados mecanismos para

cuantificar, monitorear los tipos, los volúmenes, y los costos de los incidentes de seguridad de la información y de mal funcionamientos.

Diseñar e implementar un BCP (Bussines Continuity Plan) y un DRP (Disaster Recovery Plan) y el BIA (Bussines Impact Analysis) que contenga:

Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias.

Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.

Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección.

Realizar pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información.

Tener arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo.

Ordenado los cables de datos conectados de los diferentes Patch Panel de los Rack dentro del Data Center, de manera que se pueda proteger contra interceptación, interferencia o daño cumpliendo el Control A11.2.3 del Anexo A de la Norma ISO/IEC 27001:2013.

7. PLAN DE MEJORAMIENTO

Con base en este informe definitivo, se solicita al Oficina de Tecnologías y Sistemas de Información como dependencia responsable, que elabore un Plan de Mejoramiento, en el formato adjunto, que dé solución a las observaciones identificadas y sea remitido a la Oficina de Control Interno para su aprobación, dentro de los ocho (8) días hábiles siguientes al recibo del presente informe.

Se recuerda que las acciones del Plan de Mejoramiento deben ser preventivas y/o correctivas, según el caso y requieren ser formuladas de manera efectiva para subsanar las debilidades encontradas, cuyas actividades no deben ser superiores a un año a partir de la suscripción del Plan en la Oficina de Control Interno.

Igualmente es necesario tener en cuenta que si en la ejecución de las acciones de mejora que se propongan se requiere la participación y responsabilidad de otras dependencias, la dependencia responsable del proceso auditado deberá coordinar con dichas dependencias la elaboración del Plan de Mejoramiento, antes de la presentación del Plan a la OCI.

Luz Marlenny Cano

Firma del Auditor:
Luz Marlenny Cano R.

GUILLERMO ALBA CARDENAS
JEFE DE LA OFICINA DE CONTROL INTERNO