1. OBJETIVOS

Evaluar 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 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. DESCRIPCIÓN DEL TRABAJO REALIZADO, OPCIONES DE MEJORA y CONCLUSIONES:

Estado actual con respecto a la ISO/IEC 27001:2013

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, CP, CS, NA. De acuerdo a la información que se presenta en la siguiente tabla:

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	☑			
A.5.1.2	Revisión de políticas para la seguridad de la Información	☑			
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA**				

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
	INFORMACIÓN				
A.6.1	**Organización Interna**				
A.6.1.1	Roles y responsabilidades para la seguridad de la información	☑			
A.6.1.2	Separación de deberes		☑		
A.6.1.3	contacto con las Autoridades			☑	
A.6.1.4	Contacto con los grupos de Interés especial		☑		
A.6.1.5	Seguridad de la información en la gestión de proyectos			☑	
A.6.2	**Dispositivos móviles y de teletrabajo**				
A.6.2.1	Políticas para dispositivos móviles	☑			
A.6.2.2	Teletrabajo	☑			
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**				
A.7.1	**Antes de asumir el empleo**				
A.7.1.1	Selección		☑		
A.7.1.2	Términos y condiciones del empleo		☑		
A.7.2	**Durante la ejecución del empleo**				
A.7.2.1	Responsabilidades de la dirección	☑			
A.7.2.2	Toma de conciencia educación y formación de la seguridad de la información	☑			
A.7.2.3	Proceso disciplinario		☑		
A.7.3	Terminación y cambio de empleo				
A.7.3.1	Terminación o cambio de responsabilidades de empleo		☑		
A.8	**GESTION DE ACTIVOS**				
A.8.1	**Responsabilidades de los activos**				
A.8.1.1	Inventario de Activos		☑		
A.8.1.2	Propiedad de los Activos		☑		
A.8.1.3	Uso aceptable de los activos		☑		
A.8.1.4	Devolución de Activos		☑		
A.8.2	**Clasificación de la información**				
A.8.2.1	Clasificación de la información		☑		
A.8.2.2	Etiquetado de la información		☑		
A.8.2.3	Manejo de activos		☑		
A.8.3	**Manejo de medios**				
A.8.3.1	Gestión de medios removibles		☑		
A.8.3.2	Disposición de los medios		☑		
A.8.3.3	Transferencia de medios físicos	☑			
A.9	**CONTROL DE ACCESO**				
A.9.1	**Requisitos del negocio para el control de acceso**				

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
A.9.1.1	Política de control de acceso	☑			
A.9.1.2	Acceso a redes y a servicios en red	☑			
A.9.2	**Gestión de acceso a Usuarios**				
A.9.2.1	Registro y cancelación del registro de usuarios		☑		
A.9.2.2	Suministro de acceso de usuarios	☑			
A.9.2.3	Gestión de derechos de acceso privilegiado		☑		
A.9.2.4	Gestión de información de autenticación secreta de usuarios	☑			
A.9.2.5	Revisión de los derechos de acceso de usuarios	☑			
A.9.2.6	Retiro a ajuste de los derechos de acceso		☑		
A.9.3	**Responsabilidades de los usuarios**				
A.9.3.1	Uso de Información de autenticación secreta	☑			
A.9.4	**Control de Acceso a sistemas y aplicaciones**				
A.9.4.1	Restricción de acceso a la información	☑			
A.9.4.2	Procedimiento de Ingreso seguro			☑	
A.9.4.3	Sistema de gestión de contraseñas			☑	
A.9.4.4	Uso de programas utilitarios privilegiados		☑		
A.9.4.5	Control de acceso a códigos fuentes de programas			☑	
A.10	**CRIPTOGRAFIA**				
A.10.1	**Controles Criptográficos**				
A.10.1.1	Política sobre el uso de los controles criptográficos	☑			
A.10.1.2	Gestión de llaves		☑		
A.11	**SEGURIDAD FISICA Y DEL ENTORNO**				
A.11.1	Áreas seguras				
A.11.1.1	Perímetro de seguridad física	☑			
A.11.1.2	Controles de acceso físicos	☑			
A.11.1.3	Seguridad de oficinas recintos e instalaciones	☑			
A.11.1.4	Protección contra amenazas externas y ambientales	☑			
A.11.1.5	Trabajo en las áreas seguras	☑			
A.11.1.6	Áreas de despacho y carga				☑
A.11.2	**Equipos**				
A.11.2.1	Ubicación y protección de equipos	☑			
A.11.2.2	Servicios de suministro	☑			
A.11.2.3	Seguridad del cableado		☑		
A.11.2.4	Mantenimiento de equipos	☑			
A.11.2.5	Retiro de activos		☑		

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones			☑	
A.11.2.7	Disposición seguro reutilización de equipos		☑		
A.11.2.8	Equipos de usuario desatentado		☑		
A.11.2.9	Política de escritorio limpio y pantalla limpia		☑		
A.12	**SEGURIDAD DE LAS OPERACIONES**				
A.12.1	Procedimientos operaciones y responsabilidades				
A.12.1.1	Procedimientos de operación documentados		☑		
A.12.1.2	Gestión de cambios	☑			
A.12.1.3	Gestión de la capacidad		☑		
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		☑		
A.12.2	**Protección contra código maliciosos**				
A.12.2.1	controles contra códigos maliciosos	☑			
A.12.3	**copias de Respaldo**				
A.12.3.1	Respaldo de información	☑			
A.12.4	**Registro y seguimiento**				
A.12.4.1	Registro de eventos		☑		
A.12.4.2	Protección de la información de registro		☑		
A.12.4.3	Registros del administrador y del operador	☑			
A.12.4.4	Sincronización de relojes	☑			
A.12.5	**Control de software operacional**				
A.12.5.1	Instalación de software en sistemas operativos	☑			
A.12.6	**Gestión de la vulnerabilidad técnica**				
A.12.6.1	Gestión de las vulnerabilidades técnicas	☑			
A.12.6.2	Restricciones sobre la Instalación de software		☑		
A.12.7	**Consideraciones sobre auditorias de sistemas de información**				
A.12.7.1	controles de auditorías de sistemas de información	☑			
A.13	**SEGURIDAD DE LAS COMUNICACIONES**				
A.13.1	**Gestión de la seguridad de las redes**				
A.13.1.1	Controles de redes	☑			
A.13.1.2	Seguridad de los servicios de red	☑			
A.13.1.3	Separación en las redes	☑			
A.13.2	**Transferencia de la información**				
A.13.2.1	Políticas y procedimientos de transferencia de información	☑			
A.13.2.2	Acuerdos sobre transferencia de información		☑		
A.13.2.3	Mensajería electrónica	☑			

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	☑			
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	☑			
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	☑			
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	☑			
A.14.2	**Seguridad en los procesos de desarrollo y soporte**				
A.14.2.1	Política de desarrollo seguro	☑			
A.14.2.2	Procedimiento de control de cambio de Sistemas		☑		
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de la operación		☑		
A.14.2.4	Restricciones en los cambios a los paquetes de software	☑			
A.14.2.5	principios de construcción de los sistemas seguros			☑	
A.14.2.6	Ambiente de desarrollo seguro				☑
A.14.2.7	Desarrollo contratado externamente		☑		
A.14.2.8	Pruebas de seguridad de sistemas			☑	
A.14.2.9	Pruebas de aceptación de sistemas			☑	
A.14.3	Datos de Prueba				
A.14.3.1	Protección de datos de prueba			☑	
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		☑		
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		☑		
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		☑		
A.15.2	**Gestión de la prestación de servicios de proveedores**				
A.15.2.1	Seguimiento y revisión de los servicios de los		☑		

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
	proveedores				
A.15.2.2	Gestión de cambios en los servicios de los proveedores		☑		
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		☑		
A.16.1.2	Reporte de eventos de seguridad de la información		☑		
A.16.1.3	Reporte de debilidades de seguridad de la información		☑		
A.16.1.4	Evaluación de los eventos de seguridad de la información y decisiones sobre ellos		☑		
A.16.1.5	Respuesta a incidentes de seguridad de la información		☑		
A.16.1.6	Aprendizaje obtenido de los incidentes de SI		☑		
A.16.1.7	Recolección de evidencia		☑		
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			☑	
A.17.1.2	Implementación de la continuidad de la SI			☑	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la SI			☑	
A.17.2	Redundancias			☑	
A.17.2.1	Disponibilidad de las Instalaciones de procesamiento de la información			☑	
A.18	**CUMPLIMIENTO**				
A.18.1	Cumplimiento de los requisitos legales y contractuales				
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	☑			
A.18.1.2	Derechos de propiedad intelectual		☑		
A.18.1.3	Protección de registros		☑		
A.18.1.4	Privacidad y protección de información de datos personales	☑			
A.18.1.5	Reglamentación de controles criptográficos				☑
A.18.2	Revisiones de seguridad de la información				
A.18.2.1	Revisiones independientes de la seguridad de la información		☑		

Objetivos de Control y Controles de Referencia		CS	CP	NC	NA
A.18.2.2	cumplimiento de las políticas y normas de seguridad		☑		
A.18.2.3	Revisión del cumplimento técnico		☑		

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 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 00 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 las mismas al interior de la Entidad ultima sensibilización proyectada el día 04 mayo de 2020.

Las Resolución 1205 2021 fue aprobada por parte de la ministra doctora Mabel Torres el día 16 de junio de 2021. Se fecho por parte de la Secretaria General, 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 de 2020.

Para los planes de acción estos se apoyan desde la Alta Dirección a través de las iniciativas que se establecen en el plan de acción Institucional PAI, se incluyen en la gestión de seguridad y la privacidad de la información; y se puede consultar en https://minciencias.gov.co/quienes_somos/planeacion_y_gestion/seguridad-informacion
Y de este link 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. 50%

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 Sistema 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; 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.

De igual manera no se ha oficializado y/o normalizado el documento relacionado con contacto con las autoridades (Procedimiento de incidentes) ni el documento gestión de proyectos. A la fecha no se manejan formalmente los proyectos 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%

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 a las políticas establecidas por la Entidad también se lleva a cabo de forma parcial sobre empleados y contratistas.
Se evidencia la existencia de requisitos exigibles de seguridad de la información en contratos laborales de fecha 2020 y escenarios de ingreso de nuevos funcionarios.
Dichas exigencias se deben plasmar en los términos y condiciones del empleado durante y a la terminación de su relación laboral con la Entidad en concordancia con lo establecido en la ISO/IEC 27001:2013.

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

Falta comunicación con Logística para la terminación de cambio de responsabilidades del empleo

A.8 Gestión de activos. 50%

Se cuenta con un Manual De Inventario de Activos, Clasificación y Publicación de la Información 2020-11-04, donde menciona en el punto 10. PUBLICACIÓN DE LOS ACTIVOS DE INFORMACIÓN; *El inventario y valoración de activos de información es un documento clasificado, custodiado por el responsable de seguridad de la información de la Oficina de Tecnologías y Sistemas de Información*. Sin embargo, el reporte presentado de la herramienta WEB SAFI de Gestión de Administración de Bienes y servicios no se evidencio alineado toda vez que no se logra identificar un Id que clasifique el criterio entre las dos bases de

datos, equipos que no están relacionadas y no esta actualizada la información con la placa de inventario

La Entidad llevo a cabo un inventario de activos de información en el año 2020 razón por la cual existe un criterio de riesgo de desactualización de los mismos.

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 no contempla la revisión del área de tecnología)

A.9 Control de accesos. 80%

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 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 no se pudo evidenciar.

A.10 Criptografía 50%

Con la criptografía se busca asegurar el uso apropiado y eficaz de esta para proteger ENTRE OTRAS, la 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 las llaves 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.

A.11 Seguridad física y del entorno. **80%**

Se observa que la entidad ha tomado medidas para controlar el acceso físico no autorizado, el daño y la interferencia a la información.

Se hace énfasis en que la responsabilidad de gestión del acceso físico a recintos e instalaciones se encuentra compartida entre Gestión de Tecnologías de Información y Gestión de Administración de Bienes y Servicios, razón por la cual no se evidencia la implementación de un procedimiento general conjunto, puesto que a pesar de que existe no incluye todos los aspectos de la operación.

A.12 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 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

A.13 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.14 Adquisición de sistemas, desarrollo y mantenimiento. 50%

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.

Se evidenció durante el proceso de entrevistas, que la implementación de un Sistema de Gestión Electrónica de Documentos de Archivos SGDEA, nace en la vigencia 2021 como una iniciativa estratégica, asociada al programa estratégico por una gestión administrativa y financiera moderna e innovadora.

La fase I, la cual es la que está contemplada para esta vigencia, se desarrolla, mediante el contrato 401 de 2021, suscrito con el Archivo General de la Nación cuyo objeto corresponde a: "Elaboración del diagnóstico institucional de archivo del Ministerio de Ciencia, Tecnología e Innovación, lo cual servirá de insumo para el mejoramiento de la infraestructura tecnológica de la entidad en cuanto a la creación, uso y administración de documentos y expedientes electrónicos" cuyos entregables corresponden a:

- Entregable No.1. Diagnóstico institucional del Ministerio de Ciencia Tecnología e Innovación, de los componentes: i) tecnológico (software y hardware) Arquitectura empresarial, ii) documental (documentos y expedientes electrónicos) iii) componente de conservación

- Entregable No.2. Informe de condiciones ambientales del Archivo de gestión centralizado ubicado en las instalaciones del Ministerio de Ciencia, Tecnología e Innovación

Es necesario considerar que los desarrollos de sistemas de información no están contemplados 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.

Dicho escenario genera un criterio de riesgo en la implementación de controles y por ende en las labores de seguimiento al mencionado proyecto, puesto que no existen procedimientos documentados ni la información pertinente disponible que permitan el adecuado seguimiento en el contexto del sistema integrado de seguridad de la Información.

A.15 Relación con proveedores. **60%**

En la Entidad la relación con los proveedores se establece contractualmente. Dichos contratos incluyen acuerdos de confidencialidad.

Estos 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.

A.16 Gestión de los incidentes de seguridad. 60%

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), quien informa 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.

Gestión Contractual

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

A.17 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 la matriz BIA.

A.18 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	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

Objeto	Valor estimado	Rubro	No. Contrato
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
OFERTA 371-2021. VENCE: 30-06-2021. REALIZAR LA RENOVACIÓN DE LA SUSCRIPCIÓN ANTE LACNIC POR EL DIRECCIONAMIENTO PÚBLICO IPV4 E IPV6 DEL MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN - MINCIENCIAS	$3.200.000	Adquisición de Bienes y Servicios	371-2021
OFERTA 381-2021. VENCE: 30-07-2021. REALIZAR LA RENOVACIÓN TECNOLÓGICA DEL SERVIDOR DE ADMINISTRACIÓN PARA LA SOLUCIÓN DE SEGURIDAD CHECKPOINT DEL MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN - MINCIENCIAS.…	$34.600.000	Adquisición de Bienes y Servicios	381-2021.
Renovación del licenciamiento de Tenable Security Center Continuos View y Adquisición del licenciamiento de Tenable Web Application para el Ministerio de Ciencia Tecnología e Innovación	$ 57.000.000	Adquisición de Bienes y Servicios	855-2020

Y se tiene los siguientes procesos contractuales 2021 previstos asociados al SGSI.

Objeto	Valor estimado	Rubro - Códigos UNSPSC
Contratar una solución en la nube como contingencia de las soluciones misionales de TI y adquirir una solución que permita realizar de manera sistemática los planes de contingencia del Ministerio de Ciencia, Tecnología e Innovación	95.200.000	43233701; 43232804; 81112210, 43232300
Renovación del licenciamiento de Tenable Security Center Continuos View y licenciamiento de Tenable Web Application para el Ministerio de Ciencia Tecnología e Innovación (Una herramienta que permita proporcionar detección de vulnerabilidades completa y precisa, hasta los componentes vulnerables de las aplicaciones web. Obteniendo visibilidad completa de las vulnerabilidades de los activos TI, de la nube y de las aplicaciones web en una única plataforma)	$74.000.000	81111800; 81111808; 43222500; 43233200; 32151800
Renovar los certificados SSL para dominios y subdominios del Ministerio de Ciencia, Tecnología e Innovación - Minciencias.	$60.000.000	81111801
Adquirir y renovar las licencias de las diferentes herramientas de apoyo informático y de servidores, así como de las soluciones de copias de respaldo Desktop and Laptop Option -DLO , Backup Exec de Veritas y soporte especializado, para el Ministerio de Ciencia, Tecnología e Innovación - Minciencias.	$417.288.000	43231500 43232100 43232300 43232600
Adquirir una solución Proxy web en la nube, que incluya los servicios de soporte especializado para el Ministerio de Ciencia, Tecnología e Innovación - Minciencias.	$190.000.000	43222503 43233205
Realizar la renovación del registro ante LACNIC por el direccionamiento público IPv4 e IPv6 del Ministerio de	$5.000.000	43231511, 81111820, 81111509, 81112201

Objeto	Valor estimado	Rubro - Códigos UNSPSC
Ciencia, Tecnología e Innovación - Minciencias		
Renovación del licenciamiento de las soluciones de seguridad para servidores, redes y usuario final - Trendmicro y LUMU para el Ministerio de Ciencia Tecnología e Innovación - Minciencias.	$350.0000	43232800, 43232900
Realizar la renovación del appliance administrador de toda la solución de seguridad Checkpoint, con el fin de incrementar su memoria RAM, para el Ministerio de Ciencia, Tecnología e Innovación – Minciencias.	$34.700.000	81112200 81111800 43233200 43222500

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:

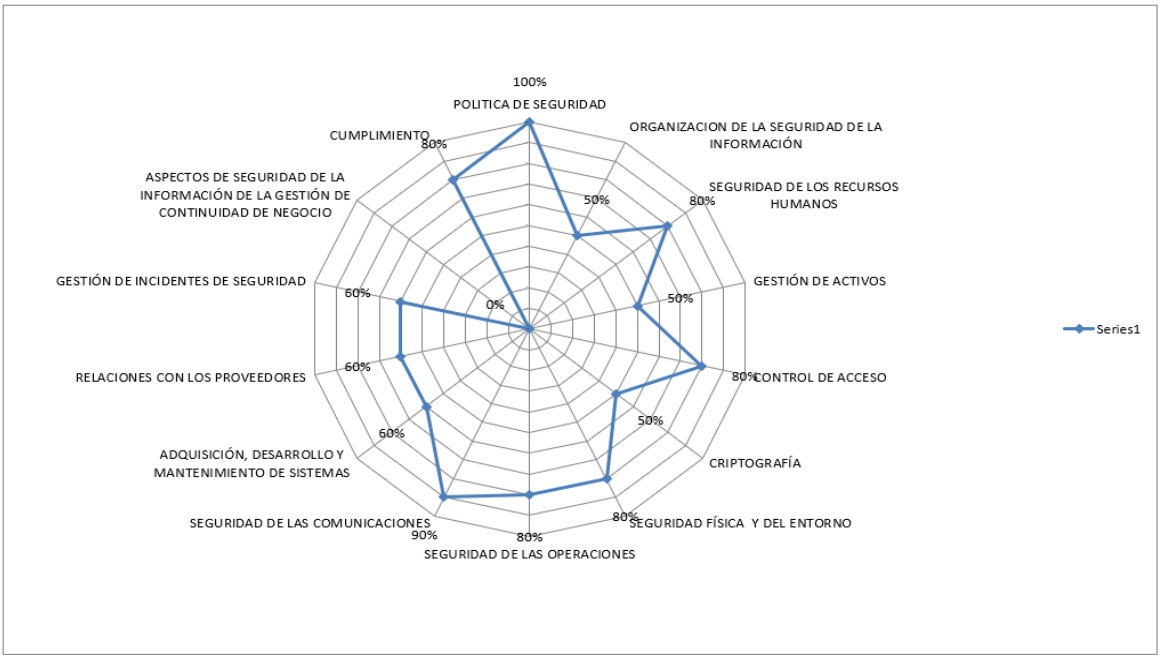
El conocimiento es de todos Minciencias	ANÁLISIS GAP - RESULTADOS POR DOMINIO NORMA ISO 27001:2013

Item	Dominios	Cumplimiento
5	POLITICA DE SEGURIDAD	100%
6	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN	50%
7	SEGURIDAD DE LOS RECURSOS HUMANOS	80%
8	GESTIÓN DE ACTIVOS	50%
9	CONTROL DE ACCESO	80%
10	CRIPTOGRAFÍA	50%
11	SEGURIDAD FÍSICA Y DEL ENTORNO	80%
12	SEGURIDAD DE LAS OPERACIONES	80%
13	SEGURIDAD DE LAS COMUNICACIONES	90%
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60%
15	RELACIONES CON LOS PROVEEDORES	60%
16	GESTIÓN DE INCIDENTES DE SEGURIDAD	60%
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	0%
18	CUMPLIMIENTO	80%
TOTAL		66%

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.

DIAGRAMA DE RED POR DOMINIOS



De acuerdo con la gráfica, se observa que los dominios con mayor nivel de madurez son política de seguridad (100%), seguridad de los recursos humanos (80%), Control de acceso (80%), Seguridad física y del entorno lo cual resulta del respaldo de la Alta Dirección y de la gestión adelantada por la Oficina de Gestión de Tecnología de Información OAI 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 junio 16 de 2021 del SGSI fue del 66% 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: gestión de activos (50%), 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. Opciones de Mejora

- Realizar los planes de continuidad de negocio, análisis de impacto del negocio (planes de contingencias, sedes alternas) y planes de recuperación desastre, a través de la generación de estrategias diversas tales como sensibilizaciones, capacitaciones, ejercicios de suplencia escalonados, etc., para disminuir el nivel de impacto, en la posibilidad de materializarse un evento que pudiese afectar la operación del negocio. Así mismo verificar a intervalos regulares los controles de continuidad de la Seguridad de la Información establecidos e implementados, con el fin de asegurar que son eficaces durante situaciones adversas
- Sensibilizar a los empleados y contratistas para tomar conciencia de su responsabilidad de reportar eventos de seguridad de la información
- Realizar con más frecuencia pruebas controladas sobre dispositivos de seguridad electrónica (controles de acceso), verificando su correcto funcionamiento y el estado de sus componentes, para prevenir posibles fallas en el escenario de poder materializarse un riesgo de seguridad física y a su vez establecer los tiempos de reacción y prestación de servicios de seguridad por terceras partes.
- Realizar procedimientos para cada una de las operaciones y/o servicios del centro de cómputo como lo establece los controles 5. del Anexo A de la Norma ISO/IEC 27001:2013.

- Verificar los detectores de humedad debajo del piso, el día de la visita se evidenció agua en los ductos debajo del piso falso del centro de cómputo.

- A pesar de que se tiene instalado un sistema de detección de incendios instalado en el techo del centro de cómputo no está por debajo del piso falso, no se evidencio con qué periodicidad se le hace mantenimiento a este sistema de extinción,
- No tiene instalados extintores manuales de incendio para los gabinetes individuales del centro de cómputo

- La temperatura en el cuarto debe ser controlada todo el tiempo, se evidencio desproporción en la zona donde se evidencio humedad (Piso falso), está en los rangos entre 18º a 24º con una humedad relativa de 30% a 55%. Así mismo se recomienda instalar un sistema de filtrado de aire que proteja a los equipos contra la contaminación como por ejemplo el polvo.

  Se deben tomar precauciones contra sismos o vibraciones como se menciona en la norma ANSI/TIA/EIA

- Los Backups de la información se realizan mediante unidad robótica, con periodos establecidos estas copias (Cintas) se almacenan en un mueble en el centro de computo
  Vulnerable al riesgo de pérdida de la información, No se cuenta con un documento interno de trabajo, que describa las actividades relacionadas con la programación y el detalle de la toma de los backups que realiza la Oficina de Tecnología de la información, incumplimiento a la NTC-SIO-IEC 27001:2013

- Frente al control de acceso del centro de cómputo no se tiene identificado el cargo que custodiará las llaves de las puertas de acceso a las áreas restringidas ni al mueble de almacenamiento de la cinta
- No están claramente identificadas las rutas de evacuación y no están libres de obstáculos se evidencio cajas con elementos que deben ser retirados.

- En cuanto al personal contratista que elabora en el centro de cómputo, no se evidencio que existe la definición respectiva para cada uno de los cargos son muy generalizadas
- En lo referente a seguridad de la información del centro de cómputo:
  - No están claramente identificadas las personas autorizadas para entregar/retirar información del CPD, en cualquier medio
  - No existe un procedimiento que defina cómo se entrega/retira del CPD el medio de información
  - Se tiene un inventario de medios magnéticos
  - No existen normas sobre acceso y préstamo de medios magnéticos a personal interno y/o externo a la empresa
  - No existe un procedimiento que defina cómo se debe rotular un medio magnético

  Lo anterior incumplimiento a la NTC-SIO-IEC 27001:2013

7. Conclusiones y Recomendaciones Sobre la verificación del grado de implementación del Sistema de Seguridad de la información (SGSI) de la CNSC en el marco de los requisitos definidos en la NTC-ISO- IEC 207001:2013 y Centro de Computo (CDP)

- Presentar resultados del grado de avance en la implementación del SIGSI al comité comité de Gestión de desempeño Institucional y Sectorial, con el fin de contar con

información sobre la gestión adelantada, de modo que la Alta Dirección pueda tomar acciones sobre la mejora continua.

- 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 alta Dirección 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.
- 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 copias de respaldo de información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con las políticas de copias de respaldo acordadas, incluyendo: Requisitos de retención y protección, así como, mejorar la herramienta con que se hace el backup adquiriendo una de mayor capacidad de modo que se dé adecuado cumplimiento con lo establecido en el numeral 8.11.3 Copias de Seguridad de la Información del Manual de Políticas de Seguridad de la Información 1 que menciona: “Seguridad del almacenamiento de backup… Los controles aplicados a los medios del sitio principal deben ser extendidos al sitio de respaldo externo…” (Subrayado fuera del texto).

- 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.
- Revisar y dar adecuado cumplimiento a las siguientes directrices de control de cambio en sistemas: a) llevar un registro de los niveles de autorización acordados; b) asegurar que los cambios se presenten a los usuarios autorizados; c) revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios; d) identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección; e) identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas; f) obtener aprobación formal para propuestas detalladas antes de que el trabajo comience; g) revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios; h) asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se lleva al archivo permanente, o se dispone de ella; i) mantener un control de versiones para todas las actualizaciones de software; j) mantener un rastro de auditoría de todas las solicitudes de cambio; k) asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados; l) asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados y contratados externamente: a) definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado. Lo anterior en razón a que en el procedimiento de desarrollo de software que se encuentra siendo objeto de revisión, no se cuenta con lo enunciado.
- Revisar las siguientes directrices: revisión técnica de las aplicaciones después de cambios en la plataforma de operación: a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones; b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación; c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio. Lo anterior en razón a que el procedimiento gestión de cambios P-TI-005 no cuenta con directrices a lo enunciado, ni con evidencias de su correcta implementación y en la entidad 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 no 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 funcionamiento.
- 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.

8. FORTALEZAS

El apoyo y disposición brindados por la Jefe de Tecnología de la información junto con su equipo de trabajo, así como la entrega 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
.

El crecimiento de la infraestructura establecidos para el 2020 y 2021 asociado al SGSI (Adquirir una solución Proxy web en la nube, que incluya los servicios de soporte especializado para el Ministerio de Ciencia, Tecnología e Innovación – Minciencias, Red de Datos, solución de Hiperconvergencia y solución de almacenamiento digital. con el fin de mejorar la calidad, seguridad y rendimiento de la operación tecnológica.

9. PLAN DE MEJORAMIENTO

Como mecanismo de control y con base en las opciones de mejora encontrados, la Oficina de Tecnología de la Información, deberá elaborar un plan de mejoramiento interno, tendiente a corregir y subsanar los puntos susceptibles de mejora, el cual será dado a conocer a la Oficina de Control Interno después de la entrega final del informe

Luz Marlenny Cano Romero

Firma del Auditor: Luz Marlenny Cano R.

_____

NOMBRE Y FIRMA DEL JEFE DE CONTROL INTERNO