

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 1 de 32

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 2 de 32

Tabla de Contenido

INTRODUCCIÓN.....	3
1. OBJETIVO	4
1.1 OBJETIVOS ESPECÍFICOS	4
2. ALCANCE	4
3. PROCESO DE REFERENCIA	5
4. DEFINICIONES	5
5. MARCO LEGAL	6
6. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	9
6.1 DIAGNÓSTICO - Contexto de la organización.....	9
6.2 PLANEACIÓN.....	11
6.3 IMPLEMENTACIÓN - Operación.....	11
6.4 EVALUACIÓN DEL DESEMPEÑO	12
6.5 MEJORA CONTINUA.....	13
7. ESTADO OBJETO DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.	13
8. ESTRATEGIA DE SEGURIDAD DIGITAL.....	16
8.1 ESTRATEGIA DE SEGURIDAD DIGITAL	17
9. PROYECTOS.....	17
BIBLIOGRAFÍA.....	31

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 3 de 32

INTRODUCCIÓN

El Plan Estratégico de Seguridad y Privacidad de la Información del Ministerio de Ciencia, Tecnología e Innovación, se elaboró con la recopilación de documentos de seguridad y privacidad de la información de la Política de Gobierno Digital, mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información – MSPI de la Política de Gobierno Digital, donde se define políticas y procedimientos eficaces y coherentes con la estrategia del Ministerio, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, con el fin de asegurar la eficacia de los controles; apoyado en los programas de auditoría y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la mejora continua del Modelo

El Ministerio adopta una metodología para la identificación y valoración de los activos de información, y una metodología para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto para la entidad y las partes interesadas.

Bajo esta perspectiva, con el fin de lograr una correcta implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información, instituye el Plan Estratégico de Seguridad y Privacidad de la Información, documento en el cual establecen los aspectos a tener en cuenta para el establecimiento de un sistema que cumple con los mejores estándares a nivel nacional e internacional. Para lo anterior, se realiza un análisis de la situación actual y deseada, así mismo se plantean las herramientas y diferentes aspectos como proyectos y actividades que se requieren llevar a cabo por parte Ministerio, para lograr un nivel adecuado para la protección de la confidencialidad, integridad y disponibilidad de su información, principios fundamentales que constituyen el pilar de la protección de los activos de la información

En resumen, el plan estratégico de seguridad de la información es fundamental para proteger los activos de información del Ministerio, garantizar el cumplimiento normativo, mitigar riesgos, y mantener la confianza y la continuidad del negocio.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 4 de 32

1. OBJETIVO

Adoptar e implementar los lineamientos del Modelo de Seguridad y Privacidad de la Información y la Estrategia de seguridad digital conforme a lo establecido por el Gobierno Nacional con el fin de fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del Ministerio y el tratamiento de sus riesgos.

1.1 OBJETIVOS ESPECÍFICOS

1. Definir y comunicar la Estrategia de seguridad de la información y seguridad digital.
2. Definir y establecer las necesidades del Ministerio para la implementación del Sistema de Gestión de Seguridad de la Información y seguridad digital.
3. Incrementar el nivel de madurez en la gestión de la seguridad de la información y seguridad digital.
4. Priorizar los proyectos a implementar para la correcta implementación del Sistema de Gestión de Seguridad de la Información - SGSI y seguridad digital.
5. Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información y seguridad digital.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información define iniciativas y proyectos orientados a la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, y comprende el alcance definido en el Manual de políticas de Seguridad de la Información, en el cual se indica que el Ministerio de Ciencia Tecnología e Innovación adopta, establece, implementa, opera, verifica y mejora el Sistema de Gestión de Seguridad de la Información (SGSI) para todos sus procesos: estratégicos, misionales, de apoyo y de control”, conforme con su misión y visión aplicables a todos los requisitos de la NTC/ISO 27001 y todos los controles del Anexo A, sin excepción alguna.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 5 de 32

3. PROCESO DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Manual de políticas de seguridad de la Información D103M01
- Manual de política de continuidad D103M07
- Resolución 500 de 2021
- ISO/IEC 27001

4. DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Modelo de Seguridad y Privacidad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 6 de 32

SGSI: Sistema de gestión de seguridad de la información

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. MARCO LEGAL

Decreto 612 de 2018 “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

Resolución 500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.

Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.

Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas.

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 7 de 32

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la agencia Nacional de espectro y se dictan otras disposiciones.

Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.

Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 0884 de 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 8 de 32

Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.

Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.

Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Directiva 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 9 de 32

ISO 22301: Norma desarrollada por ISO que especifica los requisitos para un sistema de gestión encargado de proteger a una empresa de incidentes que provoquen una interrupción en la actividad, reducir la probabilidad de que se produzcan y garantizar la recuperación de la empresa.

ISO 27001: establece los requisitos para una gestión eficaz de los riesgos que pueden afectar a la confidencialidad, la integridad y la disponibilidad de la información.

6. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El sistema de gestión de seguridad de la información (SGSI) y el presente Plan Estratégico de Seguridad de la Información (PESI), se integran y contribuyen a la consecución del Plan Estratégico Institucional y de los elementos que la componen de la siguiente manera:

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital contempla el siguiente ciclo de operación que contiene cinco (5) fases de acuerdo con la norma ISO 27001:2013, las cuales permiten al Ministerio de Ciencia Tecnología e Innovación, gestionar de forma adecuada la seguridad y privacidad de sus activos de información.

6.1 DIAGNÓSTICO - Contexto de la organización

Se realizó un análisis de las cuestiones externas e internas de la institución y su contexto, con el propósito de incluir los requisitos y expectativas de las partes interesadas del Ministerio en el alcance del Sistema de Gestión de Seguridad de la Información SGSI. Se llevó a cabo una revisión de los activos de información, para determinar si un activo de información continua o no siendo parte del inventario, adicionalmente se verificó si los valores de evaluación asignados en el inventario y clasificación de activos de información deben ser modificados, de los cuales a la fecha no se ha generado cambio en su clasificación. Una vez identificados los activos de información para el Ministerio se realizó la actualización de la matriz de inventarios de activos de tecnologías de información (código D103M02F01). Para identificar el nivel de madurez que tiene el Ministerio con respecto a la seguridad y privacidad de la información, se utiliza la herramienta "Instrumento de Evaluación MSPI de MINTIC", obteniendo en la vigencia 2024 el siguiente resultado:

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 10 de 32

Imagen No. 1



Fuente: Elaboración propia de la OTSI, adaptado del instrumento MSPI de MINTIC

En la tabla que se presenta a continuación, se registran los resultados de la efectividad de los controles:

**Tabla No. 1
Resultados efectividad de controles**

No.	Evaluación Efectividad de Controles			
	Dominio	Calificación actual	Calificación Objetivo	Evaluación Efectividad del Control
A.5	Política de Seguridad de la Información	100	100	OPTIMIZADO
A.6	Organización de la Seguridad de la Información	78	100	GESTIONADO
A.7	Seguridad de los Recursos Humanos	82	100	OPTIMIZADO
A.8	Gestión de Activos	64	100	GESTIONADO
A.9	Control de Acceso	78	100	GESTIONADO
A.10	Criptografía	50	100	EFFECTIVO
A.11	Seguridad física y del entorno	75	100	GESTIONADO
A.12	Seguridad de las operaciones	84	100	OPTIMIZADO
A.13	Seguridad de las comunicaciones	81	100	OPTIMIZADO
A.14	Adquisición, Desarrollo y Mantenimiento de Sistemas	64	100	GESTIONADO
A.15	Relaciones con los proveedores	70	100	GESTIONADO
A.16	Gestión de incidentes de Seguridad de la Información	69	100	GESTIONADO
A.17	Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio	50	100	EFFECTIVO
A.18	Cumplimiento	79	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		73	100	GESTIONADO

Fuente: Elaboración propia de la OTSI, adaptado del instrumento MSPI de MINTIC

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 11 de 32

Según la información reflejada en la tabla anterior, el Ministerio tiene un promedio de evaluación de controles de 73%, es decir los procesos y los controles se documentan y se comunican. Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente. Lo cual hace necesario para la vigencia 2024, generar un plan de trabajo con el fin de alcanzar el 100% de implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio.

6.2 PLANEACIÓN

Se establecieron las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, en el documento Manual de roles y responsabilidades del Sistema de Gestión de Seguridad de la Información SGSI (Código: D103M07). Adicionalmente, se establecieron los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento y entendiendo la importancia de una adecuada gestión de la información, el Ministerio se comprometió con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión, generando así los lineamientos para la protección de la información buscando la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados, plasmándolo en el documento Manual de Políticas de Seguridad y Privacidad de la Información (Código: D103M01).

6.3 IMPLEMENTACIÓN - Operación

Se indica que el Ministerio debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información, por tal razón se establecieron unos riesgos de seguridad de la información para el Ministerio, a los cuales se realizó para la vigencia 2024 un seguimiento trimestral

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 12 de 32

y publicado en la página web (https://minciencias.gov.co/quienes_somos/planeacion_y_gestion/tratamiento)

Se realizó seguimiento al manual de políticas de seguridad a través de la Declaración de Aplicabilidad - controles del anexo A de la norma ISO 27001:2013 (114 controles), la cual se aprobó en el Comité de Gestión y Desempeño Sectorial e Institucional – CGDSI. Esta declaración de los controles aplicables para la operación del Sistema de Gestión de Seguridad de la Información del Ministerio, será revisada en conjunto con los resultados de cada nuevo proceso de valoración de riesgos y/o ante cambios significativos de los elementos de la plataforma tecnológica y/o de personal. Se incluyó en el Sistema de Gestión de Calidad - SGC como documento técnico Declaración de aplicabilidad para la seguridad de la Información (Código D103DT03).

6.4 EVALUACIÓN DEL DESEMPEÑO

Se definen los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información. En la vigencia 2023 se realizó una auditoría al Modelo de Seguridad y Privacidad de la Información, con el propósito de evaluar el cumplimiento de los requisitos de la Norma ISO/IEC 27001:2013, verificando el cumplimiento de las disposiciones establecidas en el Modelo de Seguridad y Privacidad de Información de la Política de Gobierno Digital, obteniendo como resultado:

- ✓ (03) fortalezas
- ✓ (00) observaciones
- ✓ (00) no conformidades
- ✓ (09) Oportunidades de mejora

Para las nueve (09) oportunidades de mejora, se realiza seguimiento al plan de mejora generado:

- Generar lineamientos para el plan de continuidad de negocio TI que busca que los servicios brindados por el Ministerio continúen presentándose de manera continua y en caso de que exista alguna interrupción o falla ésta sea restablecida en el menor tiempo posible
- Realizar simulacro a los activos críticos del Ministerio de manera que se verifique y evalúe los controles de continuidad, con el fin de garantizar la continuidad de las operaciones y servicios que provee la Entidad.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 13 de 32

- Documentar un estándar para evaluar el desempeño del Data Center, en el cual se describen los componentes redundantes como un diferenciador clave, con rutas de distribución redundantes para atender al entorno crítico.
- Realizar un simulacro al Data Center para cumplir con la disponibilidad de los servicios y sistemas críticos del Ministerio que pudieran verse afectados o comprometidos por un evento o incidente de alto impacto.
- Establecer controles criptográficos y gestión de claves para determinar patrones o comportamientos similares o reincidencia
- Documentar un estándar para evaluar el desempeño del Data Center, donde se referencie la infraestructura necesaria para las operaciones del Data Center y alinear las inversiones de infraestructura con los objetivos del Ministerio
- Realizar un simulacro al Data Center para la protección de los equipos y la información, con el fin de asegurar el funcionamiento y efectividad de los controles.
- Documentar un estándar para evaluar el desempeño del Data Center, donde se referencie la infraestructura necesaria para las operaciones del Data Center y alinear las inversiones de infraestructura con los objetivos del Ministerio
- Realizar el seguimiento a la ejecución de las contrataciones propuestas, de conformidad con la dinámica de las necesidades de la Oficina de Tecnologías y Sistemas de Información

6.5 MEJORA CONTINUA

Se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las No Conformidades que ocurran, el Ministerio debe establecer las acciones más efectivas para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

7. ESTADO OBJETO DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Tabla No. 2

Situación actual y objeto de Seguridad de la Información

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 14 de 32

TEMÁTICA	SITUACIÓN ACTUAL	SITUACIÓN OBJETO
Mantenimiento del Sistema de Gestión de Seguridad de la Información – SGSI	El SGSI se encuentra documentado de acuerdo con los lineamientos de la norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información de MinTIC.	Realizar la transición a los lineamientos de la norma ISO 27001
Manual de políticas de seguridad de la Información	Se encuentra aprobado y publicado el manual de políticas de Seguridad y Privacidad de la Información	Mantener actualizado el Manual de políticas de Seguridad y Privacidad de la Información de acuerdo con la transición a la norma ISO 27001
Riesgos de Seguridad de la Información	Se tiene implementada una metodología de riesgos de gestión y se realiza el tratamiento de riesgos de seguridad de la información	Realizar gestión de riesgos conforme a los lineamientos de la norma ISO 27001
Seguridad Perimetral Lógica	Se realiza detección y visibilidad de análisis de vulnerabilidades interno y externo contra amenazas persistentes	Implementar y monitorear constantemente al Sistema de Gestión de Eventos y Seguridad de la Información que permita analizar eventos extraños en la entidad y actuar oportunamente ante posibles incidentes. Sistema de protección y monitoreo contra ataques cibernéticos y amenazas internas para los datos críticos alojados en las bases de datos debidamente parametrizado. Realizar pruebas de Ethical Hacking anualmente para análisis de vulnerabilidades del Ministerio
Seguridad Perimetral Física	El Ministerio cuenta con acceso a través de tarjeta de proximidad y accesos por huella, además de un sistema CCTV (Circuito Cerrado de Televisión) que cubre varias áreas del Ministerio, sin embargo, no existen los planos de áreas seguras y muchos controles físicos no están debidamente justificados en su ubicación.	Identificar y documentar las áreas seguras plenamente identificadas y documentadas que cuenten con un Sistema de CCTV con cobertura para las mismas.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 15 de 32

Transferencia Segura de Información	El Ministerio cuenta con una guía de transferencia de la información	Establecer lineamientos de información almacenada o transportada fuera del Ministerio protegida contra acceso no autorizado.
Seguridad en proyectos TI	El Ministerio en la actualidad incluye en sus proyectos de contratación, aspectos básicos como acuerdos de confidencialidad. Sin embargo, no cuenta con políticas documentadas establecidas para la relación con los proveedores conforme al SGSI.	Actualizar las políticas de relación con proveedores y gestión de proyectos conforme al SGSI alineadas con la norma ISO 27001
Continuidad de Negocio	El Ministerio cuenta con un plan de continuidad del negocio que establece la criticidad de los servicios tecnológicos y sus tiempos de recuperación. Implicando que en una eventualidad la operación y se ejecuta un plan de pruebas	Establecer planes de contingencia para restaurar la operación del negocio para los activos críticos del Ministerio Establecer Centro de cómputo alternativo con infraestructura suficiente para recuperar los servicios tecnológicos del Ministerio
Capacitación y sensibilización en Seguridad de la Información.	Se realiza concientización a la comunidad Minciencias con respecto al Sistema de Gestión de Seguridad de la Información.	Mejorar las estrategias de concientización a la comunidad de Minciencias en las política y lineamientos de seguridad de la información que permita un adecuado uso y gestión de los activos de la organización.

Fuente: elaboración propia OTSI

Para lo anterior se requiere seguir implementando los lineamientos en el Ministerio y emprender proyectos para adquirir infraestructura o las redundancias necesarias para la continuidad del negocio y seguridad de la información, renovación de servidores, fortalecimiento de controles de acceso físico y lógica del Ministerio.

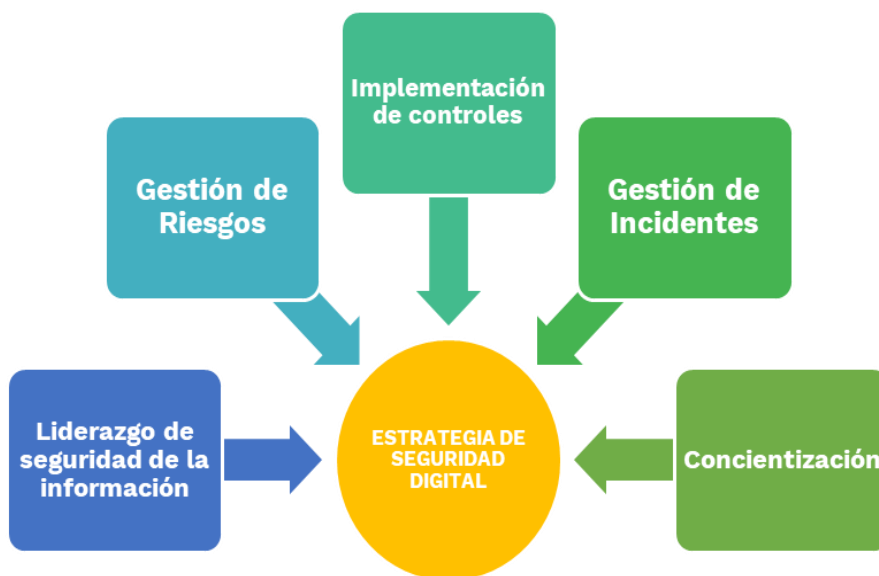
	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 16 de 32

8. ESTRATEGIA DE SEGURIDAD DIGITAL

El Ministerio establece la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía para la gestión del riesgo D102PR03G01 y del procedimiento de gestión de incidentes de seguridad de la información D103PR03.

Por tal motivo, el Ministerio define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

Imagen No. 2
Estrategias Seguridad Digital



Fuente: Ministerio de Tecnologías y Comunicaciones MinTic

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 17 de 32

8.1 ESTRATEGIA DE SEGURIDAD DIGITAL

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades con lo descrito el MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados teniendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.

Fuente: Ministerio de Tecnologías y Comunicaciones MinTic

9. PROYECTOS

Se define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 18 de 32

Proyecto No. 1: Mantenimiento y Monitoreo del Modelo de Seguridad y Privacidad de la Información	
Descripción Proyecto	Ejecutar las acciones orientadas al mantenimiento y monitoreo del Modelo de seguridad y privacidad de la información, orientadas a garantizar la disponibilidad, confidencialidad e integridad de la información, y para realizar monitoreo y acciones de mejora al cumplimiento de los lineamientos de la política de gobierno digital en la materia.
¿Para qué?	Fortalecer la gestión de seguridad y privacidad de la información del Ministerio, enmarcados en la implementación de un 100% del Modelo de Seguridad y Privacidad de la Información, basado en la identificación y valoración de los riesgos asociados, propendiendo por la protección de la confidencialidad, integridad y disponibilidad de la Información Con el fin de implementar la estrategia de seguridad digital para el Ministerio, alineado las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021
¿Por qué?	Es deber del Ministerio y con el apoyo de seguridad de la información garantizar la confiabilidad, disponibilidad e integridad de los activos de información de la Entidad, en cumplimiento del marco normativo vigente y la Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020).
¿Cómo?	Con la definición e implementación de políticas, procedimientos, directrices, normas y leyes, con el fin de asegurar la información del Ministerio, la ejecución de proyectos de adquisición y de herramientas o de implementación de normas o buenas prácticas y actividades inherentes al modelo de seguridad de la información que nos ayudará a minimizar las brechas de seguridad.
Ejes de Transformación Digital	<ul style="list-style-type: none"> • Seguridad y confianza digital • Infraestructura de datos • Transformación digital pública
Áreas funcionales beneficiarias del Proyecto.	Todas las áreas del Ministerio

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 19 de 32

Responsable	Profesionales Seguridad de la Información
Línea de tiempo del proyecto	Vigencia 2024 a 2026
Indicador	(Número total de tareas realizadas / Número total de tareas planeadas) X 100
Meta del Indicador	100% de cumplimiento del plan de trabajo para la vigencia
Entregables Asociados	Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI. Resultados del plan de ejecución de auditorías y revisiones al MSPI.
Presupuesto Estimado:	<ul style="list-style-type: none"> • Vigencia 2024: \$ 322.200.360 • Vigencia 2025: Por establecer • Vigencia 2026: Por establecer

Proyecto No. 2: Implementación de acciones para la continuidad de la seguridad de la información de infraestructura y servicios de tecnología de la información	
Descripción Proyecto	Implementación de acciones para la continuidad de la seguridad de la información, de infraestructura y servicios de tecnologías de la información
¿Para qué?	<p>Es necesario para el Ministerio de Ciencia, Tecnología e Innovación resolver las necesidades que a continuación se mencionan:</p> <p>La Entidad no cuenta con un plan de continuidad de tecnología de la información, que le permita determinar las actividades a ejecutar y los mecanismos de recuperación de los servicios de Tecnologías de la Información en eventos disruptivos (desastres, fallas de seguridad, pérdida del servicio y disponibilidad del servicio)</p> <p>La Entidad no cuenta con un sitio alterno de procesamiento de información (Datacenter Secundario) que le permita recuperar</p>

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 20 de 32

	<p>los servicios críticos de Tecnologías de la Información en caso de una falla crítica y/o un evento catastrófico.</p> <p>La Entidad contrató una consultoría en 2020 que definió la formulación y documentación del Plan de Recuperación ante Desastres - DRP, identificando los sistemas de información que deben recuperarse en el menor tiempo posible, en concordancia con el análisis de impacto del negocio BIA, sin embargo, es necesario actualizar la documentación, con el fin de garantizar la disponibilidad de la información del Ministerio en el momento en que suceda un evento.</p> <p>En año 2023 se contrató un profesional en Continuidad del Negocio, para la implementación del Sistema de gestión de la continuidad del negocio para el Ministerio, de conformidad con el modelo de seguridad y privacidad de la información (MSPI) de MINTIC, la norma ISO 22301 y lo estipulado en la Política de Gobierno Digital.</p>
<p>¿Por qué?</p>	<p>Contar con la continuidad de la seguridad de la información, de la infraestructura y servicios de tecnologías de la información, disminuye la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, la Entidad estar preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado.</p> <p>Contar con la continuidad de servicios de tecnologías de la información ayuda a la Entidad a establecer procedimientos que deben seguir en caso de un desastre o materialización de un riesgo y reconocer los servicios que como negocio tendrán que restablecerse de manera oportuna para garantizar la operación y atención a los grupos de valor. De esta forma la organización podrá reducir el impacto de un desastre o cualquier evento disruptivos y fortalecer la respuesta ante un evento de este tipo, garantizando así menores pérdidas que pudieran ser humanas, materiales y económicas</p>

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 21 de 32

	<p>La Entidad debe tener la capacidad de discernir entre sus operaciones de misión crítica y no crítica, además de saber cuánto les cuesta y cuál es el impacto en sus operaciones ante una contingencia, ya sea debido a un fenómeno natural o por causa de una falla humana.</p> <p>El Ministerio de Ciencia Tecnología e Innovación, requiere llevar a cabo el desarrollo e implementar un plan de continuidad de seguridad de la información, de la infraestructura y servicios de tecnologías de la información, que le permitan garantizar que sus servicios misionales estarán siempre disponibles para sus grupos de valor.</p>
¿Cómo?	<p>Implementar un plan de continuidad del negocio (BCP, por sus siglas en inglés Business Continuity Plan) en el Ministerio requiere una planificación y una ejecución para asegurar que las funciones críticas puedan seguir operando durante y después de una interrupción. Se requiere un paso a paso para implementar un BCP en un ministerio:</p> <ol style="list-style-type: none"> 1. Formar un Equipo de Continuidad del Negocio <ul style="list-style-type: none"> - Seleccionar un líder del proyecto: Asignar un responsable que coordine todas las actividades relacionadas con el BCP. - Incluir responsables: Asegurar la participación de representantes de todas las áreas críticas del ministerio, incluyendo TI, recursos humanos, finanzas, operaciones y seguridad. 2. Realizar un Análisis de Impacto en el Negocio (BIA) <ul style="list-style-type: none"> - Identificar procesos críticos: Determinar cuáles son las funciones y procesos esenciales para la operación del ministerio. - Evaluar el impacto: Analizar cómo las interrupciones pueden afectar estos procesos, tanto a corto como a largo plazo. - Definir prioridades: Establecer las prioridades de recuperación basadas en el impacto y la criticidad de los procesos.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 22 de 32

	<p>3. Evaluar riesgos y amenazas</p> <ul style="list-style-type: none"> - Identificar amenazas potenciales: Considerar amenazas naturales, tecnológicas, humanas y otras que puedan afectar la continuidad del negocio. - Evaluar la probabilidad y el impacto: Calificar cada amenaza en términos de probabilidad de ocurrencia e impacto en el ministerio. - Desarrollar estrategias de mitigación: Crear estrategias para reducir la probabilidad y/o el impacto de cada riesgo identificado. <p>4. Desarrollar estrategias de continuidad</p> <ul style="list-style-type: none"> - Definir estrategias de recuperación: Desarrollar planes detallados para la recuperación de cada proceso crítico, incluyendo la recuperación de datos y sistemas de TI. - Establecer sitios alternos: Identificar y preparar ubicaciones alternativas donde el ministerio pueda operar en caso de una interrupción en la ubicación principal. - Garantizar la disponibilidad de recursos: Asegurar que se disponga de los recursos necesarios (personal, tecnología, infraestructura) en las ubicaciones alternativas. <p>5. Desarrollar el plan de continuidad del negocio</p> <ul style="list-style-type: none"> - Documentar el BCP: Redactar un documento claro y comprensible que incluya todos los procedimientos y pasos necesarios
Ejes de Transformación Digital	<ul style="list-style-type: none"> • Seguridad y confianza digital • Infraestructura de datos • Transformación digital pública
Áreas funcionales beneficiarias del Proyecto.	Todas las áreas del Ministerio
Responsable	Profesionales Seguridad de la Información
Línea de tiempo del proyecto	Vigencias 2024 a 2026

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 23 de 32

Indicador	100% de cumplimiento del plan de trabajo para la vigencia
Meta del Indicador	(Número total de tareas realizadas / Número total de tareas planeadas) X 100
Entregables Asociados	<u>Vigencia 2024:</u> Plan de continuidad de los procesos críticos del Ministerio. Análisis de Impacto BIA Diagnóstico de Plan de Recuperación de Desastres de TI - DRP. <u>Vigencia 2025:</u> Actualización al Plan de Continuidad de los procesos críticos de acuerdo con el análisis de Impacto Críticos - BIA Plan de Recuperación desastres- DRP <u>Vigencia 2026:</u> Seguimiento y actualización del plan de Continuidad del Negocio y plan de Recuperación desastres
Presupuesto Estimado:	<ul style="list-style-type: none"> • Vigencia 2024: \$84.000.000 • Vigencia 2025: Por establecer • Vigencia 2026: Por establecer

Proyecto No. 3: Evaluar proyectos de TI alineado criterios de seguridad de la información

Descripción Proyecto	Garantizar la adecuada identificación de los controles aplicables en cada etapa de un proyecto TI, desde el Sistema de Gestión de Seguridad de la Información - SGSI y Continuidad del Negocio
¿Para qué?	Para proteger los activos de información críticos y de la información sensible del Ministerio contra accesos no autorizados, pérdidas y amenazas cibernéticas. Adicionalmente, promoviendo una cultura de seguridad y mejorando la resiliencia ante posibles incidentes de seguridad de la información.
¿Por qué?	Los controles aplicables de seguridad de la información en un proyecto TI, son fundamentales para proteger datos sensibles, asegurar la confianza de los usuarios, prevenir costos elevados, permitir un escalamiento seguro, proteger la propiedad

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 24 de 32

	<p>intelectual y fomentar una cultura organizacional de seguridad. Estas razones contribuyen a la viabilidad y éxito a largo plazo del proyecto TI.</p>
<p>¿Cómo?</p>	<p>Con el fin de alinear los criterios de seguridad de la Información en los proyectos de TI se requiere de una estructura y de un equipo de recurso humano para garantizar la seguridad de la información así:</p> <p>1. Planificación del Proyecto</p> <p>Identificación de Activos:</p> <ul style="list-style-type: none"> - Identificar y clasificar los activos de información. - Determinar la criticidad y sensibilidad de los datos. <p>Análisis de Riesgos:</p> <ul style="list-style-type: none"> - Realizar un análisis de riesgos específico para el proyecto. - Identificar amenazas y vulnerabilidades. - Evaluar el impacto potencial y la probabilidad de ocurrencia. <p>Definición de Controles:</p> <ul style="list-style-type: none"> - Seleccionar controles de seguridad basados en los resultados del análisis de riesgos. - Alinear los controles con las políticas y estándares del SGSI. <p>2. Desarrollo y Adquisición</p> <p>Controles de Desarrollo Seguro:</p> <ul style="list-style-type: none"> - Integrar prácticas de desarrollo seguro (por ejemplo, OWASP) en el ciclo de vida del desarrollo de software. - Realizar revisiones de código y pruebas de seguridad. <p>Controles de Adquisición:</p> <ul style="list-style-type: none"> - Evaluar la seguridad de los proveedores y sus productos. - Incluir cláusulas de seguridad en los contratos con proveedores.

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 25 de 32

	<p>3. Implementación</p> <p>Pruebas de Seguridad:</p> <p>Realizar pruebas de penetración y análisis de vulnerabilidades en el entorno de implementación.</p> <p>Implementar un MVP (Minimum Viable Product) de seguridad de la información, el cual es crucial para garantizar que la seguridad se aborde desde las primeras etapas del desarrollo del proyecto:</p> <ul style="list-style-type: none"> Detección Temprana de Vulnerabilidades Protección de Datos Cumplimiento Regulatorio Confianza y Credibilidad Reducción de Costos a Largo Plazo Ahorro de Recursos Preparación para el Crecimiento Escalabilidad Segura: Protección de la Propiedad Intelectual Salvaguarda de Activos Fomento de una Cultura de Seguridad Prevención de Incidentes Minimización de Riesgos Mejora Continua <p>Implementar un MVP de seguridad de la información protege el proyecto desde sus etapas iniciales, sino que también establece una base sólida para un desarrollo seguro y confiable a largo plazo.</p> <p>4. Gestión de Cambios:</p> <ul style="list-style-type: none"> - Establecer un proceso de gestión de cambios con evaluaciones de impacto en la seguridad.
--	--

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 26 de 32

	<ul style="list-style-type: none"> - Asegurar que los cambios se revisen y aprueben adecuadamente. <p>5. Operación y Mantenimiento</p> <p>Monitoreo y Detección:</p> <ul style="list-style-type: none"> - Implementar sistemas de monitoreo y detección de intrusos (IDS/IPS). - Configurar alertas y notificaciones de eventos de seguridad. <p>Gestión de Incidentes:</p> <ul style="list-style-type: none"> - Establecer procedimientos para la gestión y respuesta a incidentes. - Realizar simulacros y pruebas de los planes de respuesta a incidentes. <p>6. Evaluación y Auditoría</p> <p>Revisión de Controles:</p> <ul style="list-style-type: none"> - Realizar auditorías periódicas de los controles de seguridad implementados. - Revisar y actualizar los controles según sea necesario. <p>Evaluación Continua de Riesgos:</p> <ul style="list-style-type: none"> - Continuar evaluando los riesgos a medida que el proyecto evoluciona y el entorno cambia. - Ajustar los controles y las políticas en respuesta a nuevas amenazas y vulnerabilidades. <p>7. Continuidad del Negocio</p> <p>Planificación de la Continuidad del Negocio (BCP):</p> <ul style="list-style-type: none"> - Desarrollar y mantener un Plan de Continuidad del Negocio específico para el proyecto. - Incluir análisis de impacto en el negocio (BIA) para identificar procesos críticos. <p>Pruebas de BCP:</p>
--	---

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 27 de 32

	<ul style="list-style-type: none"> - Realizar pruebas regulares del plan de continuidad del negocio. - Evaluar la efectividad de los planes y hacer ajustes según los resultados de las pruebas. <p>8. Sensibilización y Concienciación</p> <p>Formación Continua:</p> <ul style="list-style-type: none"> - Proporcionar formación continua en seguridad de la información y continuidad del negocio a todos los involucrados en el proyecto. - Realizar simulacros y ejercicios de concienciación para reforzar la importancia de la seguridad. <p>Implementar este enfoque estructurado asegura que los controles de seguridad se identifiquen y apliquen adecuadamente en cada etapa del proyecto, protegido contra amenazas y vulnerabilidades, manteniendo la confidencialidad, integridad y disponibilidad de los datos, alineándose con los objetivos del SGSI y los planes de continuidad del negocio.</p>
Ejes de Transformación Digital	<ul style="list-style-type: none"> • Seguridad y confianza digital • Infraestructura de datos • Transformación digital pública
Áreas funcionales beneficiarias del Proyecto.	Todas las áreas del Ministerio
Responsable	Profesionales Seguridad de la Información
Línea de tiempo del proyecto	Vigencias 2024 a 2026
Indicador	100% de cumplimiento del plan de trabajo para la vigencia
Meta del Indicador	(Número total de tareas realizadas / Número total de tareas planeadas) X 100
Entregables Asociados	MVP (Minimum Viable Product) Políticas y procedimientos de seguridad de la información

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 28 de 32

	Personal capacitado Informes de auditoría de seguridad y análisis de riesgos
Presupuesto Estimado:	<ul style="list-style-type: none"> • 2024: \$44.100.000 • 2025: Por establecer • 2026: Por establecer

Proyecto No. 4: Implementación de (SOC) servicio monitoreo de operaciones de seguridad

Descripción Proyecto	Implementar recursos (Humano, económico, tecnológico), con el fin de proporcionar un enfoque avanzado y proactivo para la ciberseguridad, permitiendo al Ministerio identificar y mitigar amenazas que puedan generar un impacto legal, reputacional, económico, fiscal y de disponibilidad.
¿Para qué?	<p>Sistema de Operaciones de Seguridad (SOC) es beneficioso para el Ministerio en varios aspectos:</p> <p>Gestión de riesgos: Permite identificar, evaluar y gestionar los riesgos a los que se enfrenta el Ministerio. Al implementar controles internos efectivos, el SOC ayuda a mitigar estos riesgos y proteger los activos del Ministerio.</p> <p>Prevención de fraudes y errores: Prevenir y detectar fraudes internos y errores antes de que causen daños significativos. Al establecer controles adecuados sobre los procesos financieros, la gestión de activos y el acceso a la información, se reduce la probabilidad de manipulación indebida o malversación de fondos.</p> <p>Cumplimiento normativo: Contribuir en el cumplimiento de las regulaciones que aplican para seguridad de la información, ciberseguridad y continuidad del Negocio, lo que puede evitar multas, sanciones legales y daños a la reputación del Ministerio</p> <p>Mejora Continua: Optimizar los procesos, eliminar redundancias y mejorar la asignación de recursos.</p>

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 29 de 32

	<p>Confianza de grupos de valor y de interés: Un SOC bien implementado muestra que el Ministerio gestiona de manera adecuada los riesgos y la protección de los intereses de sus partes interesadas, lo que puede aumentar la confianza y la credibilidad del Ministerio.</p> <p>En resumen, un SOC es fundamental para proteger los activos, prevenir fraudes, cumplir con las regulaciones, mejorar la eficiencia operativa y mantener la confianza de grupos de valor y de interés del Ministerio</p>
¿Por qué?	Facilitar la detección temprana de amenazas antes de que causen un daño significativo en el Ministerio
¿Cómo?	<p>Las fases de implementación de un Sistema de Control Interno (SOC) en una entidad incluyen:</p> <p>1. Planificación y Evaluación: Establecer metas claras para el SOC, como la protección de activos, la prevención de fraudes, el cumplimiento normativo, etc. Asignar personal y recursos financieros para llevar a cabo la implementación del SOC de manera efectiva.</p> <p>2. Diseño y Desarrollo: Desarrollar políticas, procedimientos y controles internos adecuados para abordar los riesgos identificados durante la fase de evaluación. Implementación de tecnología, Integrar herramientas y sistemas tecnológicos que apoyen el funcionamiento del SOC, como software de gestión de riesgos o soluciones de seguridad cibernética. Capacitación del personal, proporcionar capacitación adecuada al personal sobre los nuevos procedimientos y controles implementados.</p>

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 30 de 32

	<p>3. Implementación y Ejecución:</p> <p>Puesta en marcha de controles: Implementar los controles internos diseñados durante la fase de diseño, asegurando que estén correctamente integrados en los procesos operativos de la entidad.</p> <p>Monitoreo inicial: Iniciar el monitoreo de los controles recién implementados para asegurarse de que estén funcionando según lo previsto y de que se estén abordando los riesgos de manera efectiva.</p> <p>4. Evaluación y Mejora Continua:</p> <p>Evaluación periódica: Realizar evaluaciones regulares para determinar la efectividad de los controles internos y la gestión de riesgos de seguridad de la información en la entidad.</p> <p>Identificación de áreas de mejora: Identificar áreas de mejora en el SOC y realizar ajustes según sea necesario para abordar los nuevos riesgos o cambios en el entorno operativo de la entidad.</p> <p>Mejora continua: Implementar cambios y mejoras en el SOC de manera continua para garantizar su relevancia y eficacia a lo largo del tiempo.</p> <p>5. Reporte y Cumplimiento:</p> <p>Documentación y reporte: Mantener registros detallados de las actividades del SOC y preparar informes periódicos para la dirección, los auditores y otras partes interesadas.</p> <p>Cumplimiento normativo: Asegurarse de que el SOC cumpla con todas las regulaciones y estándares aplicables a la industria de la entidad.</p>
Ejes de Transformación Digital	<ul style="list-style-type: none"> • Seguridad y confianza digital • Infraestructura de datos • Transformación digital pública

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 31 de 32

Áreas funcionales beneficiarias del Proyecto.	Todas las áreas del Ministerio
Responsable	Profesionales Seguridad de la Información
Línea de tiempo del proyecto	Vigencias 2024 a 2026
Indicador	100% de cumplimiento del plan de trabajo para la vigencia
Meta del Indicador	(Número total de tareas realizadas / Número total de tareas planeadas) X 100
Entregables Asociados	Correlacionador de eventos Administración de herramientas de seguridad del Ministerio
Presupuesto Estimado:	<ul style="list-style-type: none"> • 2024: \$204.000.000 • 2025: Por establecer • 2026: Por establecer

BIBLIOGRAFÍA

https://gobiernodigital.mintic.gov.co/692/articles-176929_recurso_1.docx

https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

<https://www.icontec.org/wp-content/uploads/2023/03/PLAN-TRANSICION-ISOIEC-27001-2013-A-VERSION-2022.pdf>

https://gobiernodigital.mintic.gov.co/692/articles-176929_recurso_1.docx

<https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/272948:Plan-Estrategico-de-Seguridad-de-la-Informacion-PESI>

	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN	Código: D103DE02
		Versión: 01
		Fecha: 14/08/2024
		Página: 32 de 32

CONTROL DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	14/08/2024	Todos	Creación de documento

Elaboró	Revisó	Aprobó
Nombre: Erika Viviana Chacón Gamba	Nombre: Leydy Paola Rojas Lizarazo Liliana Beatriz Buitrago Barreto	Nombre: Comité de Gestión y Desempeño Sectorial e Institucional en su sesión número 19 realizada el 30 de Julio de 2024
Cargo / Rol Contratista Oficina de Tecnologías y Sistemas de Información	Cargo / Rol Jefe Oficina de Tecnologías y Sistemas de Información Contratista Oficina de Tecnologías y Sistemas de Información	