PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 2.0

CORPORACIÓN AUTÓNOMA REGIONAL DEL RIO GRAN DE LA MAGDALENA
CORMAGDALENA

2025

Plan de Seguridad y Privacidad de la Información

1. INTRODUCCIÓN

La Corporación Autónoma Regional Del Rio Grande de la Magdalena de acuerdo con lo indicado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, en la resolución 500 de 2021 que indica los lineamientos a seguir para dar cumplimiento a un MSPI (Modelo de Seguridad y Privacidad de la Información) efectivo:

"ARTÍCULO 3" Lineamientos generales. Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución.

Para todos los procesos, trámites, servicios de información, infraestructura tecnológica e infraestructura critica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital.

"ARTÍCULO 4" Sistema de gestión de seguridad de la información y seguridad digital. Los sujetos obligados deben aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia.

"ARTÍCULO 5" La estrategia de seguridad digital. Los sujetos obligados deben adoptar 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 digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales.

La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital.

Adicionalmente, la estrategia de seguridad digital debe:
1. Ser aprobada a través de un acto administrativo de carácter general.
2. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.
3. Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital.
4. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces.
5. La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.
6. Aplicar las demás consideraciones que a juicio de la entidad contribuyan a elevar sus estándares de seguridad digital.

"Parágrafo 1" Los sujetos obligados deben adoptar el Modelo de Seguridad y Privacidad de la Información – MSPI señalado en el Anexo 1 de la presente resolución, como habilitador de la política de Gobierno Digital".
Dicho lo anterior, se construye un plan de trabajo de mejora continua para seguir fortaleciendo el modelo de seguridad y privacidad de CORMAGDALENA con el fin de generar confianza en el tratamiento de la información en todos los procesos de la entidad.

2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Definir las actividades previstas en el Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, en alineación con la norma NTC/IEC ISO 27001, la política pública de seguridad digital y los criterios de continuidad de la operación de los servicios, con el fin de garantizar la seguridad y privacidad de la información gestionada en los procesos de Cormagdalena.

2.1. OBEJTIVOS ESPECIFICOS.

El Plan de Seguridad y Privacidad de la Información de CORMAGDALENA se ha diseñado teniendo en cuenta las necesidades institucionales y las dimensiones de la Política de Gobierno Digital. Los objetivos específicos de este plan son los siguientes:

- Garantizar la confidencialidad, integridad y disponibilidad de la información: Asegurar que la información y los activos digitales de CORMAGDALENA estén protegidos contra accesos no autorizados,

alteraciones indebidas y asegurando su disponibilidad cuando sea requerida por los usuarios autorizados.

- Implementar controles de seguridad alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI): Desplegar políticas y controles de seguridad que estén en sintonía con las mejores prácticas nacionales e internacionales, proporcionando una cobertura integral sobre la seguridad de la información en la entidad.

- Establecer un proceso de gestión de riesgos de seguridad de la información: Crear una metodología para la identificación, evaluación, tratamiento y monitoreo de los riesgos asociados con los activos de información de la entidad, reduciendo la exposición a amenazas y vulnerabilidades.

- Desarrollar capacidades internas de respuesta ante incidentes de seguridad: Definir y aplicar procedimientos para la detección, reporte, análisis y resolución de incidentes de seguridad de la información, fortaleciendo la capacidad de respuesta y recuperación ante incidentes cibernéticos.

- Promover la concientización y formación en seguridad digital: Desarrollar programas continuos de formación para empleados, proveedores y demás actores involucrados, con el objetivo de fomentar una cultura organizacional orientada a la ciberseguridad y la privacidad de la información.

- Asegurar el cumplimiento de las normativas y estándares vigentes: Garantizar que las políticas y procedimientos implementados estén en línea con las regulaciones nacionales e internacionales relacionadas con la seguridad y privacidad de la información, como el MSPI y otras disposiciones legales aplicables.

- Optimizar la interoperabilidad y protección de la información en los sistemas de CORMAGDALENA: Implementar mecanismos que faciliten la interoperabilidad con otras entidades del Estado, al tiempo que se garantiza la seguridad y privacidad de los datos compartidos.

- Monitorear y mejorar continuamente la seguridad digital: Establecer un ciclo de revisión y mejora continua en los procesos y sistemas de seguridad de la información para adaptarse a las nuevas amenazas y mantener los niveles de protección requeridos.

Estos objetivos específicos permiten alinear las necesidades estratégicas de CORMAGDALENA con el marco de seguridad digital exigido por el Gobierno Digital, garantizando una gestión proactiva y eficiente de la seguridad y privacidad de la información.

3. ALCANCE

El propósito del presente plan es mejorar el desempeño de la seguridad digital en todos los procesos de CORMAGDALENA, aplicándolo a todos los niveles funcionales y organizacionales. Esto implica velar por la confidencialidad, integridad y disponibilidad de los servicios de información. Al concluir la ejecución de este plan, se habrá alcanzado un nivel de madurez mayor en los procesos y procedimientos relacionados con la seguridad digital.

4. DEFINICIONES

Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).
Archivo: conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
Amenazas: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
Bases de Datos Personales: conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa almacena y transporta mediante los servicios de información que se encuentran interconectados.

Ciberespacio: es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Derecho a la Intimidad: derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Ley de Habeas Data: se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: se refiere a la Ley Estatutaria 1712 de 2014.

Plan de continuidad del negocio: plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Responsable del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

Riesgo: 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. (ISO/IEC 27000).

Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Seguridad digital: preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Titulares de la información: personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (Adoptada mediante Resolución 000278 de 30 de septiembre de 2024)

Cormagdalena, a través de la adopción e implementación del Modelo de Seguridad y Privacidad de la Información en el marco del Sistema de Gestión de Seguridad de la Información, protege, preserva y gestiona la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en su mapa de procesos. Esto se logra mediante una gestión integral de riesgos y la aplicación de controles físicos y digitales que previenen incidentes y garantizan el cumplimiento de los requisitos legales y reglamentarios. Estas acciones están orientadas hacia la mejora continua y el alto desempeño del Sistema de Gestión de Seguridad de la Información, fomentando el acceso, uso efectivo y apropiación masiva de las TIC mediante políticas y programas diseñados para optimizar los procesos.

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

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digital, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013 es de:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	40	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	40	100	REPETIBLE
A.9	CONTROL DE ACCESO	40	100	REPETIBLE
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	40	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	40	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	40	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	40	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40	100	REPETIBLE
A.18	CUMPLIMIENTO	40	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		44	100	EFECTIVO

En promedio, la entidad presenta un estado real de cumplimiento del 44% en un nivel Repetible, es decir Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado

de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.

7. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Esta política es de aplicación para todos los niveles de Cormagdalena e involucra a sus funcionarios, contratistas, proveedores, operadores y cualquier tercero que, en el cumplimiento de sus funciones o en relación con las actividades de la corporación, comparta, utilice, recolecte, procese, intercambie o consulte información de la entidad. Incluye también a los Entes de Control y Entidades relacionadas que accedan, de forma interna o externa, a cualquier archivo de información, independientemente de su ubicación. Asimismo, esta política cubre toda la información creada, procesada o utilizada por Cormagdalena, sin importar el medio, formato, presentación o ubicación en la que se encuentre.

8. COMITÉ SE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Las funciones del comité de Seguridad y Privacidad de la información serán asumidas por el comité de gestión y desempeño se debe dejar constancia mediante de resolución.

9. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes

Estrategia	Gestión	Actividades	Tareas	Responsable Actividad	Fecha de Programación Actividades	
					Fecha Inicio	Fecha Final
01		Definir los lineamientos para el levantamiento del inventario de activos de información.	Actualizar, cuando sea necesario, la metodología o la documentación relacionada con la gestión del levantamiento de activos de información	Equipo de activos de la información.	03-feb-2025	30-abr-2025
		Levantamientos activos de información.	Socializar la guía de activos de Información.	Equipo de activos de la información.	01-may-2025	30-may-2025
			Validar activos de información en el instrumento levantado en la vigencia anterior	Líder o enlace de cada proceso Equipo de activos de la información.	01-jun-2025	30-jun-2025
			Identificar nuevos activos de información en cada dependencia	Líder o enlace de cada proceso Equipo de activos de la información.	01-jun-2025	30-jun-2025
			Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones	Equipo de activos de la información	01-jul-2025	31-jul-2025
			Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Líder o enlace de cada proceso	01-jul-2025	31-jul-2025
			Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo	Líder o enlace de cada proceso	30-jul-2025	31-dic-2025

		Publicación de activos de información.	Validar y aceptar los activos de información para su publicación en el Sistema Integrado de gestión por cada líder de proceso.	Líder o enlace de cada proceso Equipo de activos de la información.	01-sept-2025	30-sept-2025
			Consolidar el instrumento de activos de Información	Equipo de activos de la información	01-sept-2025	*30-sept-2025*
			Publicar los instrumentos de activos de información consolidado en el Sistema Integrado de gestión	OAP	01-sept-2025	*30-sept-2025*
		Registros de activos de información ley 171.	Actualizar el instrumento de Registro Activos de Información con el insumo de los instrumentos de activos de Información.	Equipo de activos de información.	01-oct-2025	31-oct-2025
			Enviar a control de legalidad el instrumento de Registro Activos de información.	Equipo de activos de información	01-oct-2025	31-oct-2025
			Publicación del Registro Activos de Información en el sitio web de la Entidad.	OAP	01-oct-2025	31-oct-2025
	Gestión del riesgo	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Equipo Gestión del Riesgo	01-abr-2025	30-abr-2025
		Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo Gestión del Riesgo	01-may-2025	30-may-2025
		Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo Gestión del Riesgo	01-jun-2025	31-dic-2025
			Realimentación, revisión y verificación de los riesgos identificados(Ajustes)	Equipo Gestión del Riesgo	01-jun-2025	31-dic-2025
		Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Equipo Gestión del Riesgo	01-jul-2025	30-nov-2025
		Publicación	Publicación Matriz de riesgos – Sistema Integrado de Gestión.		01-ago-2025	30-nov-2025
		Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y	Equipo Gestión del Riesgo	01-jul-2025	31-dic-2025

			verificación de evidencias			
		Evaluación de riesgos residuales	Evaluación de riesgos residuales	Equipo Gestión del Riesgo	01-jul-2025	31-dic-2025
		Mejoramiento	identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo Gestión del Riesgo	01-jul-2025	31-dic-2025
			Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo con los cambios solicitado	Equipo Gestión del Riesgo	01-jul-2025	31-dic-2025
		Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Equipo Gestión del Riesgo	01-jul-2025	31-dic-2025
	Gestión de incidentes de Seguridad de la información	Elaboración de procedimiento de gestión de incidentes de seguridad	Elaboración del procedimiento de gestión de incidentes basados en la ISO 27035	Área de sistemas	01-jun-2025	30-jun-2025
		Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Publicar el procedimiento de gestión de incidentes de Seguridad de la Información en Sistema Integrado de Gestión	Área de sistemas	01-jul-2025	31-jul-2025
			Socializar el procedimiento a los especialistas de la OTI, indicando los cambios en el procedimiento	Área de sistemas	01-jul-2025	31-jul-2025
			Socializar el procedimiento a los colabores de la Entidad.	Área de sistemas	01-jul-2025	31-jul-2025
			Socializar el procedimiento a los colabores de la Entidad.	Área de sistemas	01-jul-2025	31-jul-2025
		Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Área de sistemas	1-ago-2025	31-dic-2025
		CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Área de sistemas	01-abr-2025	31-dic-2025
		Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Área de sistemas	01-abr-2025	31-dic-2025

	Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGS	Área de Sistemas	01-may-2025	31-may-2025
			Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los gestores de procesos .	Área de Sistemas	01-may-2025	31-may-2025
	Continuidad de la Operación	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Líder o enlace de Procesos	01-jun-2025	31-dic-2025
		Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Área de Sistemas	01-jul-2025	31-dic-2025
	Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	OAJ y área de sistemas	01-jun-2025	31-dic-2025
		Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	OAJ y área de sistemas	01-jul-2025	31-dic-2025
	Plan de Continuidad del Negocio	Documentación del Análisis de Impacto de la Operación	Actualización del Análisis de Impacto del Negocio	Equipo continuidad del negocio	01-ago-2025	31-dic-2025
			Publicación del Análisis de Impacto del Negocio	Equipo continuidad del negocio	01-ago-2025	31-dic-2025
		Documentación de Valoración de Riesgos de Interrupción	Actualización del documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación	Equipo continuidad del negocio	01-ago-2025	31-dic-2025
			Publicación Valoración de Riesgos de interrupción	Equipo continuidad del negocio	01-ago-2025	31-dic-2025
		Documentación de Estrategias de Continuidad	Actualización del documento Estrategias de Continuidad de la Operación	Equipo continuidad del negocio	01-ago-2025	31-dic-2025
			Actualización del documento Estrategias de Continuidad de la Operación	Equipo continuidad del negocio	01-ago-2025	31-dic-2025
		Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	Equipo continuidad del negocio	01-ago-2025	31-dic-2025
			Aprobación del Plan de continuidad de la Operación	Equipo continuidad del negocio	01-ago-2025	31-dic-2025

	Acciones correctivas y Notas de mejoras SGSI	Reporte del estado de las Acciones Correctivas y Oportunidades de Mejora	Generar reporte del estado actual de las AC y OM en SIMIG	OAP	03-feb-2025	31-dic-2025
			Solicitar el cargue del análisis de causas o plan de tratamiento según sea requerido	OAP	03-feb-2025	31-dic-2025
		Generar observaciones o recomendaciones a los acompañamientos realizados a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	OAP	03-feb-2025	31-dic-2025
	Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Área de sistemas	03-feb-2025	30-may-2025
			informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.	Área de sistemas	02-may-2025	31-dic-2025
	Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Área de sistemas	03-feb-2025	28-feb-2025
			Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Área de sistemas	01-marz-2025	30-marz-2025
			Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Área de sistemas	01-abr-2025	30-abr-2025
			Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Área de sistemas	01-abr-2025	31-dic-2025
		CCOC	Cumplimiento requerimientos infraestructuras críticas del gobierno	Área de sistemas	03-feb-2025	31-dic-2025
	Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas en el PAA	Todos los procesos	01-nov-2025	31-dic-2025
	Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de	Área de sistemas	03-feb-2025	31-dic-2025

			Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación			
	Indicadores SGSI	Provisión de información a los indicadores de medición del SGS	Formular, Implementar y actualizar los indicadores del SGSI	Área Sistemas	01-abr-2025	30-jun-2025
			Reportar indicadores	Lideres o encargado de procesos	01-jul-2025	31-dic-2025
	Vulnerabilidades	Definir lineamientos para ejecutas las pruebas de vulnerabilidades.	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Área Sistemas	01-abr-2025	31-abr-2025
	Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Área Sistemas	01-mar-2025	31-mar-2025
		revisión de la base de datos.	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Área Sistemas -	01-abr-2025	31-dic2025
		Registro y actualización de las bases de datos.	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Área Sistemas -	01-may-2025	31-dic-2025

10. RESPONSABLES

1. Representante Legal de la Entidad: Aprobar los documentos de Alto Nivel.
2. Secretario (a) General: Velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Responsable de Seguridad Digital / CIO / Enlace TIC: Coordinar las actividades de implementación del MSPI.

11. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

Control De Cambios

Fecha	Versión	Descripción Del Cambio
23-07-2024	Versión 1	Elaboración del Plan
31-01-2025	Versión 2	Actualización del Plan por cambio de vigencia 2025.