PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1.0

CORPORACIÓN AUTÓNOMA REGIONAL DEL RIO GRAN DE LA MAGDALENA
CORMAGDALENA

2024

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

Seguir un proceso de mejora continua conforme al Modelo de Seguridad y Privacidad de la Información (https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf), alineado con la norma NTC/IEC ISO 27001.

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

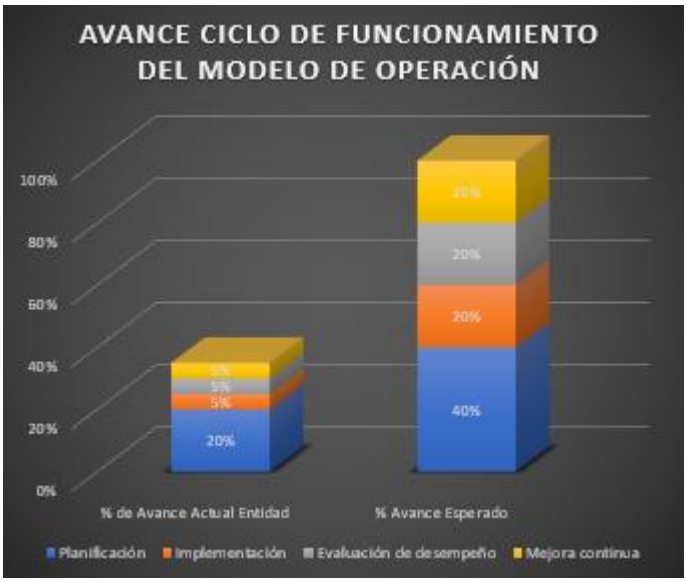
Basados en el uso del "INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD", se obtuvieron los siguientes resultados del análisis de brechas sobre la efectividad de los controles durante el seguimiento realizado en agosto de 2024.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	20	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	20	100	INICIAL
A.9	CONTROL DE ACCESO	20	100	INICIAL
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	20	100	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	20	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	20	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	20	100	INICIAL
	PROMEDIO EVALUACIÓN DE CONTROLES	**20**	**100**	INICIAL

En promedio, la entidad presenta un estado real de cumplimiento del 20 en un nivel Inicial, es decir, ha identificado la necesidad de implementar acciones y se evidencia una planeación para tratar dicha necesidad

En cuanto al análisis de brecha para el avance del PHVA se tiene:

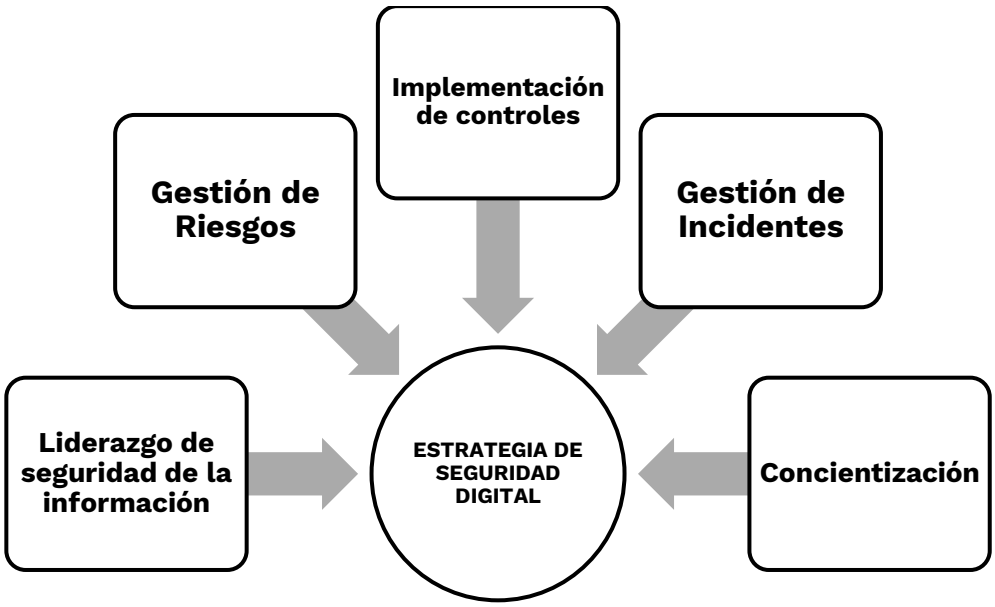
Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	20%	40%
2025	Implementación	5%	20%
2026	Evaluación de desempeño	5%	20%
2027	Mejora continua	5%	20%
TOTAL		35%	100%



6. ESTRATEGIA DE SEGURIDAD DIGITAL

CORMAGDALENA establecerá una 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 en torno a 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 que debe establecerse (Ver Resolución 500 de 2021).

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



6.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECIFICAS (EJES).

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del 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 tendiendo 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.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

6.2. PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

CORMAGDALENA 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):

Componente	Actividades	2024	2025	2026	2027
1.Fase de Planeación	1.1 Revisión de Políticas de Seguridad y Privacidad de la Información.	Crear, aprobar y divulgar Políticas	Actualizar, aprobar y divulgar Políticas	Actualizar, aprobar y divulgar Políticas	Actualizar, aprobar y divulgar Políticas
	1.2. Revisión Procedimientos de Seguridad de la Información.	Crear Procedimientos acorde con ISO 27001	Actualizar Procedimientos	Actualizar Procedimientos	Actualizar Procedimientos
	1.3. Roles y Responsabilidades de Seguridad.	Crear , Definir y aprobar Roles y responsabilidades.	Actualizar Roles y responsabilidades	Actualizar Roles y responsabilidades	Actualizar Roles y responsabilidades
	1.4. Identificación, documentación y aprobación de activos de información	Documentar y aprobar activos de información	Actualizar activos de información	Actualizar activos de información	Actualizar activos de información
	1.5. Identificación, Valoración Y Tratamiento de Riesgos	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos
	1.6. Capacitación y sensibilización.	Diseñar y aprobar programas y planes para los funcionarios sobre conciencia y comunicación de las políticas	Funcionarios toman conciencia de la seguridad y privacidad de la información.	Funcionarios toman conciencia de la seguridad y privacidad de la información.	Funcionarios toman conciencia de la seguridad y privacidad de la información.
	1.7. Implementar el Modelo de	Mantener nivel de Madurez Gestionado	Alcanzar Madurez Definido	Mantener Madurez Definido	Alcanzar Madurez gestionado

	Seguridad y Privacidad de la Información.				cuantitativamente

Componente	Actividades	2024	2025	2026	2027
2. Implementación	2.1. Planificación y Control Operacional	Crear la documentación para el control operacional	Aprobar la documentación	Aprobar la documentación	Aprobar la documentación
	2.2. Implementación del plan de tratamiento de riesgos	Verificar ejecución de acciones para el tratamiento de riesgos	Verificar ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos
	2.3. Indicadores De Gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión
	2.4. Plan de Transición de IPv4 a IPv6	Implementar y realizar seguimiento plan de transición	Renovación del pool de licencias		
Componente	**Actividades**	**2024**	**2025**	**2026**	**2027**
3.Evaluación del Desempeño	3.1. Plan de revisión y seguimiento a la implementación del MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI
	3.2. Plan de Ejecución de Auditorias	Planear y ejecutar auditorías	Planear y ejecutar auditorías	Planear y ejecutar auditorías	Planear y ejecutar auditorías
Componente	**Actividades**	**2024**	**2025**	**2026**	**2027**
4.Mejora Continua	4.1. Plan de mejora continua	Documentar el plan de mejoramiento.	Documentar el plan de mejoramiento.	Documentar el plan de mejoramiento.	Documentar el plan de mejoramiento.
	4.2. Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSP	Documentar el seguimiento al plan de mejoramiento	Documentar el seguimiento al plan de mejoramiento	Documentar el seguimiento al plan de mejoramiento	Documentar el seguimiento al plan de mejoramiento
	4.2. Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSP	Socializar resultados del plan	Socializar resultados del plan	Socializar resultados del plan	Socializar resultados del plan
Componente	**Actividades**	**2024**	**2025**	**2026**	**2027**
5. Modelo de Madurez	5.1. Autodiagnóstico nivel de madurez	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico
	5.2. Identificación del nivel madurez	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico
	5.3. Análisis de brecha	Realizar Análisis	Realizar Análisis	Realizar Análisis	Realizar Análisis

Componente	Actividades	2024	2025	2026	2027
6. Privacidad de la Información.	6.1. Contar con una herramienta de análisis sobre impacto privacidad	No aplica	Realizar la herramienta de análisis sobre impacto en la privacidad.	Ajustar la herramienta	Ajustar la herramienta
	6.2. Descripción de los flujos de información	No Aplica	Documentar los procesos	Revisar procesos documentados	Revisar procesos documentados
	6.3. Identificar los riesgos de privacidad	No Aplica	Elaborar matriz de riesgos de privacidad	Actualizar matriz de riesgos de privacidad.	Actualizar matriz de riesgos de privacidad.
Componente	**Actividades**	**2024**	**2025**	**2026**	**2027**
7. Adopción del protocolo IPV6	7.1. Plan y estrategia de transición de IPv4 a IPv6.	Verificar y actualizar el plan			
	7.2. Implementación del plan y estrategia de transición de IPv4 a IPv6.	Implementar el plan			
	7.3. Plan de pruebas de funcionalidad de IPv4 a IPv6.	Realizar pruebas			

7. 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.

8. 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.

ELABORÓ		REVISÓ		APROBÓ
Juan David Mosquera	Luis Romero G.			Firmado digitalmente por ALVARO JOSE REDONDO CASTILLO
Nombre: Juan David Mosquera Fonseca	Nombre: Luis Alfonso Romero Gazabon.	Nombre: Carlos Arturo Sarmiento Royero	Nombre: Cesar Rico Morales	Nombre: Álvaro Redondo Castillo
Cargo: Ingeniero TI Contratista Secretaria General	Cargo: Ingeniero TI Contratista Secretaria General	Cargo: Ingeniero Sistemas Contratista Dirección Ejecutiva	Cargo: Profesional Universitario Área TI	Cargo: Director Ejecutivo