CORPORACIÓN AUTÓNOMA REGIONAL DEL RIO GRAN DE LA MAGDALENA CORMAGDALENA

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024.

Contenido

1. INTRODUCCIÓN

La Corporación Autónoma Regional del Rio Grande de la Magdalena - CORMAGDALENA elaboro la presente política para disposición de los servidores públicos, contratistas y terceros que prestan sus servicios a la entidad, donde se establecen lineamientos, compromisos y un enfoque para la adecuada gestión, seguridad, privacidad y protección de la información obtenida, generada y procesada por la entidad, en el desarrollo de sus objetivos misionales y estratégicos.

La política de Seguridad y privacidad de la información de CORMAGDALENA hace parte del Modelo de Seguridad y Privacidad de la entidad y aporta a la implementación del habilitador transversal Seguridad y privacidad de la información de la política de Gobierno Digital (Decreto 1008 de 2018).

Los lineamientos de la presente política de Seguridad fueron desarrollados basados en los controles de la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001:2013, TÉCNICAS DE SEGURIDAD, SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI), los cuales deben ser aplicados en los procesos de cada una de las áreas de la entidad que hacen parte de CORMAGDALENA.

La política de seguridad y privacidad de la información tiene como fin primordial establecer lineamientos de fácil comprensión para asegurar la confidencialidad, integridad y disponibilidad de la Información de CORMAGDALENA.

CORMAGDALENA implementara la política en dos partes, una primera que va asociada con cada una de las generalidades que comprenden los objetivos, definiciones, el marco normativo, política General, Compromiso de la alta Dirección, alcance y aplicabilidad, sanciones, seguimiento, medición, análisis, evaluación, aprobación y revisión de la política y Comunicación; la segunda es la que está asociada con las políticas específicas para cada uno de los dominios establecidos en el Anexo A de la Norma 27001:2013 (Seguridad de los recursos humanos, gestión de activos, control de acceso, seguridad de los recursos criptográficos, seguridad física y del entorno, seguridad de las operaciones de TI, seguridad de las comunicaciones, seguridad para la adquisición, desarrollo y mantenimiento de sistemas, seguridad para la relación con los proveedores, gestión de incidentes de seguridad de la información, Seguridad para la Continuidad del negocio y cumplimiento)

2. OBJETIVO

Fijar los lineamientos, compromisos y enfoque para una adecuada gestión, seguridad, privacidad, y protección de la información utilizada, adquirida y procesada por CORMAGDALENA para gestionar adecuadamente la integridad, confidencialidad y disponibilidad en el marco de las políticas de Seguridad Digital y Gobierno Digital del Modelo Integrado de Planeación y Gestión (MIPG).

3. GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, locación/edificio, personas) que tenga valor para la organización. (ISO/IEC 27000).
Backup: Una copia de seguridad, respaldo, copia de respaldo o copia de reserva (en inglés backup y data backup) en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
Centro de datos: Son espacios dedicados a almacenar y procesar datos digitales, es el punto de área local (LAN)- Paneles de conexión y servidores.
Confidencialidad: Propiedad de salvaguardar la exactitud y estado completo de los activos .Es la garantía de que la información está disponible y es divulgada a personas, entidades o procesos solo autorizados.
Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
Medio removible: Son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente (Memorias USB, Discos duros extraíbles, DVD, CD entre otros).
Modelo de Seguridad y Privacidad: Conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo.
Plan de Continuidad de Negocio: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles pre - definidos después de un incidente que afecte la continuidad de las operaciones.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
Terceros: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se define la Política de Seguridad y Privacidad de la Información como la manifestación que hace la alta dirección de la Corporación Autónoma Regional del Río Grande de la Magdalena - CORMAGDALENA, sobre la intención institucional de definir las bases y la gobernanza para gestionar de manera adecuada y efectiva, la seguridad de la información; garantizando la confidencialidad, integridad y disponibilidad de sus activos de información.
CORMAGDALENA en su finalidad de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

- Minimizar el riesgo en las funciones más importantes de CORMAGDALENA.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de CORMAGDALENA.
  Garantizar la continuidad del negocio frente a incidentes.
- CORMAGDALENA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información SGSI, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

La presente Política de Seguridad y Privacidad de la información se define y la debe aprobar la Dirección Ejecutiva y se deben establecer en ella de forma clara, las líneas de actuación en esta materia, las cuales deben estar alineadas con los objetivos estratégicos de la entidad.

Por lo anterior el documento debe ser publicado y comunicado a todos los funcionarios, contratistas y terceras partes. Deben de ser de dominio público las intenciones y objetivos de CORMAGDALENA relacionados con la Seguridad de la Información, esto es fundamental para que todo el personal (funcionarios, contratistas, proveedores, terceros, etc.) perciban la importancia del tema y sean conscientes, que no es una comunicación más dentro de la entidad, sino que debe ser tenida en cuenta y puesta en práctica.

5. COMPROMISO DE LA DIRECCIÓN EJECUTIVA

La Dirección ejecutiva de CORMAGDALENA se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora de la Seguridad de la Información en la entidad, de igual forma se compromete a revisar el avance de la implementación de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener la seguridad y privacidad de la información, así mismo, incluirá dentro de los planes institucionales, actividades relacionadas con el cumplimiento de los objetivos de la política.

6. ALCANCE Y APLICABILIDAD

La política de seguridad y privacidad de la información debe ser cumplida por los funcionarios de CORMAGDALENA , así como contratistas, proveedores y en general todos aquellos que tengan relación con la entidad y apoyan la generación, procesamiento, almacenamiento y entrega de la información, busca evitar la materialización de los riesgos identificados en los activos de información de la entidad, el cumplimiento legal y normativo en las entidades públicas, disminuir las amenazas a la seguridad de la información y los datos, cuidar y proteger los recursos tecnológicos, concientizar. a los usuarios de la seguridad de la información a través del buen manejo de la infraestructura tecnológica de la entidad.

7. NIVEL DE CUMPLIMIENTO

A continuación, se establecen los 12 principios de seguridad que soportan el SGSI de CORMAGDALENA:

- CORMAGDALENA ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información SGSI, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas o terceros.

- **CORMAGDALENA** protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.

- **CORMAGDALENA** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- **CORMAGDALENA** protegerá su información de las amenazas originadas por parte del personal.

- **CORMAGDALENA** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- **CORMAGDALENA** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- **CORMAGDALENA** implementará control de acceso a la información, sistemas y recursos de red.

- **CORMAGDALENA** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- **CORMAGDALENA** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- **CORMAGDALENA** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

- **CORMAGDALENA** garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas en la seguridad y privacidad de la información.**

8. SANCIONES

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.
Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de esta.

9. APROBACIÓN Y REVISIÓN DE LA POLÍTICA

Le Corresponde al Director Ejecutivo, en su calidad de Representante Legal, Coordinar, Adoptar , Implementar, y hacer seguimiento y verificación de la Política de gobierno Digital en Cormagdalena , conforme lo prescribe el articulo 2.2.9.1.3.2 del Decreto 767 de 2015.

10. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DE LA POLÍTICA

CORMAGDALENA debe establecer indicadores para medir el cumplimiento y sensibilización de la política y sus objetivos y realizar revisiones periódicas.

11. LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN CORMAGDALENA

11.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En esta política se definen los roles y responsabilidades de la Seguridad de la Información, específicamente con respecto a la protección de los activos de información. Esta política se aplica a todos los funcionarios, contratistas y terceros de la entidad sin excepción, en donde cada uno de los cuales cumple un rol en la administración de la seguridad de la información. Todos funcionarios, contratistas y terceros de la entidad son responsables de mantener un ambiente seguro, en tanto que la Secretaría General y el Oficial de Seguridad de la Información debe monitorear el cumplimiento de las políticas de seguridad definidas y realizar las actualizaciones que sean necesarias.
Las políticas deben ser revisadas mínimo una vez al año o cuando se produzcan cambios relevantes en la operación que implique realizar ajustes o producto de los cambios en el entorno tecnológico y/o de las necesidades de la operación.

Se deben definir de forma clara los roles de la Dirección Ejecutiva, el comité de gestión y desempeño Institucional, del jefe o Coordinador de Tecnologías de la Información y de las Comunicaciones, en las funciones de coordinación, aprobación , orientación e implantación de la política de Gobierno Digital en la Corporación.

11.1.1 ORGANIZACIÓN INTERNA

La responsabilidad y aplicación de la seguridad de la información es de carácter obligatorio para todo el personal vinculado a CORMAGDALENA, cualquiera que sea su tipo de vinculación, la sede o Subdirección a la cual se encuentra adscrito y el nivel de funciones o actividades que desempeñe.

Director Ejecutivo.
Comité de Gestión y desempeño Institucional.
Secretaria General
Coordinador TIC.

Para asegurar la implementación y desarrollo de la Presente Política De Seguridad y Privacidad de la Información , El Comité de Gestión y Desempeño Institucional Deberá.

- Realizar seguimiento la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información en CORMAGDALENA
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de CORMAGDALENA
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

.

La Secretaria General de la Corporación, en apoyo con el área de Sistemas, deberá someter a consideración del Comité de Gestión y Desempeño Institucional el Plan de Seguridad y Privacidad de la Información, para ejecutar en cada vigencia, este debe incluir las revisiones y actualizaciones a que haya lugar, en busca del mejoramiento continuo.

La Dirección ejecutiva deberá realizar la divulgación de la aplicación de la Política de Seguridad y Privacidad de la Información, a todo el personal que se vincule a CORMAGDALENA, independientemente del tipo de vinculación que tenga. Todo el personal vinculado a la entidad deberá firmar un acuerdo o compromiso donde exprese la intención de cumplimiento de la Política de Seguridad y Privacidad de la Información, el uso adecuado y cuidado de las herramientas TIC dentro y fuera de la corporación. Para el personal contratista se deberá dejar estipulado en el contrato de vinculación. Para el personal de Carrera, planta o provisional se realizará mediante carta de compromiso, según formato establecido por el área de talento humano.

12.1 GESTIÓN DE ACTIVOS

CORMAGDALENA considera necesario establecer la Política de gestión de activos para identificar los activos organizacionales, así como sus propietarios y definir las responsabilidades de protección apropiadas.
La política se compone de los siguientes lineamientos, aplicables al roll que desempeñe en la entidad cada funcionario o contratista:
Lineamientos:

a) El Oficial o Líder de seguridad de la información es el responsable de dirigir las actividades para la identificación de activos de información en cada proceso, asegurando que el inventario sea exacto, consistente y esté alineado con los criterios establecidos por la entidad para la valoración y calificación de los activos, cumpliendo que:

   Toda la información contenida en los activos debe ser clasificada por su criticidad, valor, y requisitos legales determinados por los propietarios. Cada activo debe tener un etiquetado en donde se identifique el nivel de clasificación asignado. El etiquetado de la información debe ser utilizado en la información física o magnética.

   Toda la información contenida en el Inventario y clasificación de activos de información es reservada y de propiedad de la entidad.

   El Inventario y clasificación de activos de información debe permanecer en un repositorio seguro con acceso restringido.

Cualquier modificación, inclusión o exclusión que se realice en el Inventario y clasificación de activos de información debe ser debidamente documentado y controlado en el historial de cambios.

El inventario y clasificación de activos de información debe ser actualizado por lo menos una vez al año y cuando se presenten retiros, adquisiciones o reemplazos en los activos identificados.

b) Los propietarios de los activos deben asegurar que éstos cuenten con los niveles de seguridad pertinentes para su protección y cumplan con las políticas determinadas por el SGSI.
c) El Oficial o Líder de seguridad de la información, en cualquier medio que contenga información de la entidad y deba ser reutilizado, antes de ser asignado al nuevo propietario, se debe asegurar que se ejecute un proceso de borrado seguro que impida la recuperación de información del medio.
d) El Oficial o Líder de seguridad de la información debe asegurar que los medios removibles no queden desatendidos debido a que pueden ser susceptibles a pérdida o robo de la información, considerando que: La información contenida en los medios es reservada o sensible para la entidad, se debe usar un cifrado que asegure la integridad y confidencialidad de la información. Se debe llevar un registro de la información contenida dentr de los medios removibles, con el objetivo de que no afecte la confidencialidad, integridad y disponibilidad de la información.
e) Cuando se termine el contrato de algún contratista o funcionario, por cualquier razón, el jefe inmediato debe asegurar la devolución de los activos que estaban bajo la responsabilidad del contratista o funcionario.
f) 6. Para cualquier activo que sea retirado o desvinculado del inventario de los activos de la de la entidad, el Oficial o Líder de seguridad de la información debe garantizar que la información sea eliminada de forma segura.
g) Todo contratista o funcionario, custodio de un activo, debe hacer un uso adecuado de los activos teniendo en cuenta los requisitos de seguridad de la información establecidos por CORMAGDALENA.
h) Los propietarios de los activos de información identificados deben cumplir con las políticas de seguridad de la información establecidas en el del marco del Sistema de Gestión de Seguridad de la Información.

12.2 GESTIÓN DE ACCESO

CORMAGDALENA considera preciso establecer la Política de control de acceso para limitar el acceso a la información y a instalaciones de procesamiento de información

La política se compone de los siguientes lineamientos, aplicables al roll que desempeñe en la entidad cada funcionario o contratista:
Lineamientos:

a) El Oficial o Líder de seguridad de la información desarrollará los lineamientos y los procedimientos de acceso a los recursos tecnológicos necesarios para que los usuarios, funcionarios y/o contratistas puedan desempeñar sus funciones.
b) El Oficial o Líder de seguridad de la información desarrollará los lineamientos y las respectivas responsabilidades claramente definidas por los jefes de las dependencias y de los supervisores de los contratos.
c) El Oficial o Líder de seguridad de la información debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la entidad.
d) El Oficial o Líder de seguridad de la información debe establecer la periodicidad con la cual debe verificar los controles de acceso de los funcionarios y contratistas de la entidad, y cerciorarse que los usuarios acceden solamente a los recursos autorizados los cuales necesita para la realización de sus tareas.
e) Es responsabilidad de los funcionarios y contratistas el manejo y uso de los recursos, así como de las claves asignadas.
f) El Administrador del control de acceso lógico debe asegurar que las redes inalámbricas cuenten con métodos de autenticación que evite accesos no autorizados.

12.3 GESTIÓN DE ACCESO DE USUARIOS

CORMAGDALENA considera preciso establecer la Política de control de acceso para asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
La política se compone de los siguientes lineamientos, aplicables al roll que desempeñe en la entidad cada funcionario o contratista:

Lineamientos:

CORMAGDALENA a través del área de tecnología o sistemas, desarrollará los lineamientos para el acceso de usuarios teniendo en cuenta lo siguiente:

a) El Administrador del control de acceso lógico debe implementar controles para asegurar el acceso de los usuarios autorizados y evitar el acceso de los usuarios no autorizados a los sistemas, datos y servicios de información.
b) El Administrador del control de acceso lógico debe activar las claves de acceso a los diferentes activos de información cuando es un usuario

nuevo; o cuando un usuario actual haya sido trasladado de dependencia en el interior de la entidad; o cuando un usuario actual le hayan sido modificadas sus funciones, actividades y/u obligaciones.

c) El Administrador del control de acceso lógico deben inactivar las claves de acceso a los diferentes activos de información cuando es un usuario ha sido desvinculado o ya no desarrolle contrato o convenio alguno con la entidad; o cuando hayan sido suspendidas sus funciones y/u obligaciones; o cuando haya sido trasladado a otra dependencia.
d) Los jefes de las áreas o dependencias deben definir los usuarios que puedan utilizar los recursos informáticos, así como los perfiles que se les asigna (consultar, ingresar o modificar información, etc.). Para cada uno de estos perfiles se deben generar cláusulas de confidencialidad entre los empleados que lo utilizan.
e) Cualquier cambio en las funciones de los usuarios, deben ser notificados por el jefe del área o dependencia al área de tecnología o sistemas.
f) El Administrador del control de acceso lógico debe revisar los derechos de acceso de los usuarios a intervalos regulares.
g) Las contraseñas deben cambiarse obligatoriamente cuando lo establezca el área de tecnología o sistemas.
h) Después de un número determinado de intentos no exitosos de ingreso de la contraseña, el usuario será bloqueado de manera inmediata y deberá solicitar el desbloqueo a través del área de tecnología o sistemas.

12.4 NO REPUDIO

Se debe contar con la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción, incluyendo:

- Realizar trazabilidad de acciones para seguimiento de creación, origen, recepción, entrega de información, entre otros.
- Se deberá retener la información de acciones realizadas por usuarios (logs) por un periodo de tiempo definido por CORMAGDALENA, de acuerdo con su necesidad actual.
- El plan de auditoría debe incluir la revisión de acciones críticas de las partes interesadas.
- En los intercambios electrónicos de información se garantizará el no repudio.

12.5 PRIVACIDAD Y CONFIDENCIALIDAD

Es Responsabilidad de la Dirección Ejecutiva a través de la Secretaria General con el apoyo del Área de Sistemas de la Corporación asegurar el cumplimiento de la Ley 1582 de 2012, por medio de la cual se regula la protección de datos personales en Colombia.7

Las áreas que procesan datos personales de usuarios internos y externos de la Corporación u otros deberán cumplir con la política de seguridad de la información, cumplir la normatividad colombiana de seguridad de información e implementar controles necesarios para asegurar el tratamiento de la información sensible de los mismos, garantizando la confidencialidad, integridad y disponibilidad de la información.
el equipo de sistemas de CORMAGDALENA debe implantar los controles necesarios para proteger la información personal interno y externo e información sensible almacenada en base de datos o cualquier otro repositorio, evitando su divulgación (confidencialidad), alteración (integridad) o eliminación (disponibilidad) sin la autorización respectiva.

Los usuarios de la información corporativa deberán guardar total discreción y reserva con el uso de la misma; esta debe ser usada para el apoyo a la gestión y desarrollo de procesos misionales corporativos. Es necesario identificar la identidad de las personas o terceros a quienes se les entrega información. Esta entrega debe estar autorizada por un integrante de la alta dirección en cada una de las dependencias de CORMGADALENA.

Los usuarios de los sistemas de información de la Corporación deberán empoderase de la responsabilidad propia sobre las claves de acceso y autorización asignadas, para lo cual, deben cambiarla periódicamente para evitar ataques de ingeniería Social. Sus equipos de cómputo deben estar bloqueados en los momentos de inactividad o pausas activas, como mecanismo de seguridad y control.

12.6 INTEGRIDAD

Entendiendo la información como uno de los activos más importantes de la Corporación, deberá dársele un manejo íntegro a toda la información interna y externa, tanto por parte de los funcionarios como de los contratistas y externos. Así, toda la información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

Para los funcionarios de Cormagdalena con vinculación contractual, se recomienda incluir el compromiso del manejo íntegro e integral de la información en las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información. Esta política aplica al personal vinculado a

CORMAGDALENA a lo largo de la vigencia de su contrato o periodo de la vinculación.

12.7 DISPONIBILIDAD DEL SERVICIO DE INFORMACIÓN

CORMAGDALENA deberá contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

La política de disponibilidad debe incluir como mínimo los siguientes aspectos:

- Niveles de disponibilidad: Esta política debe velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con clientes, proveedores y/o terceros en función de las necesidades de la Entidad, los acuerdos de nivel de servicios ofrecidos y evaluaciones de riesgos.

- Planes de recuperación: La política debe incluir los planes de recuperación que incluyan las necesidades de disponibilidad del negocio.

- Interrupciones: La política debe velar por la gestión de interrupciones de mantenimiento de los servicios que afecten la disponibilidad de este.

- Acuerdos de Nivel de servicio: Tener en cuenta los acuerdos de niveles de servicios (ANS) en las interrupciones del servicio.

- Segregación de ambientes: Esta política debe establecer la segregación de ambientes para minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción.

- Gestión de Cambios: La política debe incluir gestión de cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

-

12.8 REGISTRO Y AUDITORIA

Esta política debe velar por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.
Esta política debe contener:

- Responsabilidad: Incluir la responsabilidad de la Oficina de Control Interno, acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.

- Almacenamiento de registros: La política debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de estas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.

- Normatividad: La política de auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimientos legales que le apliquen a la UMV.

- Garantía cumplimiento: La política de auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la entidad, así como las recomendaciones que puedan surgir a partir de dicha evaluación.

- Periodicidad: La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logra a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad.

12.9 GESTIÓN DE INCIDENTES DE LA INFORMACIÓN

CORMAGDALENA considera preciso establecer la Política para la gestión de incidentes, cuyo objetivo es asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

La política se compone de los siguientes lineamientos, aplicables al roll que desempeñe en la entidad cada funcionario o contratista
La entidad debe definir:

- Los responsables de la gestión de incidentes de seguridad de la información.
- Los medios dispuestos por la entidad para el reporte de los incidentes de seguridad de la información.
- Los mecanismos y métodos para la recolección de evidencias de los incidentes de seguridad de la información.
- La gestión de incidentes debe compartirse con todos los colaboradores, lo cual permite que puedan identificar y reportar todos los incidentes que afecten uno o varios de los pilares de seguridad de la información (confidencialidad, integridad y disponibilidad).
- La gestión de incidentes debe contar con mecanismos o herramientas que permitan cumplir con los tiempos de respuesta antes los incidentes que se presenten.

A partir de los incidentes presentados, el Oficial o Líder de seguridad de la información debe proporcionar los mecanismos para el aprendizaje que permitan reducir la probabilidad de ocurrencia de incidentes semejantes.

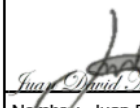
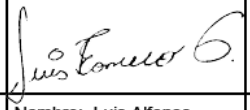
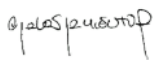
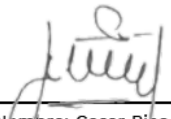
12.10 CAPACITACIÓN Y SENSIBILIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN

La política de seguridad será publicada en la página web de la entidad, en lugar de fácil acceso y socializada al personal de la entidad (contratistas, funcionarios, y responsables de la seguridad de la información), y debe ser incluida en el proceso de inducción de nuevos funcionarios y contratistas.

CORMAGDALENA al inicio de la vigencia del plan de acción debe diseñar e implementar un Plan de comunicación, sensibilización y capacitación sobre seguridad y privacidad de la información aprobado por la Dirección Ejecutiva o el comité de seguridad de la información realizando ajustes de ser necesario anualmente.

CORMAGDALENA debe destinar recursos para implementar la política y brindar formación en temas relacionados con la seguridad de la información, con el fin de disminuir las vulnerabilidades y amenazas que afecten a los procesos por parte de los funcionarios.

REGISTRO DE APROBACIÓN			
Versión	0	Fecha	Septiembre de 2024
MOTIVO DEL CAMBIO			
Creación de la política			
RESUMEN DEL CAMBIO			
Se establecen los lineamientos específicos para cada uno de los dominios establecidos en la Norma 27001 para la seguridad y privacidad de la información de CORMAGDALENA.			

ELABORÓ		REVISÓ		APROBÓ
				 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