RESOLUCIÓN No. 5 846

FECHA: 28 DIC. 2021

"POR MEDIO DE LA CUAL SE ADOPTAN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI), LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LA POLÍTICA DE SEGURIDAD DIGITAL DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL MAGDALENA – CORPAMAG"

El suscrito Director General de la Corporación Autónoma Regional del Magdalena, en uso de sus facultades legales, en especial las conferidas por la Ley 99 de 1993 y

CONSIDERANDO:

Que el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*, en el artículo 2.2.9.1.1.3., incluye la Seguridad de la Información entre los principios de la Política de Gobierno Digital; de igual manera, en el artículo 2.2.9.1.2.1., se establece que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales, y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital. Resaltando así, que las disposiciones de este Decreto representan la evaluación de la estrategia de *"Gobierno en Línea"* a la política pública de *"Gobierno Digital"*, cuyo objetivo es incentivar el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones - TIC, para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entono de confianza digital.

Que las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998, como es el caso de la Corporación Autónoma Regional del Magdalena, están obligadas a adoptar la política de Gobierno Digital, siguiendo los lineamientos del Manual de Gobierno Digital, que define procedimientos, estándares y acciones a ejecutar por parte de las entidades.

Que la adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) es una decisión estratégica para una entidad pública y que se encuentra influenciada por las necesidades y objetivos de la entidad, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización.

Que el Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), adoptó el Modelo Integrado de Planeación y Gestión – MIPG, definiéndolo en su artículo 2.2.22.3.2 como *" ...un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y*

resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio".

Que la ley 1712 de 2014 *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*, tiene como objetivo principal regular el derecho de acceso a la información publica, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

Que la Ley 1955 de 2019 Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 – *"Pacto por Colombia, Pacto por la Equidad"*, el numeral 7 del artículo 3, establece que el Plan Nacional de Desarrollo está compuesto por objetivos de política pública denominados pactos; dichos pactos contienen estrategias transversales como el *"Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento"*, lo cual se articula con los objetivos del Ministerio de Ciencia, Tecnología e Innovación, en relación con el desarrollo del conocimiento científico, tecnológico y de innovación, en aras de la modelización del Estado, según lo establecido en el artículo 126 de la Ley 1955 de 2019, que modificó parcialmente el artículo 2 de la Ley 1951 de 2019 por la cual se crea el MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN, se fortalece el SISTEMA NACIONAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN y se dictan otras disposiciones.

Que dicho pacto tiene como objetivo el uso y aprovechamiento de las TIC para mejorar la provisión de servicios digitales de confianza, el desarrollo de procesos internos eficientes, la toma de decisiones basadas en datos confiables y actualizados, el empoderamiento de los ciudadanos y el impulso en el desarrollo de territorios y ciudades inteligentes, logrados a partir de la consolidación de un Estado y ciudadanos competitivos, proactivos, e innovadores, que generan valor público en un entono de confianza digital.

Que por consiguiente, la aplicación de este pacto por el buen uso de las Tecnologías de la Información y las Comunicaciones – TIC, permitirá a las entidades públicas mejorar su funcionamiento y su relación con otras entidades, con los ciudadanos y agentes del sector, fortaleciendo la relación con el Estado en un entono confiable, que permita la apertura y aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, la participación en el diseño de servicios y programas, así como la identificación de soluciones a problemáticas de interés común, todo esto en el marco de la eficiencia en la prestación del servicio público.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expidió la Resolución 500 de 2021, "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital*", plantea los lineamientos generales para la implementación

RESOLUCIÓN No. 5 846

FECHA: 28 DIC. 2021

"POR MEDIO DE LA CUAL SE ADOPTAN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI), LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LA POLÍTICA DE SEGURIDAD DIGITAL DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL MAGDALENA – CORPAMAG"

del Modelo de Seguridad y Privacidad de la Información - MSPI y la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital. Asimismo, establece las directrices y estándares para la estrategia de seguridad digital.

Que descrito lo anterior, se hace necesario adoptar mediante el presente acto administrativo, el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política General de Seguridad y Privacidad de la Información y de Seguridad Digital, en la Corporación Autónoma Regional del Magdalena – CORPAMAG, articulando lo expuesto con los objetivos del pacto por la transformación digital, como estrategia transversal establecida por el Plan Nacional de Desarrollo 2018-2022.

Que, en mérito de lo expuesto, este Despacho

RESUELVE:

CAPITULO I
DISPOSICIONES GENERALES

ARTÍCULO PRIMERO: Objeto. La presente Resolución tiene como objeto adoptar la Política General de Seguridad y Privacidad de la Información y la Política de Seguridad Digital de la Corporación Autónoma Regional Del Magdalena – Corpamag. Así como definir lineamientos frente al uso y manejo de la información.

ARTÍCULO SEGUNDO: Alcance y Aplicación. La presente Política General de Seguridad y Privacidad de la Información y la Política de Seguridad Digital, se dicta en cumplimiento de las disposiciones legales vigentes y basada en la norma IS027001:2013, con el ánimo de gestionar adecuadamente la seguridad de la información en los procesos, en los activos, en sistemas informáticos y lógicos, partes interesadas, la infraestructura de red de la organización, instalaciones físicas y el entorno.

Esta política aplica a los procesos y procedimientos de la entidad y está dirigida a todos los usuarios internos, externos, servidores, funcionarios en todas las vinculaciones, y a todos los clientes internos y externos, que sean usuarios de los servicios informáticos, digitales y manuales de la Corporación Autónoma Regional Del Magdalena – Corpamag, que traten datos y generen información.

El modelo de seguridad de la información para la Corporación Autónoma Regional Del Magdalena – Corpamag, estará conformado por políticas, estándares, procedimientos y

mecanismos de seguridad, basados en el modelo del Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC). Son fundamentos de la seguridad de la información: la Confidencialidad, la Integridad y la Disponibilidad, según la norma ISO 27001.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad informática, de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en la entidad; este proceso será liderado de manera permanente por la Oficina de Planeación de Corpamag.

Esta política será revisada con regularidad como parte del proceso de revisión institucional, o cuando se identifiquen cambios en la entidad, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran integralmente a la política

ARTÍCULO TERCERO: Definiciones. Para los efectos de la presente resolución, se adoptan las siguientes definiciones básicas, sin perjuicio de desarrollar su naturaleza, características, contenido y alcance en el respectivo procedimiento de seguridad y privacidad de la información de la Corporación, que hace parte integral de este acto administrativo.

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Antivirus: Programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

Aplicaciones web: Son un tipo de software que se codifica en un lenguaje soportado por los navegadores web y cuya ejecución es llevada a cabo por el navegador en Internet o de una intranet. Autenticación: cuando se puede garantizar la identidad de quien solicita acceso a la informática.

Autorización: Cuando la informática es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo.

Código malicioso: Es un término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso.

Confidencialidad: Cuando la informática es solo accesible por aquellos a los cuales se ha autorizado a tener acceso.

Controles criptográficos: Proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.

Correo electrónico: Es un medio de comunicación electrónico que permite el intercambio de mensajes con usuarios internos externos a través de una cuenta de correo electrónico institucional de manera segura, ágil y confiable que facilite el desarrollo de sus funciones.

Criptografía: Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

Declaración de Aplicabilidad: De la norma ISO 27001, es una relación completa de Controles de Seguridad de la Información, donde se indica si cada uno de ellos resulta de aplicación o no a la organización. Los Controles serán considerados aplicables según la actividad, la gestión interna y el entorno de la empresa. En cada caso, se deberán detallar los motivos por los que se aplica o no dicho Control, y tener información de su estado de implantación.

Disponibilidad: Cuando la informática es accesible a los usuarios autorizados en el momento de requerirla. Un ejemplo de control para garantizar la disponibilidad son los planes de contingencia.

El software malicioso: Conocido en inglés como "malware", es un software diseñado específicamente para obtener acceso a un equipo o dañarlo sin que el usuario tenga conocimiento

El spyware: Programa espía es un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

El riesgo de seguridad: Es la probabilidad de que se materialice el peligro: es decir, que les genere daño a las personas, bienes o al entorno.

Informática: Se refiere a toda comunicación o representación de conocimiento a partir de datos, representados en diferentes formas, incluías formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio que implique almacenamiento (sistemas de informática), transmisión, ya sea por medio electrónico (correo electrónico, fax) o por medio oral (telefonía fija, móvil, correo de voz, contestadoras): medio audiovisual (prensa,

radio, TV), medios masivos (publicaciones científicas, académicas y periodísticas, redes sociales), papel, entre otros.

Infraestructura: Es el conjunto de elementos o servicios que están considerados como necesarios para que una organización pueda funcionar o bien para que una actividad se desarrolle efectivamente.

Integridad: Cuando la informática es exacta y completa.

IS027001: Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.
Matriz de requisitos legales: Es un documento que contiene toda la información sobre la normatividad que una empresa debe cumplir legalmente.

Matriz de requisitos legales: Matriz legal es un documento que contiene toda la información sobre la normatividad que una empresa debe cumplir legalmente

Mecanismos de control: Distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos y para fortalecer la confidencialidad, la integridad y la disponibilidad de la información tanto física como digital.

Mesa de Servicio: Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación

MIPG: El Modelo Integrado de Planeación y Gestión es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas con el fin de generar resultados que atiendan a los planes de desarrollo y que resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en los servicios.

No repudiación: Cuando la informática involucrada en un evento corresponde a quien participa, quien no podrá evadir su intervención en este.

Página Web: Es conocida como un documento de tipo electrónico, el cual contiene información digital, la cual puede venir dada por datos visuales y sonoros, o una mezcla de ambos, a través de textos, imágenes, gráficos, audio o vídeos y otros tantos materiales dinámicos o estáticos.

Plataforma tecnológica: Es toda la base tecnológica que una empresa o institución tiene y ofrece a toda su comunidad, orientada a todo lo que es el enfoque o nivel de servicio y

tecnología. En tecnología, hace referencia a lo relacionado con instalaciones de plataformas, portal de servicios web, plataformas de correos, servidores de archivos, instalaciones de servidores físicos donde se alojan todas las herramientas y recursos que se ofrecen, conectividad a internet y dentro de la entidad (cableado estructurado), acceso a todos los equipos y dispositivos, licenciamiento de antivirus a nivel organizacional, soluciones a nivel de virtualización, entre otros.

Política de navegación: El contenido en esta política de navegación web, aplica a los servicios de navegación web que brinda la Corporación Autónoma Regional del Magdalena - Corpamag, con personal interno o externo, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos y esta publicada en el sistema de gestión de calidad de la entidad.

Portal: Es sitio Web que ofrece al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados a un mismo tema. Incluye: enlaces, buscadores, foros, documentos, aplicaciones, compra electrónica, etc.
Recursos tecnológicos: Es un medio que se vale de la tecnología para cumplir con su propósito.

ARTICULO CUARTO: Objetivos. La Política General de Seguridad y Privacidad de la Información tendrá los siguientes objetivos:

1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
2. Gestionar los riesgos de seguridad y privacidad de la información.
3. Mitigar los incidentes de Seguridad y Privacidad de la Información de forma efectiva. eficaz y eficiente.
4. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad de la información de la Corporación.
5. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
6. Fortalecer la cultura de Seguridad y Privacidad de la Información en los usuarios, proveedores, visitantes, tercerizados, contratistas y funcionarios de Corpamag.
7. Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información.
8. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

"POR MEDIO DE LA CUAL SE ADOPTAN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI), LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LA POLÍTICA DE SEGURIDAD DIGITAL DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL MAGDALENA – CORPAMAG"

CAPITULO II
POLÍTICAS ESPECÍFICAS DE MANEJO DE INFORMACION

ARTICULO QUINTO: Política de Gestión de Activos. La Corporación Autónoma Regional del Magdalena – Corpamag, a través de la Secretaría General, establecerá y divulgará los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información con el objetivo de garantizar su protección, y estarán alineados a los procesos de la entidad:

A. ***Identificación de Activos:*** Los activos de la Corporación Autónoma Regional del Magdalena deben ser identificados, clasificados, valorados y controlados para garantizar su uso adecuado, protección y recuperación ante desastres. Por tal motivo, se diseñará una metodología con los lineamientos necesarios para llevar la identificación de los activos de información de su propiedad, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la Entidad disponga.

B. ***Protección:*** Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargaran de proteger la información, mantener y actualizar el inventario de activos de información relacionados con sus servicios (Información física o digital, software, hardware y recurso humano).

C. ***Archivos de Gestión:*** La Secretaria General a través del grupo encargado de la gestión documental de Corpamag y con el acompañamiento de la Oficina Planeación, deben implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad, con el fin de proteger y conservar la confidencialidad, la integridad y la disponibilidad de la información de la Entidad.

D. ***Clasificación de la Información:*** La clasificación de la información de Corpamag, tendrá en cuenta las previsiones contenidas en la Ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, la Ley 594 de 2000 (Ley General de Archivos), y lo estipulado en la Guía para Desarrollo de Inventario y Clasificación de Activos de Información de la Corporación.

ARTICULO SEXTO: Política de Seguridad de los Recursos Humanos. La Corporación Autónoma Regional del Magdalena – Corpamag a través de la oficina de Talento Humano debe asegurar que los funcionarios, contratista y demás colaboradores adopten sus responsabilidades en relación con las políticas de la Seguridad y Privacidad de la Información y

actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

PARAGRAFO. En relación con los contratistas, la Oficina Asesora de Contratación deberá incluir en las minutas de los contratos cualquiera que sea su denominación que se le dé al mismo, las clausulas u obligaciones correspondientes a la Seguridad de la Información con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones, medios y recursos tecnológicos, asegurando la confidencialidad, disponibilidad e integridad de la información y serán divulgadas a los contratistas a través de los supervisores, y que resalten la existencia de los tres principios que debe respetar la gestión de la información en cualquier Entidad para poder cumplir, de forma correcta, los criterios de eficiencia y eficacia, es garantizar tres aspectos: confidencialidad, integridad y disponibilidad de la Información como algo general para mantener un sistema y sus entorno seguro y fiable.

ARTICULO SEPTIMO: Política de Seguridad Física y del Entorno La Corporación Autónoma Regional del Magdalena – Corpamag, debe adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas; para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), además para mitigar los riesgos y amenazas externas y ambientales, con el fin de evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la Entidad.

ARTICULO OCTAVO: Política de Control de Acceso. Los propietarios de los activos de información y teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso: a nivel de red, sistema operativo, sistemas de información. servicios de tecnologías e infraestructura física (instalaciones y oficinas) con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de personal no autorizado, y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información de La Corporación Autónoma Regional del Magdalena.

ARTICULO NOVENO: Política de Seguridad de las Operaciones de TI. La Secretaría General de Corpamag, será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación en la Entidad. De igual forma, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, y asegurando que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de prueba y producción sean controlados y debidamente autorizados.

"POR MEDIO DE LA CUAL SE ADOPTAN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI), LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LA POLÍTICA DE SEGURIDAD DIGITAL DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL MAGDALENA – CORPAMAG"

De igual manera, estará encargada de proveer la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, realizando los respectivos análisis y proyecciones de crecimiento y provisiones en la infraestructura tecnológica de acuerdo al crecimiento de la Entidad basados en la dinámica de la misma, así como, implementar mecanismos de contingencias y continuidad del negocio con el fin de propender por la disponibilidad de los servicios de Tecnologías de la información en el marco de la operación de La Corporación Autónoma Regional del Magdalena.

La Secretaría General de Corpamag, deberá realizar y mantener copias de seguridad de la información de la Entidad en medio digital, reportada por el responsable de esta en una bitácora o registro de seguimiento, con el objetivo de contar con la descripción exacta y pueda ser recuperarla en caso de cualquier tipo de falla. Realizará las copias respectiva de acuerdo con el esquema definido previamente en el procedimiento que describa la gestión, copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos de la Entidad; el diseño de este procedimiento se hará en acompañamiento con la Oficina de Planeación y a su vez, en conjunto con los líderes de procesos, con el fin de determinar la información a respaldar y la periodicidad del respaldo, los tiempos de recuperación y restauración, y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información.

ARTICULO DÉCIMO: Política de Seguridad de las Comunicaciones. La Secretaría General de Corpamag, será la encargada de establecer los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de Corpamag.

Desde Oficina de Planeación se establecerán mecanismos necesarios para que el intercambio de información con las partes interesadas internas o externas se realice asegurando su integridad. En el evento que los acuerdos de intercambio de información requieran del desarrollo de webservice o cualquier otro medio tecnológico utilizado en comunicaciones o Interoperabilidad, el intercambio deberá realizarse con los controles criptográficos requeridos definidos por cada protocolo a utilizar.

ARTICULO DÉCIMO PRIMERO: Política de Gestión de Incidentes Seguridad de la Información. La Corporación Autónoma Regional del Magdalena – Corpamag, promoverá entre los servidores públicos y contratistas el reporte y seguimiento de incidentes relacionados con la seguridad de la información y sus medios. Así mismo, asignara responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo con su criticidad.

PARAGRAFO. La Oficina de Planeación conforme al rol de los profesionales encargados, serán los autorizados para reportar incidentes de seguridad ante las autoridades, previo análisis, reporte y levantamiento de información del caso realizado por los encargados del soporte y recursos tecnológicos en Secretaría General de Corpamag; así mismo, se debe tener en cuenta los canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía de llegar a ser requerido.

ARTICULO DÉCIMO SEGUNDO: Política de Cumplimiento. La Corporación Autónoma Regional del Magdalena – Corpamag, velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional.

ARTICULO DÉCIMO TERCERO: Lineamientos de las Políticas de Seguridad de la Información. Todas las políticas identificadas en este Capítulo se podrán actualizar o reglamentar de manera detallada y clara en una Declaración de Aplicabilidad (SOA) y en el Manual de Políticas de Seguridad de la Información de la Corporación Autónoma Regional del Magdalena. Documentos que serán desarrollados por la Secretaría General y la Oficina de Planeación, si se determinan necesario durante la vigencia de las mismas.

CAPITULO III
RESPONSABILIDADES FRENTE AL USO DE LOS SERVICIOS TECNOLOGICOS

ARTICULO DÉCIMO CUARTO: Responsabilidad. Todos los funcionarios públicos y contratistas que hagan uso de los recursos tecnológicos de Corpamag, tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios de TI y, por ende, el cumplimento de la misión institucional. Para ello, se deben acatar las siguientes disposiciones:

A. **Del Uso de los recursos Tecnológicos:** Los recursos tecnológicos de Corpamag, son herramientas de apoyo a las actividades y responsabilidades de los funcionarios públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

    1. Solo está permitido el uso de software licenciado por la Corporación o aquel que sin requerir licencia sea expresamente validado por el personal encargado del Soporte Técnico. Las aplicaciones generadas o adquiridas por la Entidad, en desarrollo de su operación institucional, deben ser reportadas para su respectiva validación y evaluación de requerimientos técnicos de la capacidad disponible.

"POR MEDIO DE LA CUAL SE ADOPTAN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI), LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LA POLÍTICA DE SEGURIDAD DIGITAL DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL MAGDALENA – CORPAMAG"

2. Los equipos de cómputo de la Entidad, serán utilizados de manera exclusiva y bajo la completa responsabilidad por el funcionario o contratista al cual han sido asignados, y únicamente para el correcto desempeño de las funciones del cargo o las actividades desempeñadas. Por tanto, no pueden ser utilizados con fines personales o por terceros, no autorizados por Jefes de Oficina, Secretaría General, Director o Subdirectores

3. En caso de que un funcionario público o contratista deba hacer uso de equipos ajenos a Corpamag, estos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red de la Entidad una vez este avalado por los encargados del Soporte Técnico de la Corporación.

4. Los funcionarios o contratista, no deben mantener almacenados en los discos locales de los equipos o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.

5. No se permite fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los dispositivos tecnológicos, en la medida que la exposición de los equipos a estos puede ocasionar daños en los mismo.

6. Únicamente estarán autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar, actualizar o reparar sus componentes, son los designados por la Secretaría General y los encargados del Soporte Técnico de la Entidad para tal labor.

7. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Secretaría General, previo consenso a la solicitud de traslado, con el fin de llevar el control individual de inventario de los activos de este tipo. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos vigentes.

8. Cuando se presente pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, el funcionario o contratista responsable, debe Informar la oficina o sede donde se detecta la pérdida del bien a su Jefe directo, coordinador o supervisor para realizar lo establecido para este tipo de siniestro, así como también a la Secretaría General con el fin de reportar el evento o incidente se seguridad de la información.

9. La pérdida de información debe ser informada con el detalle de la información afectada al personal de Soporte Técnico de la Secretaría General para el diligenciamiento del reporte de gestión de incidente o evento de seguridad a la mayor brevedad posible para dar la solución.

10. Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad. Inicialmente a la Secretaría General a través de los encargados del Soporte Técnico para el levantamiento de información del incidente o evento de seguridad.

11. Todo acceso a la red de la Corporación, mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por los Responsables desde la Secretaría General.

12. La conexión a la red inalámbrica o Wii de la Entidad disponible para funcionarios públicos y contratistas deberá ser administrada desde la Secretaría General a través de los encargados, quienes a su vez entregaran el insumo requerido por la Oficina de Planeación para realizar lineamientos o políticas que fortalezcan la seguridad de la información y seguridad digital.

13. Los equipos deben quedar apagados al final de la jornada laboral, fin de semana o cada vez que el funcionario o contratista no se encuentre en la oficina durante la jornada, esto es, con el fin de proteger la seguridad y distribuir bien los recursos de la Entidad, siempre y cuando se programe actividades vía remota deben ser autorizadas por los encargados del Soporte Técnico.

B. **Del Uso de los Sistemas o Herramientas de Información:** Todos los funcionarios y contratistas de Corpamag, son responsables de proteger la información a la que acceden o procesan durante la realización de sus actividades y de evitar su pérdida, alteración, destrucción o uso indebido, para lo cual se dictan los siguientes lineamientos:

1. Las credenciales (Usuario y Contraseña) de acceso a la red o recursos informáticos, son de carácter personal e intransferible; los funcionarios y contratistas no deben revelar éstas a terceros ni utilizar claves ajenas, ni dejarlas expuestas donde puedan ser fácilmente observadas y utilizadas por terceros.

2. Todo funcionario y contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente o cuando

será requerido automáticamente por el controlador de dominio. Al igual que si las credenciales son olvidadas deben realizar un respectivo procedimiento de renovación.

3. Todo funcionario y contratista es responsable de los registros o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.

4. En el caso de terminación del vínculo laboral de un funcionario de planta permanente o temporal, desde la Coordinación de Talento Humano, se debe informar la novedad tanto a la Secretaria General y su personal Técnico como a la Oficina de Planeación, para la inactivación de los servicios tecnológicos correspondientes, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración, uso indebido o suplantación de identidad.

5. De igual forma para los contratistas, en el caso de terminación de ejecución contrato con Corpamag y si este contaba con acceso y credenciales, los supervisores deberán informar la novedad tanto a la Secretaria General y su personal Técnico como a la Oficina de Planeación, para la inactivación de los servicios tecnológicos correspondientes, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración, uso indebido o suplantación de identidad.

6. Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato en Corpamag, la información generada por funcionario o contratista será inventariada, respaldada y entregada de acuerdo el procedimiento establecido en la Entidad a petición del jefe o supervisor del contrato.

C. **Del Uso del Correo Electrónico:** El correo electrónico institucional es una herramienta de apoyo a la realización de actividades, funciones y obligaciones de los funcionarios públicos y contratistas de la Corporación Autónoma Regional del Magdalena, cuyo uso se definirá en los siguientes términos:

1. El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la Entidad es el asignado por la Corporación, a través de la Oficina de Planeación, que cuenta con el dominio ***@corpamag.gov.co***, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso

además de respaldo periódicamente de la base de datos de los correos electrónicos de cada usuario.

2. El servicio de correo electrónico corporativo o institucional debe ser empleado para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la Corporación.

3. En cumplimiento de la iniciativa del uso racional y eficiente del papel y del principio de la Eficiencia Administrativa, y siempre que la Ley lo permita, se debe preferir el uso del correo electrónico institucional para el envío de documentos físicos.

4. Los mensajes de correo electrónico, tendrán en cuenta las previsiones contenidas en la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.), normativa que establece la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.

5. Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Secretaría General a través de los funcionarios encargados del Soporte Técnico y que, a su vez, posterior a la evaluación del caso, escalará de ser necesario a la Oficina de Planeación como incidente de seguridad; y deberán acatarse las indicaciones recibidas para su tratamiento. Lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones, exe, .bat, .prg, .bak, .pif, o explicitas referencias no relacionadas con la misión Institucional (por ejemplo: contenidos sexuales, historias de famosos, ganancias económicas atractivas, herencias por reclamar, validación de cuentas bancarios y demás contenidos sospechosos o poco usual de recibir). Esta expresamente prohibido el envío y reenvió de cadena de mensajes.

6. La Cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o a cualquier otra instancia ajena a los fines y misionalidad de la Corporación al igual que, se prohíbe del correo institucional para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.

D. **Del Uso del Internet:** La Secretaría General, a través del personal encargado y responsable del servicio de internet, y con apoyo de la Oficina de Planeación, en conjunto con el profesional de la Seguridad de la Información, establecerá políticas, instructivos, guías o lineamientos de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Sera responsabilidad de los funcionarios públicos y contratista las siguientes, entre otras:

1. El uso del servicio de Internet está limitado exclusivamente para propósitos laborales y los servicios a los que un determinado usuario pueda acceder desde internet dependerán del rol o funciones que desempeña el funcionario o contratista, y para los cuales este formal y expresamente autorizado de ser necesario.

2. Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.

3. Abstenerse de enviar y descargar cualquier tipo de software o archivos de fuentes externas y de procedencia desconocida y no licenciadas ni autorizadas.

4. Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

La Corporación Autónoma Regional del Magdalena - Corpamag, se reserva el derecho de controlar los accesos a los sitios web, navegados desde la red interna hacia la Internet, con el fin de evitar fuga de información y accesos a sitios que pongan en riesgo la integridad y disponibilidad de la red local institucional, los equipos de cómputo y demás infraestructura tecnológica, y por tanto el uso del servicio de internet de todos sus funcionarios y contratistas, puede limitar el acceso a determinadas páginas de Internet, los horarios de conexión, el acceso a los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad que vaya en contra vía de la confidencialidad, integridad y disponibilidad de la información y de la seguridad digital.

CAPITULO IV
REVISIÓN, VIGENCIA Y DEROGATORIA

ARTÍCULO DÉCIMO QUINTO: Revisión. La Política General de Seguridad y Privacidad de la Información y de Seguridad Digital de la Corporación Autónoma Regional Del Magdalena – Corpamag, será revisada anualmente, o antes si se llegaran a requerir de manera extraordinaria, modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y

eficaz. Este proceso será liderado por la Oficina de Planeación y el profesional de Seguridad de la Información.

ARTICULO DÉCIMO SEXTO: Vigencia y Derogatoria. La presente resolución rige a partir de la fecha de su expedición, es de obligatorio conocimiento, aplicación y acato por todos los funcionarios y contratistas.

PUBLIQUESE, COMUNIQUESE Y CUMPLASE

CARLOS FRANCISCO DIAZ GRANADOS MARTINEZ
DIRECTOR GENERAL

Elaboró: Franklin Suárez
Revisó: Carlos Santodomingo
Aprobó. Rosana Lastra - Paul Laguna