## POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Corporación Autónoma Regional del Alto Magdalena-CAM como entidad encargada de administrar el medio ambiente, los recursos naturales renovables y propender por el desarrollo sostenible del departamento, establece que la información es de vital importancia para lograr una adecuada gestión de las actividades, en razón que es una herramienta primordial para la toma de decisiones; motivo por el cual la Corporación está comprometida en proteger los activos de información de la entidad, orientando sus esfuerzos en la preservación de la confidencialidad, integridad, disponibilidad, continuidad de los procesos, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información de la CAM.

Toda la información que es generada por los funcionarios, contratistas y terceros que presten sus servicios a la CAM en beneficio y desarrollo de las actividades propias de la Corporación es propiedad de la CAM, a menos que se acuerde lo contrario en los contratos escritos y autorizados.

La CAM para el cumplimiento de su misión, visión, objetivo estratégico, establece la presente política de Seguridad de la Información en la Entidad, con el objetivo de:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de nuestras partes interesadas
- 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.

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

## POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

### POLÍTICA DE SEGURIDAD PARA LOS RECURSOS HUMANOS

La Corporación Autónoma Regional del Alto Magdalena debe proteger la información por medio de la validación, formación y concientización del recurso humano que hará uso de la misma.

**Antes de asumir el empleo**

El personal de la Corporación, independientemente de su tipo de vinculación, funcionarios en carrera administrativa, contratistas, libre nombramiento y remoción es uno de los activos mas importantes en la gestión de los procesos estratégicos, misionales y de apoyo, por lo tanto, es vital contar con el recurso humano mejor calificado, para lo cual se deben definir estándares de seguridad que aseguren un proceso formal de selección.

Dentro de los procesos de contratación de personal o de prestación de servicios, deberá realizarse la verificación de antecedentes cuando así lo amerite. Esto aplica especialmente cuando el funcionario vaya a tener acceso a información de la Corporación que haya sido clasificada como confidencial o reservada.

La Secretaría General, en cabeza del proceso de Talento Humano, es el responsable de realizar la verificación de antecedentes, para lo cual puede llevar a cabo cualquiera de las siguientes actividades: verificación de referencias personales y laborales y validación de la hoja de vida de la persona que aplica al cargo.

**Términos y condiciones laborales**

Los funcionarios de la Corporación deben cumplir con los requerimientos de seguridad de la información y estos deben hacer parte integral de los contratos o documento de vinculación a que haya lugar, especificando en las obligaciones específicas del contratista que debe garantizar la confidencialidad e integridad de la información de la Corporación. Así mismo cumplir con la cláusula de Derechos de Autor de acuerdo con el artículo 20 de la Ley 23 de 1982, modificado por el artículo 28 de la Ley 1450 de 2011.

**Durante la ejecución del Empleo**

La oficina de talento Humano deberá realizar la divulgación de la aplicación del Manual de Políticas de Seguridad de la Información, a todo el personal vinculado a la CAM durante el proceso de inducción, independientemente del tipo de vinculación que tenga.

Para iniciar las labores, todo el personal de la entidad deberá firmar un acuerdo o compromiso donde exprese la intención de cumplimiento de la Política, acuerdo de confidencialidad de la información y el uso adecuado y cuidado de las herramientas TIC, dentro y fuera de la Corporación.

Cada supervisor o jefe inmediato deberá comprobar el cumplimiento de la firma de los acuerdos de confidencialidad de la información por parte de los contratistas o funcionarios asignados, antes de autorizar el acceso a la información. Esta Política aplica para todo el personal inclusive al provisto por empresas contratistas que realicen labores en la Corporación.

El jefe encargado de la dependencia debe informar al área de tecnologías de la información y a los administradores encargados de cada aplicativo, la vinculación del

personal nuevo, ya sea en carrera administrativa, provisionalidad, libre nombramiento y remoción o contratistas, indicando de acuerdo a las labores a realizar, los aplicativos a los cuales pueden tener acceso y de esta manera crear los usuarios, claves, correos electrónicos, configuraciones de acceso a la red, instalación de aplicativos e instalación de herramientas tecnológicas.

Talento Humano en compañía de Tecnologías de la Información de la Corporación, deben establecer jornadas de capacitación en temáticas relacionadas con la seguridad de la información, las cuales serán incluidas dentro del Plan Institucional de capacitación - PIC. La asistencia de todo personal de planta es de carácter obligatorio y la asistencia por parte de contratistas es obligatoria dependiendo el grado de relación con la información misional y de apoyo de la Corporación, según sus funciones y cargo.

**Desvinculación, licencias, vacaciones o cambio de labores**

El área de Talento Humano debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios de la Corporación llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.
El área de talento humano debe informar al área de sistemas y a los administradores de los aplicativos, las novedades de personal de planta (desvinculación, licencias, vacaciones o cambios de labores) con el fin de realizar la desactivación de los correos electrónicos, claves de acceso a los aplicativos existentes.
El supervisor o jefe inmediato tendrá la responsabilidad de asegurar que toda la información suministrada al funcionario al momento del ingreso y la generada en el desarrollo de su proceso laboral en la Corporación, sea entregada en su totalidad y que se garantice su confidencialidad.
Con respecto a la información producida por los funcionarios de planta, provisionalidad y libre nombramiento y remoción que terminan su vinculación laboral con la Corporación, deben realizar la entrega de esta al área de sistemas, quienes serán los encargados de custodiar la información entregada.

**Procesos Disciplinarios**
A todos los incidentes de seguridad de la información ocurridos en la Corporación, se les debe dar el tratamiento respectivo con el fin de determinar sus causas y responsables. Dependiendo la gravedad del incidente, control interno disciplinario deberá tomar las acciones necesarias de acuerdo a lo establecido en la ley. (Ajuste Dr, Alberto.

## GESTIÓN DE ACTIVOS TECNOLÓGICOS

**Política de uso de correo electrónico.**

La Corporación Autónoma Regional del Alto Magdalena debe definir las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

- **Usos aceptables del servicio**

El correo electrónico es de uso exclusivo para realizar tareas propias de la función desarrollada por la Corporación, no se debe usar para ningún otro fin. De igual forma se debe administrar con ética, responsabilidad, eficiencia, sin abusar ni generar riesgos para la operación de los equipos o sistemas de información de la CAM.

La asignación de usuarios para el correo electrónico se realiza únicamente para los funcionarios de planta, provisionalidad y libre nombramiento y remoción y en casos excepcionales a los contratistas que por el desarrollo de sus funciones deban tener una cuenta en el correo corporativo

Los funcionarios a los cuales se les ha autorizado el uso de correo electrónico son responsables de todas las actividades realizadas con sus usuarios de acceso a los buzones de correo, así como de mantener un comportamiento ético y evitar prácticas o usos que puedan comprometer la seguridad de la información de la Corporación.

Los mensajes enviados deberán respetar el estándar de formato e imagen corporativa definido por la Corporación.

- **Usos no aceptables del servicio**

Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivos, obsceno, pornográfico, chistes, político, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

Distribución de información de la Corporación, no pública, a otras entidades o ciudadanos son la debida autorización.

Apertura, uso o revisión indebida de la cuenta de correo electrónico de otro usuario como si fuera propia sin la debida autorización.

Enviar información Confidencial o Reservada de la Corporación a personas u organizaciones externas, salvo en los casos expresamente previstos en la Constitución Política y en la Ley, y por parte de los funcionarios autorizados internamente para ello.

- **Condiciones de uso del servicio**

El password o clave de acceso al servicio es la mejor defensa contra el uso no autorizado de la cuenta de acceso al servicio y/o a la red de datos de la Corporación, por lo tanto, se requiere que se mantenga en la mayor reserva posible, no debe suministrarse a otras personas o exhibirse en público.

El usuario no debe responder mensajes donde le solicitan información personal o financiera para participar en sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Estas situaciones se deben informar a la Oficina de Tecnologías de la Información y las Comunicaciones, con el fin de bloquear dicho remitente y evitar que esos mensajes lleguen a más funcionarios. Igualmente se deben marcar estos mensajes como no deseados desde el cliente de correo.

- **Responsabilidades**

El área de Talento Humano es la responsable de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Correo electrónico corporativo de los funcionarios de planta a la oficina de Tecnologías de la Información. Si se detecta que se solicita una cuenta institucional y que no se hace uso de ella, la oficina de tecnología podrá eliminar dicha cuenta.
El jefe de oficina o supervisor es el responsable en solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Correo electrónico corporativo de los contratistas que por su objeto contractual necesiten acceso a estas.
Los funcionarios, en el desarrollo de sus tareas habituales u ocasionales que utilicen cualquier servicio de tecnología de la información que provea la Corporación, son responsables del cumplimiento y seguimiento de esta Política.
La oficina de tecnologías de la información es la responsable de administrar la plataforma tecnológica que soporta el acceso a la red/cuentas de usuario y/o al servicio de correo electrónico corporativo para los funcionarios que desempeñen labores o actividades en la CAM.
La Oficina de Tecnologías de la Información se reserva el derecho de monitorear las comunicaciones y/o información que se comuniquen mediante el servicio de correo electrónico corporativo.

## Política de uso de internet

La Corporación Autónoma Regional de Alto Magdalena –CAM debe definir las pautas generales para asegurar una adecuada protección de la información, en el uso de servicio de internet por pare de los usuarios autorizados.

- **Usos aceptables del servicio**

  Este servicio debe utilizarse exclusivamente para las tareas propias de la función/actividad desarrollada en la Corporación y no debe utilizarse para ningún otro fin.
  Los usuarios autorizados para usar el servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la CAM.

- **Usos no aceptables del servicio**

Este servicio no debe ser usado para :

- Envío y/o descarga de información masiva de gran tamaño que pueda congestionar la red.
- Envío y/o descarga y/o visualización de información con contenidos que atenten contra la integridad moral de las personas o instituciones.

- **Condiciones de uso del servicio**

El acceso al servicio de internet podrá ser asignado a las personas que tengan algún tipo de vinculación con la Corporación como funcionarios, para lo cual se hace necesario realizar el registro del equipo de cómputo portátil diligenciando el formato Concepciones acceso de red WiFi, con el fin de tener identificados los equipos que usan la red de la CAM.
El servicio de internet debe utilizarse únicamente para desarrollar las tareas propias de la Corporación y no se le debe dar ningún otro fin.
Los usuarios son responsables tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la rede de la Corporación o descargue desde internet.
No se permitirá el acceso a páginas relacionadas con pornografía, actividades criminales, crímenes computacionales, contenidos maliciosos, suplantación de identidad o páginas catalogadas como de alto riesgo.
No se permitirá la descarga, uso, intercambio y/o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.
La Corporación, desde el área de tecnologías de la información, realizará monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios. Así mismo, podrá inspeccionar, registrar y evaluar las actividades realizadas durante la navegación.
Los funcionarios no podrán asumir en nombre de la CAM, posiciones personales en encuestas de opinión, foros u otros medios similares

- **Responsabilidades**

Cada funcionario es responsable de solicitar la creación, modificación o cancelación del servicio de internet a la oficina de tecnologías de la información
Los funcionarios, en el desarrollo de sus tareas habituales u ocasionales que utilicen cualquier servicio de tecnología de la información que provea la Corporación, son responsables del cumplimiento y seguimiento de esta política.
La oficina de Tecnologías de la Información es el responsable de administrar la plataforma tecnológica que soporta el acceso a la red/cuentas de usuario y/o al servicio de internet para los funcionarios que desempeñen labores/actividades en la Corporación.

- **Política de uso de redes sociales**

La Corporación debe definir los estándares de seguridad con el fin de garantizar la protección de la información, en el uso del servicio de redes sociales por parte de los usuarios autorizados.
Los funcionarios a los cuales se les han otorgado los permisos para el ingreso a redes sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la Corporación.
El uso de las redes sociales debe ser utilizado exclusivamente para actividades relacionadas con la misión de la Corporación. Todas las comunicaciones establecidas mediante este servicio pueden ser monitoreadas por la oficina de tecnologías de la información o cualquier instancia de vigilancia y control.
La Corporación facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un complemento a muchas actividades que se realizan por estos medios, sin embargo, es necesario utilizar este medio de forma correcta.
No es permitido descargar programas ejecutables o ficheros que sean susceptibles de contener "software malicioso".
No es permitido descargar, difundir, o distribuir material obsceno, degradante, terrorista, político, abusivo o calumniante a través de las redes sociales.
La oficina de Tecnologías de la información, será la encargada de determinar las directrices y lineamientos para el uso de los diferentes sistemas o plataformas de redes sociales de la entidad.

- **Usos no aceptables del servicio**

Envío y/o descarga de información masiva de gran tamaño que pueda congestionar la red.
Envío, descarga o visualización de información con contenidos que atenten contra la integridad moral de las personas o instituciones.
Cualquier otro propósito diferente a las actividades relacionadas con la Corporación.

**Política de uso de Recursos tecnológicos**

La Corporación debe definir las pautas generales para asegurar una adecuada protección de la información, a través de la definición de las condiciones de uso aceptable de los recursos tecnológicos.
La CAM asignará destinará diferentes recursos tecnológicos como herramientas de trabajo para uso exclusivo de los funcionarios autorizados. El uso adecuado de estos recursos se reglamentara bajo las siguientes directrices:
La instalación de cualquier tipo de software en los equipos de cómputo de la CAM, debe ser realizada por la oficina de Tecnologías de la Información, por lo tanto, son los únicos autorizados para realizar esta labor.
Los usuarios no deberán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, protector de pantalla

corporativo o traslado de hardware. Estos cambios podrán ser realizados únicamente por el área de tecnologías de la información.
El área de tecnologías de la información definirá la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en los computadores del personal de planta, así mismos, realizará el control y verificación de cumplimiento de licenciamiento del respectivo software y aplicaciones asociadas.
Los funcionarios de la Corporación son responsables de hacer buen uso de los recursos tecnológicos de la CAM y en ningún momento podrán ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros funcionarios, terceros, la legislación vigente y las políticas y lineamiento de seguridad de la información de la CAM.
La información de carácter personal almacenada en dispositivos de cómputo, medios de almacenamiento o cuentas de correo institucionales debe ser almacenada en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada "PERSONAL".

**Política de Uso de contraseñas y usuarios**

La asignación de usuarios y contraseñas es un permiso que la CAM otorga a sus funcionarios, contratistas o practicantes con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información institucional.
Los objetivos específicos de los lineamientos para el uso de usuarios y contraseñas son:
• Presentar a todos los funcionarios y contratistas de la CAM responsables de la asignación, creación y modificación de usuarios y contraseñas las directrices a seguir y verificar que se cumplan a cabalidad con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información de la CAM.
• Concientizar a todos los funcionarios, contratistas o practicantes sobre los riesgos asociados con el uso de las credenciales de acceso (usuario y contraseña) y las consecuencias de exponer de manera inadecuada la identidad ante cualquier tercero, en el entendido que los usuarios y claves asignados a cada funcionarios, contratistas o practicantes son personales e intransferibles.
• Asegurar el correcto manejo de la información privada de la institución.

**Condiciones de Uso del Servicio**

Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada funcionario y contratista es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen. Se permite su uso única y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con la Corporación Autónoma Regional del Alto Magdalena.

Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.
Cuando un funcionario ingresa a la corporación el área de tecnologías de la información le crea las cuentas de los sistemas u aplicativos y equipos de cómputo que el jefe de dependencia o el profesional de talento humano autorice. Para lo cual se establece un usuario y una contraseña temporal que es enviada al correo electrónico del nuevo funcionario para que, de acuerdo a esta política, establezca una nueva contraseña.
La creación de los usuarios se asigna con la primera letra del primer nombre en mayúscula y el primer apellido, este patrón es para la creación de todos los usuarios de todos los sistemas, equipos de cómputo y aplicativos de la Corporación.
El cambio de las contraseñas de los equipos de cómputo de los funcionarios de planta se cambiará mensualmente de manera obligatoria, teniendo en cuenta que los computadores ya están programados y no permite el ingreso pasado el tiempo
Todo funcionario o contratista que se retire de la Corporación de forma definitiva o temporal, deberá hacer entrega formal a quien lo reemplace en sus funciones o a su superior inmediato de las claves de acceso de las cuentas asignadas, con el fin de garantizar la continuidad de las operaciones a su cargo.
Los usuarios y contraseñas de los aplicativos son únicos para cada individuo y solo será válido para recurso tecnológico asignado.
El acceso a los diferentes aplicativos será bloqueado con 5 intentos al digitar la contraseña. El desbloqueo de la contraseña dependiendo el aplicativo, posterior a unas preguntas realizadas por será realizado por el área de tecnologías de la información.
El acceso a la data center, cuarto de equipos, cuarto de cableado y cuarto de UPS, deberá tener acceso restringido a personas no autorizadas, personal del área de sistemas y jefe de oficina de planeación.

**Responsable**

El área de sistemas es responsable de la asignación y administración de las claves de acceso a todos los sistemas y aplicativos con los que cuenta la corporación.
El profesional de talento humano es el responsable de reportar oportunamente el ingreso de los nuevos funcionarios al área de sistemas para la asignación de los usuarios y claves de acceso.
El profesional de talento humano es el responsable de reportar oportunamente al área de tecnologías de la información, los funcionarios que por alguna de las diferentes situaciones administrativas (vacaciones, retiro, comisión) no preste mas sus servicios a la corporación, con el fin de deshabilitar las cuentas que le habían sido asignadas.

***Las políticas enunciadas anteriormente fueron aprobadas en comité institucional de gestión y desempeño del 22 de septiembre de 2020.***