Plan de seguridad y privacidad de la información

CORMACARENA

Tabla de Contenido

GLOSARIO

Integralidad: Propiedad de salvaguardar la exactitud y estado completo de los activos [1]

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera[2].

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados[3].

Irrefutabilidad (no repudio): posibilidad de impedir que un emisor niegue posteriormente que ha enviado un mensaje o realizado una acción, igual el receptor.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

Activos de la información: toda la información de carácter digital o física que representa algún valor por más mínimo que sea, para algún proceso misional, o un proceso de apoyo al interior de la Corporación.

Gestión de información: Conjunto de acciones que tiene como finalidad, garantizar la seguridad, la calidad, la adecuada circulación, la entrega y el almacenamiento de la información.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización.

Licencias de Uso: son los permisos para el uso de la información ambiental o interna de la Corporación, por parte de terceros

Archivo: Es el conjunto de documentos, sea cual fuera su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión. El archivo debe cumplir con las normas y principios de gestión documental como garantizar la posterior consulta de la información

Documento electrónico: Información elaborada y procesada electrónicamente.

---

[1] Ibídem
[2] Ibídem
[3] Ibídem

Expediente Electrónico: El expediente electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan. El expediente electrónico debe garantizar la confidencialidad, integridad y disponibilidad de la información como los procesos de gestión documental de acuerdo a lo establecido en la Ley 1437 de 2011 y el Decreto 2609 de 2012.

Firmas digitales o electrónicas: Son los métodos que permiten darle seguridad a los mensajes de datos de conformidad con la Ley 527 de 1999 y el Decreto 2364 de 2012

Sistemas de información: Es el conjunto integrado de actores, sistemas, políticas, procesos, datos, mecanismos, software, tecnologías involucradas en la gestión, uso de la información en la Corporación.

Esquema de publicación: Es el instrumento de conformidad con el Decreto 103 de 2015, para informar de forma ordenada y controlada la forma como se publica la información en la Corporación.

Ataque Cibernético: Intento de penetración de un sistema información por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones perjudiciales.

Contraseña: Una contraseña o clave (en inglés password) es una formar de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

Desastre: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de equipo de cómputo necesarios para la operación normal dentro de una organización

Incidente: Un incidente de seguridad está definido como un evento que atente contra la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos

Impacto: Consecuencia al materializarse una amenaza

Política: Son instrucciones mandatarias que indican la intención de la alta dirección respecto a la operación de la organización

Gestión del riego: gestión para analizar, valorar y avaluar los riesgos.

Seguridad: Estado de cualquier tipo de información que nos indica que ese sistema está libre de peligro, daño o riesgo

Usuario: persona que solicita un servicio o acceso algún programa, aplicativo o sistema, o

para atender un incidente o problema que se presente con la tecnología informática, sea contratista, servidor público y otro que esté autorizado para prestar servicios para la Entidad.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios de la Corporación, pero por actividades que realizan en la Entidad, deban tener acceso a recursos informáticos.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

Medios Removibles: Componentes Extraíbles que se usa para almacenar información (Discos Duros Externos, memorias y CDs o DVDs)

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

La Dirección General de CORMACARENA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para CORMACARENA la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

La política de Seguridad de la información, estará determinada por las siguientes premisas:

- 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 sus clientes 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 CORMACARENA.
- Garantizar la continuidad del negocio frente a incidentes.

DESCRIPCION DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- CORMACARENA protegerá la información definida de las amenazas originadas por parte del personal.

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

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

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

A continuación, se agrupan las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en CORMACARENA:

POLITICA 1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

Esta política garantizara que existen responsabilidades claramente asignadas en todos los niveles organizacionales para la gestión de seguridad de los activos de la información; se contara con un comité directivo de seguridad de la información conformado por personal idóneo, que apoyara como asesor interno de seguridad, con el objetivo de direccionar y hacer cumplir los lineamientos de la Corporación, en la materia y revisar las posibles incidencias y acciones que se deben tomar.

Todos los funcionarios, contratistas, pasantes y externos con acceso a los activos de información de la Corporación, tendrán el compromiso con la seguridad, cumplir las políticas y normas que la Corporación dicte, así como reportar los incidentes que se puedan detectar

- Los servidores públicos, contratistas, pasantes de la Corporación son responsables de la información que manejan y deberán cumplir con los lineamientos generales y especiales dados por la Corporación y por la Ley para proteger y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.
- Todo servidor público, contratista y/o pasante que labore en la Corporación y detecte el mal uso de la información (copia indebida, transferencia a terceros sin autorización, daño, información oculta, adulteración o incumplimiento de la política), está en la obligación de reportar el hecho a la Oficina de Gestión de servicios de información y tecnologías GSIT y/o Control Interno Disciplinario. El comité directivo de la seguridad de la información la conforma: La Oficina Gestión de Servicios de Información y tecnologías GSIT, Control Interno y Archivo y Correspondencia.
- La Oficina de Control Interno será la responsable de verificar el cumplimiento de las políticas de seguridad de la información.
- La oficina de gestión de servicios de información y tecnologías será la responsable de la actualización de las políticas de seguridad de la información.

POLITICA 2. GESTION DE ACTIVOS

2.1. Identificación y clasificación de Activos

La Corporación realizará la identificación, clasificación y actualización de los activos de

información, de acuerdo a las directrices establecidas en el decreto 103 de 2015, Artículos 37 y 38, este se actualizará de acuerdo a los lineamientos establecidos en el programa de Gestión Documental.

Toda la información de la Corporación, así como los activos donde se procesa y se almacena deberá ser inventariada y asignada a un área responsable; se realizará y se publicará el inventario de activos de información, el índice de información clasificada y reservada y el esquema de publicación de acuerdo a las directrices de la Ley 1712 de 2014 y decreto 103 de 2015.

El inventario de activos de información, el índice de información clasificada y reservada y el esquema de publicación debe ser actualizada cuando se presenten cambios en la información o normatividad que pueda afectarla.

Todo servidor público, contratista o pasante que utilice los sistemas de información, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

2.2. Devolución de activos

Es deber de todo servidor público, contratista y/o pasante que labore en la Corporación, al dejar de prestar sus servicios, entregar toda información del producto del trabajo realizado y hacer entrega de los equipos y recursos tecnológicos en perfecto estado, conforme al

formato PS-GH.2.74.20 Acta entrega puesto de trabajo, de acuerdo a las condiciones establecidas en el contrato o convenio. Una vez retirado, debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante la gestión en la Corporación, directamente o a través de terceros.

2.3. Dispositivos móviles

En los dispositivos móviles de los funcionarios que autoricen, se configura la cuenta corporativa de Google, en dado caso que el celular se extravié desde la Oficina de gestión de servicios de información y tecnología GSIT se puede eliminar la cuenta y datos del celular

2.4. Gestión de Medios Removibles

La Corporación se reserva el derecho de restringir el uso de medios removibles; mientras esté permitido es responsabilidad de los funcionarios, contratistas, pasante y/o terceros que el medio removible conectado esté libre de virus y/o código malicioso, que pueda poner en riesgo la Integridad, confidencialidad y disponibilidad de la información y de los recursos tecnológicos de la Corporación.

2.5. Disposición de activos

- Ningún servidor público de la Corporación está autorizado para realizar labores de mantenimiento y/o reparación de los equipos de cómputo, portátiles, impresoras, escáner, redes, cámaras, GPS y demás dispositivos electrónicos, para tal fin se debe comunicar con la dependencia responsable.
- Los funcionarios deben velar por el buen uso de los recursos tecnológicos asignados, pues son los directamente responsables de cualquier daño. En caso de presentar falla física o lógica se deberá notificar a la Oficina de gestión de servicios de información y tecnología GSIT o al personal responsable de dar servicio a los mismos para que los revisen, corrijan la falla o de ser necesario ordenen la reparación de los mismos.
- Cualquier cambio que se requiera realizar en los equipos de cómputo de la Corporación (cambios de procesador, adición de memoria, discos duros o tarjetas) debe tener previamente una evaluación técnica y autorización de la Oficina de gestión de servicios de información y tecnología GSIT
- La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.
- Los computadores corporativos son asignados a los servidores públicos, con el propósito de mejorar su ambiente de trabajo, mecanizar funciones y procesar información oficial, por lo cual se prohíbe el uso de los mismos para fines personales.
- Los usuarios sólo podrán utilizar los programas con que cuenta el computador que se le asignó, toda modificación del sistema será realizada bajo supervisión de la Oficina de gestión de servicios de información y tecnología GSIT.
- Todo recurso tecnológico cuando cumpla su vida útil ya sea por obsolescencia o daño debe ser reintegrado a la Oficina de gestión de servicios de información y tecnología GSIT, la cual hará el procedimiento correspondiente para la devolución o reintegro al Almacén
- Se debe cerrar las sesiones abiertas de los diferentes Sistemas de Información, Correo Electrónico y demás aplicaciones al finalizar la jornada de trabajo y apagar el computador, estación de trabajo, portátil, etc., a excepción de los servidores y equipos del Centro de Cómputo, los cuales deben permanecer activos las 24 horas.

POLITICA 3. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3.1. Plan de Seguridad y Privacidad de la Información

El comité de seguridad de la información define el plan con el cual la entidad realiza la valoración de los riesgos de los activos de información en el formato PS-GSIT.1.3.74.15 mapa de riesgos de seguridad de la información

POLITICA 4. CONTROL DE ACCESO

En el caso de personas ajenas a la Corporación, la Dirección General, Subdirecciones, Jefes de Oficina o Coordinadores deberán autorizar el acceso indispensable de acuerdo con el trabajo a realizar por estas personas, previa justificación.

En todos los contratos deberá hacerse taxativa la cláusula de confidencialidad, responsabilidad, integridad, buen uso, etc., sobre la información institucional que el contratista en desarrollo de su trabajo deba utilizar.

Los proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

Todo usuario de los sistemas de información deberá tener asignado una cuenta y una contraseña para su utilización, de acuerdo a los estándares que maneja la oficina de gestión de servicios de información y tecnología GSIT, previa solicitud de la Oficina de Talento Humano para funcionarios y del Supervisor, Director o Jefe o Coordinador para contratistas. El uso de la misma es responsabilidad de la persona a la que está asignada, es de carácter personal e intransferible.

La cuenta de usuario administrador dispone a todos los privilegios y características que le permiten administrar completamente el equipo, por tal motivo dicha cuenta debe manejarse únicamente por el personal de la oficina de gestión de servicios de información y tecnología GSIT.

Se debe reportar oportunamente a través del Módulo de talento humano, los eventos relacionados con traslados, vacaciones, ingresos, incapacidades, retiros de funcionarios de la entidad que ameriten activar y/o desactivar códigos de usuario, crear y/o modificar perfiles y roles de otros existentes, activar y/o desactivar servicios, etc.

4.1. Control de acceso con usuario y contraseña:

Todos los accesos y permisos para el uso de los sistemas de información de la entidad deben terminar inmediatamente después de que el servidor público, contratista o pasante cesa de prestar sus servicios a la corporación

4.2. Suministro del control de acceso:

El suministro del control de acceso del usuario de las diferentes aplicaciones que se utilizan en CORMACARENA, depende del tipo de funcionario que lo esté solicitando

4.2.1. Privilegio Alto:

Son aquellos que permiten crear, modificar o borrar información de las aplicaciones y estos privilegios son otorgados personal de oficina de gestión de servicios de información y tecnología GSIT, Directivos, Administrativa y financiera, Archivo y Correspondencia

4.2.2. Privilegio Medio:
Son aquellos que permiten Modificar la información de las Aplicaciones.

4.2.3. Privilegio Bajo:
Son aquellos que permiten leer la información de la aplicación sin ninguna acción adicional. Este privilegio se otorga a todos los funcionarios de la entidad

Si en algún momento un funcionario solicita que su usuario tenga un privilegio alto deberá enviar una notificación a la Oficina de gestión de servicios de información y tecnología GSIT dirigida por el Jefe de área o coordinador indicando el por qué se solicita y por cuanto tiempo.

4.3. Gestión de Contraseñas

4.3.1. Características

Las contraseñas de Windows y los Aplicativos de Docunet, Aranda y Pimisys contienen condiciones para su ingreso.

4.3.2. Periodicidad de Cambio:

La periodicidad de cambio de las contraseñas de las aplicaciones de CORMACARENA se hace mensualmente y es solicitada automáticamente.

4.4. Perímetros de Seguridad

4.4.1 Seguridad de la Oficina de GSIT
La oficina de GSIT cuenta con solo un acceso al área, el cual solo los funcionarios de la oficina tienen las llaves, adicionalmente se cuenta con una cámara que está enfocada al acceso de la oficina.

4.4.2. Seguridad para el acceso al área del Data Center

El acceso al Data Center está limitado solo a los funcionarios del área de Gestión de servicios de información y tecnologías GSIT y son los únicos con la clave de acceso a esta área.
Dado el caso de terceros soliciten el ingreso al Data Center estos deben tener previa autorización y acompañamiento de la Oficina de Gestión de servicios de información y tecnologías GSIT

4.5. Controles de Seguridad para los equipos y software

4.5.1. Firewall

La Corporación cuenta con un Firewall que ejerce el control de las entradas y salidas a

internet y la red interna, cuyas políticas son administradas por la oficina de GSIT y si un funcionario trata de ingresar a una página restringida aparece un mensaje de no acceso al sitio prohibido.

4.5.2. Antivirus

CORMACARENA cuenta con un antivirus para la protección de los equipos de cómputo y servidores con configuraciones para evitar la intrusión de virus por medios Magnéticos Externos y por ataque de internet apoyado el bloqueo adicional del Firewall.

4.5.3. Control de Acceso Remoto y VPN

Las conexiones de control remoto y la VPN son usadas por los funcionarios de GSIT, y son los únicos que brindan el acceso al proveedor dado caso que estos lo necesiten para algún servidor o equipo de la corporación

POLITICA 5. SEGURIDAD DE LOS SERVICIOS INFORMATICOS

5.1. Uso del correo electrónico:

- Los buzones de Correo electrónico asignados a los funcionarios, contratista o dependencias, deben ser usados solamente para el envío o recepción de documentos relacionados con las actividades propias del cumplimiento de las funciones institucionales.
- El usuario titular de la cuenta de correo es el único y directo responsable de todas las acciones y mensajes que se envíen a través de dicha cuenta.
- Los usuarios del servicio de Correo Electrónico de la Corporación no pueden enviar, distribuir, difundir y participar en la propagación de "cadenas" de mensajes o propaganda comercial.
- El Correo Electrónico no se debe utilizar para enviar o distribuir ningún mensaje que pueda ser considerado difamatorio, acosador, explícitamente sexual, o que pueda ofender a alguien con base en su raza, religión, género, nacionalidad, orientación sexual, religión, política o discapacidad.
- Los mensajes masivos solamente podrán ser enviados siempre y cuando se trate de temas de carácter oficial y de interés general evitando en lo posible enviar archivos anexos de gran tamaño y solamente por personas autorizadas para tal fin. Esto debe hacerse con la autorización del Director o Jefe de Oficina o coordinador.
- La Corporación se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico Institucional para cualquier propósito. Para este efecto el funcionario o contratista autorizará a la Corporación para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

- Todo uso indebido del correo electrónico, acarrea suspensión temporal de la cuenta de acuerdo al nivel de la falta cometida.

5.2. Uso y manejo de Internet:

- Los funcionarios de la Corporación no deben descargar archivos que puedan ser nocivos para los sistemas como virus, software espía, programas maliciosos capaces de alojarse en computadores permitiendo el acceso a usuarios externos y atacantes que pongan en riesgo la seguridad de la información, así mismo no deben acceder a sitios desconocidos o de baja confianza, ni aceptar los mensajes sobre instalación de software que ofrezcan las diferentes páginas sin la debida autorización de la Oficina de gestión de servicios de información y tecnología GSIT
- Para evitar la congestión en los canales de comunicación, la Corporación se reserva el derecho de restringir el acceso a ciertas páginas (no oficiales, categorías maliciosas y otras), aplicar limitación de ancho de banda a páginas web, como redes sociales y almacenamiento en la nube no oficial. Si por requerimiento del trabajo se requiere utilizar algunas de las páginas restringidas se debe solicitar la autorización a
- la Oficina de gestión de servicios de información y tecnología GSIT, por medio de comunicado oficial.
- Se prohíbe el uso de software que omita las políticas de seguridad de la información, como proxy, Tune, VPN no autorizada, entre otros

5.3. Uso red inalámbrica:

- La Red Inalámbrica de la Corporación permitirá el acceso solo al personal autorizado, ya sean servidores públicos, contratistas o usuarios invitados.
- La Oficina de gestión de servicios de información y tecnología GSIT; se reserva el derecho de negar el acceso a la Red Inalámbrica en caso que se requiera.

5.4. Escritorios limpios:

- Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, USB, unidades de disco
- Todo servidor público, contratista, pasante y/o colaborador de la Corporación que se retire de su escritorio por un tiempo prolongado, deberá garantizar el bloqueo de la pantalla del computador, PC, estación de trabajo, servidor u otro equipo con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

POLITICA 6. SEGURIDAD DE COMUNICACIONES Y OPERACIONES

- Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Corporación, deberán ser consideradas y tratadas como información confidencial. Su diseño, administración, operación y mantenimiento está a cargo del Proceso de gestión de servicios de información y tecnología GSIT.
- Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la Corporación, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.
- Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar autorizado por la Oficina de gestión de servicios de información y tecnología GSIT
- Los equipos, Servidores, Equipos de Comunicaciones no deben moverse o reubicarse sin la aprobación previa de la Oficina de gestión de servicios de información y tecnología GSIT
- Para seguridad de los equipos tecnológicos, debe tenerse en cuenta que la conexión eléctrica debe realizarse a las tomas de corriente regulada (identificadas con color naranja).
- Los servidores públicos se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que genere caídas de la energía.
- Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no están autorizados para utilizar los recursos informáticos de la Corporación.
- Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad vigentes en la Corporación. La CORPORACION se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos.
- La Oficina de gestión de servicios de información y tecnología GSIT se reserva el derecho de monitorear el tráfico de la red con el fin de garantizar el uso productivo del espacio (ancho de banda), detectar y prevenir fallas, estudiar tendencias de tráfico y detectar y prevenir el acceso no autorizado a los diferentes sistemas de información.

6.1. Adquisición de recursos tecnológicos:

- Toda adquisición de recursos tecnológicos debe estar avalado por el proceso de gestión de servicios de información y tecnología GSIT, quienes

deberán participar en todo el proceso para garantizar las características tecnológicas mínimas, su compatibilidad, confiabilidad y adaptabilidad de los mismos con la infraestructura tecnológica de la entidad.

6.2. Acceso al centro de cómputo:

- Para el ingreso al centro de cómputo del personal encargado de actividades como: mantenimiento del aire acondicionado, instalación y mantenimiento de servidores, instalación y mantenimiento de software, los visitantes y el personal de limpieza deberán estar identificados plenamente en sus actividades, y deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal responsable.
- Todo cambio relacionado con modificación de acceso, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.
- Los centros o áreas cableados que la Corporación considere críticas, deben ser lugares de acceso restringido.

POLITICA 7. SOFTWARE

- Todo software que utilice la Corporación, será adquirido de acuerdo con las. normas vigentes y siguiendo el procedimiento determinado para la Adquisición de software.
- Todo desarrollo, adquisición o modificación de Software debe estar aprobado por el proceso de Gestión de Tecnologías de la Información, quienes deberán participar en todo el proceso para garantizar los estándares requeridos, su seguridad, compatibilidad, confiabilidad y adaptabilidad del mismo.
- Está prohibida la descarga y uso de software no autorizado.
- Los usuarios no pueden descargar y/o emplear archivos de imagen/sonido o similares que estén o puedan estar protegidos por derechos de autor de terceros sin la previa autorización de los mismos.
- Se realizará seguimiento o revisión para ejercer control sobre el uso de Software legalmente adquirido y licenciado por la Corporación.
- Está prohibida la reproducción de cualquier software perteneciente a la Corporación, bien sea que se haya adquirido o desarrollado internamente, para beneficio personal de cualquiera de sus usuarios o de terceras partes.
- La entrega de software desarrollado a otras entidades debe estar autorizado por la Dirección General de la Corporación.
- Antes de que un nuevo sistema se desarrolle o se adquiera, los directivos, Jefes de oficina, coordinadores en conjunto con la Oficina de gestión de servicios de información y tecnología, deberán definir las especificaciones y requerimientos de seguridad necesarios.
- La seguridad debe ser implementada por los analistas, diseñadores y

desarrolladores del sistema desde el inicio del proceso hasta la implementación y entrega en ambiente de producción

POLITICA 8. ALMACENANIIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología de la Corporación deberá ser almacenada y respaldada de acuerdo a lo establecido en el procedimiento "PS- GSIT1.3.72.2 Procedimiento para copias de seguridad de la información", de tal forma que se garantice su disponibilidad.

Los servidores públicos, contratista y pasantes que tiene a cargo equipos de cómputo de la entidad, son responsables de los respaldos de la información almacenada localmente en el computador asignado, la oficina gestión de servicios de información y tecnologías brinda el espacio específico para realizar la copia de seguridad de la información de los diferentes grupos, deberán utilizar la carpeta compartida correspondiente en el servidor ZEUS. La información de los archivos contenidos en las copias de seguridad debe ser única y exclusivamente de uso institucional y no personal. Garantizando el resguardo en forma segura de toda la información digital que dentro del desarrollo de las funciones considere importante y crítica.

POLITICA 9. DOCUMENTOS ELECTRONICOS

Los documentos generados o cargados al Sistema de Gestión Documental, deben incorporar condiciones de seguridad mediante la utilización del formato PDF/A

Las firmas digitales adquiridas por la Corporación y asignadas a los Directivos, Jefes y/o autorizados, son personales e intransferibles y sólo se pueden utilizar para firma de documentos pertinentes a la Corporación. Una vez terminado el vínculo laboral del Director, Jefe y/o autorizados la firma electrónica será cancelada

Todas las comunicaciones externas que se envíen por correo electrónico, deberá ser enviadas a través de correo electrónico institucional.

Los cambios, adiciones y/o modificaciones que se requiera hacer al Sistema De Gestión Documental, serán aprobados y solicitados por el área de Archivo y correspondencia de la Subdirección Administrativa y Financiera.

Establecer estrategias de preservación digital para garantizar que la información almacenada pueda permanecer en el futuro, pese a los cambios tecnológicos u otras causas que puedan alterar la información que contiene, manteniendo su confidencialidad, integridad y disponibilidad.

El tiempo de retención y disposición final de las series documentales generadas en el sistema estarán definidos en las Tablas de Retención Documental de la Corporación.

Los lineamientos y directrices para la conformación de expedientes híbridos y digitalización de documentos se establecerán en el Programa de Gestión Documental de la entidad.

Los Manuales, instructivos, procesos y procedimientos se verificarán y ajustarán de manera periódica, con el fin de garantizar la preservación digital de los documentos

POLÍTICA 10: REGISTRO AUDITORIA

Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la Corporación, como son sistemas de información en ambiente productivo, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar registros de auditoría.

Todos los archivos de auditorías deben proporcionar suficiente información para apoyar el monitoreo, control y seguimiento que se requiera y preservarse por períodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

POLITICA 10. DISPONIBILIDAD DEL SERVICIO DE LA INFORMACIÓN (PLAN DE CONTINUIDAD DEL NEGOCIO)

10.1 Niveles de disponibilidad

El nivel de disponibilidad de los servicios e información que cuenta CORMACARENA supera el 95% ya que están disponibles las 24 horas de los 7 días de la semana durante los 365 días del año

10.2 Planes de recuperación

La recuperación de los sistemas de información de la Corporación es importante porque la mayoría de los procesos dependen de ellos. El Sistema de información financiero y Sistema de mesa de ayuda aplicativos con que cuenta CORMACARENA están virtualizados, lo que facilita la disponibilidad de la información de dichos sistemas, el Sistema de gestión documental está en un servidor físico el cual cuenta con soporte por parte del proveedor para su reinstalación, el servicio de la página web se encuentra en un servidor cloud el cual cuenta con su respectivo Backup realizado por el proveedor.

10.3 Interrupciones

Las interrupciones de los sistemas de información se hacen los fines de semanas o en horarios no laborales para que no sea afectada la disponibilidad de la información, en caso de presentarse la interrupción de algún servicio en horario laboral, se notificará al personal.

10.4 Acuerdos de Nivel de servicio

10.4.1 Sistema de Información Pimisys Unión

Los tiempos de Soporte técnico de manera oportuna a los requerimientos que la entidad realiza a través de medios electrónicos, escritos y telefónicos, se atiende en un tiempo máximo de seis
(6) horas hábiles siguientes durante los 5 días de la semana y en el horario de 8:00 AM a 6:00 PM

10.4.2 Software de Gestión Documental Docunet Web

Los tiempos de soporte, actualización y mantenimiento vigente están de acuerdo a los siguientes parámetros:

A. Severidad 1- Bloqueante: Diagnóstico dentro de las doce (12) horas hábiles siguientes a la recepción del reporte, solución temporal o definitiva, dentro de las treinta y seis (36) horas hábiles siguientes al diagnóstico.

B. Severidad 2- Funcional: Diagnóstico, dentro de las veinticuatro (24) horas hábiles siguientes a la recepción del reporte, solución temporal o definitiva, dentro de las setenta y dos (72) horas hábiles siguientes al diagnóstico.

C. Severidad 3- Presentación Diagnóstico: dentro de las cuarenta y ocho (48) horas hábiles siguientes a la recepción del reporte, Solución temporal o definitiva, en la siguiente versión del producto. En caso de que el grado de complejidad de la falla sea muy alto y su solución temporal o definitiva excede la capacidad operacional del Contratista, CORMACARENA e Innova Systems SAS se pondrán de acuerdo para definir la fecha de solución a la falla. Definida la solución, el Contratista, proporcionará al cliente una sola copia del software, en el medio adecuado. CORMACARENA distribuirá la reparación o solución de trabajo a los Programas Soportados conforme sea necesario. Para la solución definitiva de cualquier nivel de severidad, Innova Systems SAS y CORMACARENA, acordaran la fecha de entrega.

10.4.3 Aranda

Los tiempos de atención de soporte técnico a la entidad son de cinco (5) días hábiles una vez enviada la solicitud de ejecución de cualquier servicio contratado, el horario de ejecución de todos los servicios es de 5 x 8 (lunes a viernes de 8:00 am a 6:00 pm) durante la vigencia del contrato de soporte. El Soporte se realizará mediante conexión de escritorio remoto usando software especializado. a. Una respuesta directa a los usuarios con respecto a las interrogantes relativas a la funcionalidad u operación de los Programas Soportados; b. Una respuesta directa a los usuarios con respecto a los problemas o deficiencias de los Programas Soportados; c. Un diagnóstico de los problemas o deficiencias de los Programas Soportados; y d. Una solución a los problemas o deficiencias de los Programas Soportados. El Soporte, asesoría y capacitación al software Aranda vía telefónica, por internet o mediante conexión de escritorio remoto usando software especializado.

10.5 Periodicidad:

La revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad en materia de seguridad de la información se aborda a través de la gestión de los riesgos y oportunidades de acuerdo a lo establecido en el PEV-GCI.1.1.73.2 PROCEDIMIENTO ADMINISTRACION DE RIESGOS Y OPORTUNIDADES, el cual contempla la periodicidad tanto para la identificación y actualización de los riesgos y oportunidades como la periodicidad para el seguimiento y monitoreo de los mismos. Este seguimiento y monitoreo es realizado por parte del proceso Gestión de Servicios de Información y Tecnología y la Oficina de Control Interno.

POLITICA 11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Gestión de los incidentes y eventos de seguridad de la información de Cormacarena. Inicia con la detección del incidente de seguridad de la información continua con la estrategia de contención y termina con el análisis post-incidente tal como tal como se indica en la GUIA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

POLITICA 12. POLITICA Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS

Los funcionarios de la entidad deben tener en cuenta el documento PE-GP.1.3.68.1 MANUAL DE POLITICAS Y PROCEDIMIENTOS PROTECCION DE DATOS, en la cual se establece el manejo y el trato que se da a la información que acoge o publica la entidad.

POLITICA 13. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La capacitación se realizará como se establece en el plan de comunicación y sensibilización de la cultura y seguridad informática.

Es responsabilidad del Comité Seguridad de la información evaluar, actualizar, verificar y socializar las políticas de seguridad de la información, conforme a esto, el presente documento tendrá una revisión anual, o antes en caso de ser necesario.

Esta política debe ser socializada de acuerdo a las actualizaciones que puedan llevarse a cabo, y publicarla en la intranet y pagina web de la Corporación para conocimiento de todo el personal objetivo e incluirla en el proceso de inducción de nuevos funcionarios y contratistas cada vez que talento Humano las programe.

El Comité Seguridad de la información a través de los funcionarios responsables de administrar la infraestructura de las Tecnologías de la Información y las Comunicaciones será el responsable de efectuar el seguimiento al cumplimiento de la Política de Seguridad de la Información con el fin de verificar y controlar que se esté aplicando adecuadamente. Los casos de incumplimiento serán reportados a la Oficina de Control Disciplinario Interno, para ser aplicadas las sanciones a que haya lugar.