



**MANUAL DE POLÍTICAS DE SEGURIDAD
DE LA INFORMACIÓN**

Código: M-PSI-001


Versión: 04

Página 1 de 26

Proceso: Sistemas

Fecha de Aprobación: Enero 30 de 2023

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 2 de 26
	Proceso: Sistemas	Fecha de Aprobación: marzo 2022

CONTENIDO

INTRODUCCIÓN	4
1. OBJETIVO	5
2. ALCANCE	5
3. MARCO NORMATIVO.....	5
4. DEFINICIONES	6
5. LÍNEA BASE DE LA POLÍTICA.....	8
5.1. ROLES Y RESPONSABILIDAD	8
5.2. CUMPLIMIENTO	8
5.3. EXCEPCIONES.....	9
5.4. REVISIÓN DE LA POLÍTICA.....	9
6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.....	9
7. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	9
8. POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS.....	10
8.1. DEL PROCESO DE SELECCIÓN, EJECUCIÓN Y TERMINACIÓN DEL EMPLEO O CONTRATOS 10	
8.2. ACUERDO DE CONFIDENCIALIDAD PARA PROVEEDORES.....	10
8.3. CONFIDENCIALIDAD PERSONAL CONTRATISTA.....	10
8.5. ENTRENAMIENTO EN SEGURIDAD DIGITAL.....	11
8.6. TERMINACIÓN LABORAL	11
8.7. MEDIDAS DISCIPLINARIAS.....	11
8.8. CAMBIO DE CARGO Y/O RESPONSABILIDADES.....	11
9. POLÍTICAS DE GESTIÓN DE ACTIVOS.....	12
9.1. INVENTARIO DE ACTIVOS.....	12
9.2. CLASIFICACIÓN DE LA INFORMACIÓN.....	12
9.3. USO ACEPTABLE DE LOS ACTIVOS.....	13
9.4. USO DEL CORREO ELECTRÓNICO INSTITUCIONAL	13
9.5. SALIDA DE ACTIVOS	14
9.6. EQUIPOS PORTATILES PERSONALES	14
10.1. SOLICITUD DE NUEVOS INGRESOS	15
10.2. RESPONSABILIDADES DE LOS USUARIOS.....	15



MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Código: M-PSI-001


Versión: 04

Página 3 de 26

Proceso: Sistemas

Fecha de Aprobación: marzo 2022

10.3.	ADMINISTRACIÓN Y USO DE CONTRASEÑA	16
10.4.	CONTROL DE ACCESOS REMOTOS.....	16
11.	POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL	17
11.2.	RESGUARDO Y PROTECCIÓN DE LA INFORMACIÓN DE EQUIPOS DE CÓMPUTO	17
11.3.	SEGURIDAD EN ÁREAS DE TRABAJO	18
12.1.	PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS	18
12.2.	MANTENIMIENTO DE EQUIPO	19
12.3.	PÉRDIDA DE EQUIPO.....	19
12.4.	USO DE DISPOSITIVOS ESPECIALES O EXTRAIBLES	19
12.5.	DAÑO DEL EQUIPO	19
12.6.	BAJA DE LOS EQUIPOS	20
12.7.	USO DE EQUIPOS FUERA DE LA CORPORACIÓN	20
12.9.	ADMINISTRACIÓN DE LA CONFIGURACIÓN	20
12.10.	EQUIPO DESATENDIDO	21
13.	POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES TECNOLÓGICAS	21
13.1.	CONTROLES CONTRA CÓDIGO MALICIOSO.....	21
13.2.	POLÍTICAS DE RESPALDO Y RECUPERACIÓN	21
13.3.	MONITOREO DEL USO DE LOS RECURSOS TECNOLÓGICOS	22
13.4.	REGISTROS DE EVENTOS	22
13.5.	GESTIÓN DE CAMBIOS Y CAPACIDAD	22
13.6.	ACEPTACIÓN DE SOFTWARE.....	22
13.7.	INSTALACIÓN DE SOFTWARE.....	23
14.	POLÍTICAS PARA LA SEGURIDAD DE LA RED Y COMUNICACIONES	23
14.1.	USO DE REDES SOCIALES	23
14.2.	INTERNET	23
15.	POLÍTICAS DE SEGURIDAD CON PROVEEDORES	24
16.	POLÍTICA DE GESTIÓN DE INCIDENTES	24
18.	POLÍTICAS DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA	25
18.1.	DERECHOS DE PROPIEDAD INTELECTUAL	25
18.2.	REVISIONES DEL CUMPLIMIENTO.....	25
18.3.	VIOLACIONES DE SEGURIDAD INFORMÁTICA	25
20.	HISTORIAL DE CAMBIOS	26

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 4 de 26
	Proceso: Sistemas	Fecha de Aprobación: marzo 2022


INTRODUCCIÓN

Considerando los retos de la digitalización en cada uno de los procesos y los retos de ser entidades abiertas y transformadas para los ciudadanos y otras partes interesadas se hace necesario afrontar los retos y riesgos que supone la exposición al ciberespacio y los ecosistemas digitales hiperconectados. Además, de afrontar los retos de la industria 4.0 para seguridad digital que en Colombia a través del ministerio de tecnologías de la información – MINTIC ha propuesto una serie de lineamientos para la implementación de marcos de seguridad y privacidad de la información MSPI con el fin de generar elementos articuladores entre servicios digitales, componentes eficientes internos de las entidades y finalmente generar la confianza y seguridad digital de la información.

De esta manera la política de seguridad informática de, emerge como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permitan IT cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso con la entidad, conscientes de que la seguridad informática se fundamenta en la existencia de un conjunto de políticas que brinden instrucciones claras y sean el soporte de los diferentes procesos de la entidad involucrando a la alta dirección, con el objeto que las normas y procedimientos tienen la finalidad de definir, especificar y elaborar los requisitos y procedimientos de seguridad para la gestión de la protección de los activos de la información de la empresa, de una manera consistente y efectiva dentro del marco de la seguridad de los sistemas informáticos que son los siguientes:

- ✓ Garantizar los principios de la seguridad de la información como son la confidencialidad, privacidad, integridad y disponibilidad. Además de valores como la trazabilidad y no repudio de eventos y sistemas.
- ✓ Proteger los activos de información de la corporación, considerándolos como los elementos más valiosos de la entidad.
- ✓ Cumplir con las legislaciones y reglamentación vigente para la seguridad y privacidad.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 5 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

1. OBJETIVO

Establecer las medidas organizacionales, técnicas, físicas y legales, necesarias para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental considerando los riesgos del ecosistema digital y los retos emergentes de ciberseguridad.

2. ALCANCE

Esta Política es aplicable a funcionarios y contratistas, que usen activos de información que sean propiedad de la Corporación.

3. MARCO NORMATIVO

CONSTITUCIÓN POLÍTICA DE COLOMBIA. ARTÍCULO 74

Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley. El secreto profesional es inviolable.

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.

LEY 1266 DE 2008


Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 1581 DE 2012

Por la cual se dictan disposiciones generales para la protección de datos personales.

LEY 1273 DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 6 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

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.

DECRETO 2609 DE 2012

Por medio de la cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

DECRETO 2573 DE 2014

Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

DECRETO 103 DE 2015

Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

DECRETO 1008 DE 2018: (cuyas disposiciones se compilan en el Decreto 1078 de 2015, “Decreto Único Reglamentario del sector TIC”, específicamente en el capítulo 1, título 9, parte 2, libro 2), forma parte del Modelo Integrado de planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores.

RESOLUCIÓN 500 DE MARZO 10 DE 2021 DEL MINTIC: 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.

DECRETO 338 DE MARZO DE 2022 DEL MINTIC: Se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital

NTC ISO/IEC 27001 DE 2013

Esta norma internacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización.

4. DEFINICIONES


Aceptación del riesgo: Decisión de asumir un riesgo.

Activo: Es todo aquello que tiene valor para la organización (Información, Software, Hardware, Servicios, imagen institucional, Personas) y necesite protegerse.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Autenticidad: Permite verificar la identidad del generador de la información, evitando la suplantación de identidad.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 7 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

Ciberespacio: Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Contraseña: Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información. Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Gestión documental: Conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación.

Gestión de Incidentes: Conjunto de acciones y procesos tendientes a brindar a las organizaciones fortalezas y capacidades para responder en forma adecuada a la ocurrencia de incidentes de seguridad informática que afecten real o potencialmente sus servicios.

Inalterabilidad: Garantizar que un documento electrónico generado por primera vez en su forma definitiva no sea modificado a lo largo de todo su ciclo de vida, desde su producción hasta su conservación temporal o definitiva.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar a seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de la información.

Medios de almacenamiento removibles: comprende los discos duros externos, memorias USB, tarjetas SD, etc.


No repudio: el emisor no podrá negar el conocimiento de un mensaje de datos ni los compromisos adquiridos a partir de éste.

Política: Toda intención y directriz expresada formalmente por la Dirección de la entidad.

Riesgo. Combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Sistema de gestión de la seguridad de la información - SGSI: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar. Hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 8 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Recursos TIC: Las Tecnologías de la información y la comunicación - TIC, comprende la red local, internet, página web, correo electrónico, intranet, sistemas de información, carpetas compartidas y demás recursos tecnológicos de apoyo al logro de los objetivos de la Corporación.

Usuario: Toda persona que utilice los sistemas de información de la entidad debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

Vulnerabilidad. Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más Amenazas.


5. LÍNEA BASE DE LA POLÍTICA

5.1. ROLES Y RESPONSABILIDAD

- ✓ **Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo - GIT.** Configurar, hacer uso y seguimiento de las Políticas de Seguridad de la Información como parte de sus herramientas de gestión, definir los estándares, procedimientos y lineamientos que garantice su cumplimiento.
- ✓ **Directivos.** Cada subdirector, jefe de dependencia o supervisor de contrato debe velar por que su personal a cargo funcionarios y contratistas den cumplimiento a las políticas de seguridad de la información.
- ✓ **Oficina de Personal.** Incluir en el Plan de Capacitación anual de inducción y reinducción las políticas de seguridad de la información y uso de las TIC, así como garantizar que los funcionarios firmen el acuerdo de confidencialidad e informar a la oficina GIT los cambios realizados en la planta de personal.
- ✓ **Oficina de secretaría general Cuentas.** Incluir en los contratos de prestación de servicios una cláusula donde se relacionen las políticas de confidencialidad de la información y el cumplimiento de las políticas.
- ✓ **Usuarios.** Respetar y dar cumplimiento a cabalidad de las políticas de seguridad de la información definidas.
- ✓ **Sistema de Gestión Integrado.** Apoyar a la oficina GIT en la generación de procedimientos, formatos e instructivos tendientes a mejorar la seguridad de la información, así como tener en cuenta las políticas de seguridad de la información en la creación, modificación y aprobación de nuevos procedimientos y formatos.

5.2. CUMPLIMIENTO

El cumplimiento de las Políticas de Seguridad de la Información es obligatorio para todos los funcionarios y contratistas/proveedores de la Corporación, su incumplimiento podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 9 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

por las autoridades competentes.

5.3. EXCEPCIONES

Las excepciones a cualquier cumplimiento de Política de Seguridad de la Información deben ser aprobadas por Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo, la cual debe requerir autorización de la Dirección General, la Subdirección correspondiente. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas.

5.4. REVISIÓN DE LA POLÍTICA

Las políticas de seguridad de la información del presente manual serán revisadas anualmente o cuando se identifiquen cambios en la estructura, objetivos o alguna condición que afecte la política, con el fin de asegurar que se encuentren ajustadas a los requerimientos de la Entidad.


6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Dirección General de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER – CAS, reconoce la información como un activo fundamental para la prestación de los servicios y la toma de decisiones, por lo cual declara su compromiso con la preservación de la confidencialidad, integridad y disponibilidad de sus activos de información, la planeación, implementación, operación y mejora continua del marco de seguridad y privacidad – MSPI, la articulación estratégica de los objetivos de la corporación, los lineamientos nacionales y regulatorios aplicables a la entidad.

De esta manera la Corporación se compromete a identificar sus activos y gestionar los riesgos asociados a los mismos considerando las diferentes amenazas internas y externas del ciberespacio, además de promover la cultura de seguridad digital entre funcionarios, contratistas y proveedores.

7. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

- ✓ **Asegurar los activos de información** de la Corporación Autónoma Regional de Santander en su confidencialidad, integridad y disponibilidad contra amenazas internas o externas, deliberadas o accidentales.
- ✓ **Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información y ciberseguridad** articulados con la legislación o recomendaciones vigentes.
- ✓ **Fortalecer la cultura de seguridad de la información** en los funcionarios, contratistas y terceros de la Corporación Autónoma Regional de Santander.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 10 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

8. POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

Todo usuario servicios o elementos informáticos al ingresar como funcionario o contratista aceptan las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información de la Corporación Autónoma Regional de Santander -CAS-, así como el estricto cumplimiento de las Políticas de seguridad mencionadas en este documento.

8.1. DEL PROCESO DE SELECCIÓN, EJECUCIÓN Y TERMINACIÓN DEL EMPLEO O CONTRATOS


Toda vez que se requiera vinculación de personal de planta o contratistas, se debe realizar una revisión de los antecedentes de acuerdo con los requisitos del cargo y el tipo de información a la cual tendrá acceso.

8.2. ACUERDO DE CONFIDENCIALIDAD PARA PROVEEDORES

- ✓ Dentro de los contratos de proveedores se deben incluir las cláusulas de confidencialidad de la información.
- ✓ Los supervisores de contratos y jefes inmediatos son responsables de velar por el cumplimiento de las cláusulas de confidencialidad.
- ✓ Los funcionarios deben firmar el formato “Acuerdo de Confidencialidad **F-PTH-011**” en el momento de su vinculación a la Corporación.

8.3. CONFIDENCIALIDAD PERSONAL CONTRATISTA

Cualquier información intercambiada, facilitada o creada entre el contratista y la Corporación Autónoma Regional de Santander - CAS en el transcurso de su vinculación a la Corporación, será mantenida en estricta confidencialidad. La parte receptora correspondiente sólo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte titular de la información confidencial. Se considera también información confidencial: a) Aquella que haya sido declarada como confidencial por el responsable o propietario de la información, b) La que no sea de fácil acceso, c) Aquella información que esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial. d) aquella que por su naturaleza sea considerada como confidencial. No habrá deber alguno de confidencialidad en los siguientes casos: a) Cuando la parte receptora tenga evidencia de que conoce previamente la información recibida; b) Cuando la información recibida sea de dominio público y, c) Cuando la información deje de ser confidencial por ser revelada por el propietario. El presente acuerdo tendrá una duración indefinida y terminará cuando las partes de común acuerdo lo determinen.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 11 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

8.5 ENTRENAMIENTO EN SEGURIDAD DIGITAL

- ✓ Todos los funcionarios nuevos deberán ser informados sobre las políticas de seguridad de la información en la capacitación de inducción.
- ✓ Todos los funcionarios y contratistas deben recibir entrenamiento y toma de conciencia en seguridad de la información.
- ✓ Se deben construir planes de sensibilización para funcionarios y contratistas para la seguridad de la información y ciberseguridad orientados a la identificación de amenazas y buenas prácticas en estos temas.

8.6. TERMINACIÓN LABORAL


- ✓ Todo funcionario o contratista que se desvincula de la corporación debe realizar la devolución de los activos de información a su cargo y solicitar firma del “Formato de paz y salvo **F-PCT- 005**” en la Oficina de gestión de información ambiental y tecnologías de apoyo, con el fin de realizar la deshabilitación inmediata de las cuentas de acceso a la red y a los sistemas de información, igualmente deshabilitar la tarjeta de acceso físico a la entidad.
- ✓ Todo funcionario o contratista que se desvincula de la Corporación debe entregar a su jefe inmediato o supervisor de contrato la copia de respaldo de los documentos que soportan el cumplimiento de sus funciones en caso de funcionarios o la ejecución de los alcances del contrato en caso de contratista.

8.7. MEDIDAS DISCIPLINARIAS

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la Corporación, o las contempladas en la Ley 1273 de 2009. En caso de presentarse violación a las políticas de seguridad de la información se debe informar a la oficina de control interno disciplinario para los fines disciplinarios correspondientes.

8.8. CAMBIO DE CARGO Y/O RESPONSABILIDADES

- ✓ La Oficina de Personal debe informar a la Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo las novedades que se presenten en cuanto cambio de cargo y/o responsabilidades de los funcionarios con el fin de ajustar los perfiles de usuario asignados.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 12 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

- ✓ Cada Jefe de Dependencia debe solicitar mediante el formato de “Solicitud de servicios TIC **F-PGT-004**” ante la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo, la modificación de los derechos de acceso a los recursos tecnológicos de la corporación con el finde permanecer adecuados a las nuevas responsabilidades del cargo.

9. POLÍTICAS DE GESTIÓN DE ACTIVOS


9.1. INVENTARIO DE ACTIVOS

Todos los activos de información de la corporación deben estar debidamente identificados incluyendo el responsable, su ubicación, criticidad (valorado según la confidencialidad, integridad y disponibilidad) y clasificación.

9.2. CLASIFICACIÓN DE LA INFORMACIÓN

Con el fin de asegurar que la información recibe el nivel apropiado de protección, de acuerdo con su importancia para la Entidad, se ha adoptado la siguiente clasificación para toda la información que genere la Corporación en desarrollo de sus funciones:

- 1. Pública:** Es toda información que la Entidad genere, obtenga, adquiera, o controle que ha sido declarada, legalmente o por su propietario, de conocimiento público y accesible a cualquier persona. Ej. Plan de acción de la Entidad, datos abiertos, entre otros.
- 2. Uso interno:** Información que es utilizada y generada por el personal de la Entidad en cumplimiento de sus labores, y que sin ser confidencial ni reservada no es publicada para conocimiento de terceros, sin embargo, podrá ser conocida mediante solicitud a la Entidad. Ej. Memorandos, correos, reportes para entidades, manuales, documentos de trabajo.
- 3. Confidencial:** Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, potencial de fraude o requisitos legales. Solo puede ser vista por un grupo de personas o un área en particular. La divulgación a terceros solo se hace bajo autorización de un nivel directivo o autoridad competente. Ej. Configuración de equipos, resultados de evaluación de riesgos de seguridad de la información, procesos disciplinarios, etc.
- 4. Reservada:** Es aquella información que estando en poder o custodia de la Entidad, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 13 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

consagrados en el artículo 19 de la ley 1712 de 2014.

Los propietarios o responsables de la información (Funcionario o cargo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida y los tiempos de retención asociados a la misma) deben clasificar cada uno de los documentos o información generada en el ejercicio de sus funciones.

9.3 USO ACEPTABLE DE LOS ACTIVOS


Es deber de todos los funcionarios y contratistas de la corporación hacer uso adecuado y responsable de los activos de información a su cargo preservando la confidencialidad, integridad y disponibilidad de estos. Los recursos TIC dispuestos por la Corporación para el uso por parte de los funcionarios y Contratistas autorizados deben emplearse sólo con fines laborales.

9.3.1 PROHIBICIONES EN EL USO DE LOS ACTIVOS DE INFORMACIÓN

- a. Incluir en correos electrónicos, documentos, imágenes, boletines, redes sociales institucionales u otras formas de comunicación, contenido que razonablemente puede considerarse una amenaza, acoso, u ofensa para cualquier persona, o que viole la política colombiana sobre acoso laboral y abuso de autoridad.
- b. Ofrecer acceso a los recursos de las TIC o poner a disposición de personas datos sin autorización previa para acceder a ellos.
- c. Alterar, ocultar, suprimir o compartir datos sin autorización.
- d. Uso de redes de intercambio de archivos (Ares, BitTorrent, Spotify u otros software) a fin de obtener ilegalmente material con derechos de autor y la instalación de software que no ha sido aprobado para su uso.
- e. Acceder a internet a visualizar, compartir y descargar material pornográfico, videos, música, películas o escuchar emisoras online.
- f. Copia no autorizada de material protegido por derechos de autor propiedad de la CAS.
- g. Generar o enviar correos electrónicos a nombre de otro usuario sin autorización o suplantándolo.
- h. Burlar los mecanismos de seguridad, autenticación, autorización o de auditoría, de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
- i. Usar equipos o servicios informáticos para actividades diferentes a las encomendadas en los manuales de funciones, contratos o delegaciones de jefes inmediatos.

9.4. USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

- ✓ Toda comunicación por correo electrónico de origen laboral debe ser tramitada desde el correo

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 14 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

institucional, está prohibida la utilización del correo personal para los fines laborales.


- ✓ Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la CAS, a menos que cuente con la autorización de la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.
- ✓ Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la CAS.
- ✓ Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.
- ✓ Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- ✓ Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas de la corporación.
- ✓ Esta prohibido el uso de correos institucionales para el registro en servicios de mensajería automática, boletines, redes sociales u otras bases de carácter no institucional.
- ✓ La cuenta de correo institucional no debe ser inscrita en páginas o sitios publicitarios ajenos a los fines laborales

9.5. SALIDA DE ACTIVOS

- ✓ Los equipos personales de los funcionarios, contratista y/o visitantes se deben registrar tanto en el ingreso como en la salida de las instalaciones de la Corporación Autónoma Regional de Santander -CAS-
- ✓ Los equipos de cómputo de escritorio, las computadoras portátiles, y cualquier activo de tecnología de información propiedad de la CAS, podrán salir de las instalaciones de la Corporación únicamente con la autorización de salida del área de Almacén, anexando la nota de salida del equipo debidamente firmada por el Coordinador de la oficina o cargo equivalente en las dependencias de la CAS.

9.6. EQUIPOS PORTATILES PERSONALES

Es responsabilidad del propietario del equipo portátil salvaguardar la información perteneciente a la CAS que se encuentre almacenada en su equipo personal derivada de sus labores en la corporación.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 15 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

10. POLITICAS DE GESTION DE ACCESOS Y USUARIOS

- ✓ El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de la CAS debe ser proporcionado, con base en el principio de la "necesidad de saber" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.
- ✓ Cada usuario debe solicitar a la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo por medio del formato Solicitud de servicios TIC, la asignación de permisos para el acceso a los recursos TIC de la Corporación, el cual debe estar firmado por el jefe inmediato.

Los permisos de acceso asignados deben ser retirados o modificados cada vez que se produzca un cambio en la planta de personal o la terminación de un contrato de prestación de servicios.

- ✓ La Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo realizará revisión de los derechos de acceso de los usuarios a intervalos regulares con el fin de mantenerlos ajustados.


10.1. SOLICITUD DE NUEVOS INGRESOS

Todo el personal nuevo de la Corporación deberá ser notificado por cada jefe de Dependencia o Supervisor del contrato mediante el formato de "Solicitud de servicios TIC **F-PGT-004**" ante la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo para ser creado como usuario en las bases de datos requeridas, asignar tarjeta de acceso físico de acuerdo al perfil del cargo u objeto contractual y dar acceso a los recursos TIC solicitados.

La Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo validará frecuente mente al menos cada semestre las cuentas asignadas en los sistemas de información con el fin de realizar depuraciones o evitar accesos no autorizados de acuerdo con nuevos funcionarios, retiros o cambio de roles en la entidad. En caso de inhabilitación se enviará memorando o comunicación a cada dependencia con el fin de revisar dichos accesos.

10.2. RESPONSABILIDADES DE LOS USUARIOS

- ✓ Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica de la CAS, por lo cual deberá mantenerlo de forma confidencial.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 16 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

- ✓ Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario. Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el usuario y contraseña de otros usuarios.

10.3. ADMINISTRACIÓN Y USO DE CONTRASEÑA

La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

Cuando un usuario olvide o bloquee su contraseña, deberá acudir personalmente la Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo para que se le proporcione una nueva contraseña.

Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y/o lógico y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

Se deben seguir las siguientes recomendaciones con el fin de evitar la utilización de contraseñas débiles:

- Evitar utilizar la misma contraseña siempre en todas las aplicaciones.
- Evitar utilizar secuencias básicas de teclado (por ejemplo: “qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)
- No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
- No utilizar como contraseña las fechas especiales, número de identificación ni nombre de seres queridos.
- Evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
- No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.


Las contraseñas deben tener una longitud mínima de 8 caracteres y estar compuesta por tres de las siguientes características con el fin de crear contraseñas robustas, difíciles de descifrar:

- Utilizar números.
- Utilizar letras Mayúsculas.
- Utilizar letras Minúsculas.
- Incluir algún carácter especial (@\$/#_-.).

Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarla inmediatamente.

10.4. CONTROL DE ACCESOS REMOTOS

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y la Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo, así también la Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo será la única autorizada para este tipo de accesos.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 17 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023


11. POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

11.1. CONTROLES DE ACCESO FÍSICO

- ✓ El sistema de seguridad física de la Corporación debe permitir el acceso a las instalaciones y áreas restringidas de la CAS sólo a personas autorizadas, en busca de la salvaguarda de los activos de la Corporación.
- ✓ Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la CAS, a menos que se tenga el visto bueno del dueño de la información y de la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo y la autorización del director general de la CAS o su equivalente en las dependencias de la Corporación.
- ✓ Las tarjetas de acceso físico a la corporación son personales e intransferibles, en caso de pérdida o robo debe informarse inmediatamente en la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.
- ✓ Cada tarjeta de acceso debe ser configurada según el perfil del usuario, con lo cual sólo tendrá acceso a las áreas permitidas.
- ✓ El usuario es responsable del uso que se proporcione a la tarjeta de acceso asignada.
- ✓ La tarjeta de acceso asignada quedará inhabilitada automáticamente al finalizar el contrato y ésta deberá ser devuelta a la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.

11.2. RESGUARDO Y PROTECCIÓN DE LA INFORMACIÓN DE EQUIPOS DE CÓMPUTO

- El usuario deberá reportar de forma inmediata a la Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.
- El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.
- Es responsabilidad del usuario evitar en todo momento la fuga de la Información de la CAS que se encuentre almacenada en los equipos de cómputo que tenga asignados.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 18 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023


11.3. SEGURIDAD EN ÁREAS DE TRABAJO

El centro de cómputo de la CAS es un área restringida, por lo que sólo el personal autorizado por la Oficina de Gestión de la información ambiental y Tecnologías de Apoyo puede acceder a él.

12. POLITICA DE GESTIÓN DE EQUIPOS DE COMPUTOS Y OTROS DISPOSITIVOS

12.1. PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS

- Los usuarios no deben mover, reubicar o abrir los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de estos sin la autorización de la Oficina de Gestión de la información ambiental y Tecnologías de Apoyo, en caso de requerir este servicio deberá solicitarlo.
- El equipo de cómputo asignado a funcionarios o contratistas deberá ser para uso exclusivo de las funciones de la CAS.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro asignado en el servidor o en la carpeta "Mis Documentos" ya que las otras están destinadas para archivos de programa y sistema operativo. Se recomienda no guardar información en el escritorio ya que se perderá en caso de mal funcionamiento del computador y adicionalmente le resta velocidad de procesamiento al equipo.
- Mientras se opera cerca del equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitoro de la torre.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados o trozados al colocar otros objetos encima o contra ellos, en caso de que no se cumpla solicitar un reacomodo de cables con el personal de la Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo.
- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 19 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

lugares físicos de trabajo, éstos deberán ser notificados a la Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo.

12.2. MANTENIMIENTO DE EQUIPO

Únicamente el personal autorizado por la Oficina de Gestión de la información ambiental y Tecnologías de Apoyo podrá llevar a cabo el mantenimiento preventivo y/o correctivo de los equipos informáticos.

Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

12.3. PÉRDIDA DE EQUIPO

El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien en los casos de robo, extravío o pérdida de este.

El usuario deberá dar aviso inmediato a la Oficina de Gestión de la información ambiental y Tecnologías de Apoyo y almacén de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

12.4. USO DE DISPOSITIVOS ESPECIALES O EXTRAIBLES


El uso de los grabadores de discos compactos (unidades de CD/DVD) es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

Todos los medios utilizados para almacenamiento de las copias de respaldo o para almacenamiento de información en tránsito deben permanecer resguardados de forma segura evitando su acceso por parte de personas no autorizadas.

12.5. DAÑO DEL EQUIPO

Se levantará un reporte de incumplimiento de las políticas de seguridad contra el usuario que provoque algún daño por maltrato, descuido o negligencia a un equipo de cómputo o cualquier recurso de tecnología de información.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 20 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

12.6. BAJA DE LOS EQUIPOS

La Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo debe emitir concepto técnico de cada uno de los equipos susceptibles a dar de baja, determinando el estado del activo con el fin de establecer su destino final.

Se debe realizar una primera destrucción de los medios de almacenamiento de información antes de ser entregado a la empresa de disposición de residuos electrónicos.

12.7. USO DE EQUIPOS FUERA DE LA CORPORACIÓN

Los usuarios son responsables de la seguridad de los equipos y la información propiedad de la CAS utilizados fuera de las instalaciones de la Corporación, por lo tanto, se deben tomar medidas de precaución, tales como no descuidar el equipo en lugares públicos, no conectarse a redes públicas, no almacenar en el equipo información confidencial o reservada de la Entidad.


12.8 EQUIPOS PERSONALES Y MOVILES.

La Corporación en su permitirá el uso de dispositivos móviles en la red interna siempre y cuando se cumplan con los criterios de seguridad de la información adecuados para evitar infecciones o algún otro incidente en la red de la corporación, por lo tanto, es responsabilidad de funcionarios y contratistas garantizar que equipos portátiles, tabletas, teléfonos u otros dispositivos conectables se encuentre con las condiciones siguientes:

- Cuenten con un software antivirus actualizado
- Cuenten con software debidamente licenciado
- Cuenten con parches actualizados y versiones de sistema operativos soportadas
- No se tenga instalado software que atente al buen uso de activos de información descrito en el presente manual.

12.9. ADMINISTRACIÓN DE LA CONFIGURACIÓN

- ✓ Los usuarios de las dependencias de la CAS no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP, SSH), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la CAS, sin la autorización de la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.
- ✓ El personal que designe la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo son los

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 21 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

únicos autorizados para configurar o modificar la configuración de los recursos TIC de la Corporación.

12.10. EQUIPO DESATENDIDO

- ✓ Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla previamente instalados y autorizados por la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo, cuando no se encuentren en su lugar de trabajo deben cerrar la sesión de trabajo evitando así el acceso no autorizado a la información.
- ✓ Se debe mantener el escritorio limpio de documentación confidencial y medios de almacenamiento removibles con el fin de evitar pérdida o hurto de información.


13. POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES TECNOLOGICAS

13.1. CONTROLES CONTRA CÓDIGO MALICIOSO

- ✓ Para prevenir infecciones por virus informático, los usuarios de la CAS no deben hacer uso de software que no haya sido proporcionado y validado por la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.
- ✓ Los usuarios de la CAS deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado e instalado por la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.
- ✓ Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo para la detección y erradicación del virus.
- ✓ Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la CAS.
- ✓ Debido a que algunos virus son extremadamente complejos, ningún usuario de la CAS debe intentar erradicarlos de las computadoras.

13.2. POLÍTICAS DE RESPALDO Y RECUPERACIÓN

La Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo administrará los sistemas e infraestructura para realizar copias de seguridad periódicas de las bases de datos, aplicativos, página web y demás información contenida en los servidores de la Corporación. De igual manera es deber de cada área

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 22 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

usuaria validar que las políticas de respaldo con frecuencia y retención sean adecuadas a los procesos de la entidad.

La Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo deberá garantizar la correcta ejecución de los respaldos, así como los ejercicios de recuperación de la información en los medios de respaldo asignado con el fin de validar el proceso e integridad de los datos.

Cada uno de los usuarios es responsable por la realización periódica de las copias de respaldode la información que a diario generan en cumplimiento de sus labores y que es importante para la continuidad de la ejecución de los procedimientos.

13.3. MONITOREO DEL USO DE LOS RECURSOS TECNOLÓGICOS

La Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo a través de reportes de monitoreo de la red puede evidenciar el mal uso de los recursos tecnológicos y de ser necesario se encuentra en plena facultad de restringir el acceso a los recursos con el fin de preservar la seguridad de los activos de la corporación.

13.4. REGISTROS DE EVENTOS

Las actividades que realicen los usuarios en la infraestructura de Tecnología de Información de la CAS deben ser registradas y protegidas contra alteración y acceso no autorizado, los cuales se deben revisar regularmente con el fin de detectar violaciones a la seguridad de la información.


13.5. GESTIÓN DE CAMBIOS Y CAPACIDAD

Los cambios realizados a los sistemas de información deben ser controlados, para lo cual se debe solicitar el cambio a la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo siguiendo el procedimiento PSI-004 Procedimiento Control de Cambios del Software.

Para cada cambio o adquisición de recursos TIC se deben identificar los requisitos de capacidad necesarios con el fin de adaptar el sistema para garantizar su eficacia.

13.6. ACEPTACIÓN DE SOFTWARE

Se deben establecer los requisitos de seguridad para los sistemas de información nuevos o actualizaciones, los cuales deben estar definidos, acordados, documentados y probados; sólo se acepta el software después de cumplir con los requisitos acordados.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 23 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

13.7. INSTALACIÓN DE SOFTWARE.

Los usuarios que requieran la instalación de software que no sea propiedad de la CAS, deberán justificar su uso y solicitar su autorización a la Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo por medio del servicio de Soporte TI de la intranet indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación. Esto con el fin de evitar sanciones por parte de auditorías pertinentes.

Se considera una falta grave el que los usuarios instalen cualquier tipo de software (programa) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la CAS, que no esté autorizado por la Oficina de Gestión de la Información Ambiental y Tecnologías de Apoyo.

14. POLÍTICAS PARA LA SEGURIDAD DE LA RED Y COMUNICACIONES


Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la CAS, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

14.1. USO DE REDES SOCIALES

No está permitido el uso de redes sociales y mensajería instantánea desde los equipos de cómputo de la CAS por razones de seguridad, los usuarios que requieran acceso a estos servicios deberán solicitarlo a la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo por medio de la intranet – Soporte TI debidamente justificado.

14.2. INTERNET

- ✓ El acceso a internet provisto a los usuarios de la CAS es exclusivamente para las actividades relacionadas con las necesidades de las funciones y/o objeto contractual que desempeña.
- ✓ Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la CAS, en caso de necesitar una conexión especial a Internet, ésta tiene que ser notificada y aprobada por la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.
- ✓ Los usuarios del servicio de navegación en Internet, al usar el servicio están aceptando que:

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 24 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

- Serán sujetos de monitoreo de las actividades que realiza en Internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización de la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.
- Saben que el tráfico de la red esta priorizado en función de su contenido y del perfil del usuario evitando el mal uso de la herramienta y la congestión en la misma por el hecho de bajar películas, videojuegos, jugar en línea y el uso de audio y video streaming (Netflix, u otra plataforma similar) que consume recursos de red provocando pérdidas de conexión.
- La utilización de Internet es para el desempeño de su función y/o objeto contractual en la CAS y no para propósitos personales.

15. POLÍTICAS DE SEGURIDAD CON PROVEEDORES

Se deben establecer, acordar y documentar los requisitos de seguridad con los proveedores con el fin de mitigar los riesgos asociados con el acceso de proveedores a los activos de la Corporación de acuerdo con el presente manual.


16. POLÍTICA DE GESTIÓN DE INCIDENTES

- ✓ El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo por medio del servicio de Soporte TI de la intranet lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.
- ✓ Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático lo deberá notificar a la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.
- ✓ Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la CAS debe ser reportado a la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.

17. POLÍTICAS DE GESTIÓN DE LA CONTINUIDAD Y REDUNDANCIA

La Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo coordinará las acciones y procesos para documentar políticas y procedimientos para la continuidad de servicios informáticos alojados en el centro de datos o centros alternos, además es deber de la alta dirección garantizar los recursos necesarios para cumplir con este lineamiento.

Se debe de igual manera, trabajar en la identificación de procesos de negocios y definir el impacto y prioridades para

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 25 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

las necesidades de la continuidad y alta disponibilidad de servicios.

18. POLÍTICAS DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

La Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de la información en general.

18.1. DERECHOS DE PROPIEDAD INTELECTUAL

Todo material desarrollado por funcionarios o contratistas en desarrollo de sus funciones o la ejecución de los alcances del contrato en caso de contratista, en horario laboral y con la información suministrada por la Corporación son propiedad de la CAS.

18.2. REVISIONES DEL CUMPLIMIENTO

La Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo realizará acciones de verificación del cumplimiento del presente manual de políticas de seguridad de la información.


La Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de seguridad de personal.

Los jefes y responsables de los procesos establecidos en la CAS deben apoyar las revisiones del cumplimiento de los sistemas con las políticas de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

18.3. VIOLACIONES DE SEGURIDAD INFORMÁTICA

Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática.

Ningún usuario de la CAS debe probar o intentar probar fallas de la seguridad informática o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Oficina de Gestión de Información Ambiental y Tecnologías de Apoyo.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código: M-PSI-001
		Versión: 04
		Página 26 de 26
	Proceso: Sistemas	Fecha de Aprobación. Enero 30 2023

No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) malicioso diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de la CAS.

20. HISTORIAL DE CAMBIOS

Versión	Fecha de Elaboración	Cambios realizados
01	21/11/2014	Emisión inicial del documento
02	27/02/2015	Modificación del contexto de los numerales; 5.1, 8.2, 8.3, 8.5, 8.6, 8.7, 8.8, 9.3, 9.4, 11, 12.1, 12.4, 13.2, 13.8, 13.13, 14, 14.1, e inclusión de los numerales; 8.4, 9.2, 12.9, 13.3, 13.4, 13.6.
03	12/09/2016	Modificación del logotipo "Responsabilidad Ambiental, Compromiso que nos Une".
04	01/30/2023	Alineación a legislación vigente y cambio de estructura del documento al estándar ISO27001:2013, consideraciones de riesgos y conceptos de ciberespacio/ciberseguridad, actualización de logos y disposiciones de continuidad.