MANUAL DE LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CORPORACION PARA EL DESARROLLO SOSTENIBLE DEL NORTE Y EL ORIENTE AMAZÓNICO -CDA-

Inírida–Guainía

2026

Version1

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

TABLA DE CONTENIDO

Contenido

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

INTRODUCCION

La Corporación para el desarrollo sostenible del norte y oriente amazónico, dando cumplimiento a su misión y en cumplimiento de su objeto, requiere implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de la información, por lo tanto se establece que la información es un activo fundamental para el desarrollo de las actividades de Gobierno, en razón a que es una herramienta de gran importancia para la toma de decisiones, motivo por el cual, la Corporación CDA, está comprometida a proteger los activos de información de la entidad (Empleados, información y entorno laboral), orientando sus esfuerzos a la preservación de las operaciones de gobernabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información de la Corporación CDA. Estas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de Seguridad de la Información, basadas en la norma ISO 27001/2022 y al modelo de seguridad y privacidad de la información de la estrategia Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

OBJETIVO

Presentar en forma clara y coherente las pautas, directrices y reglas que conforman la política de seguridad que deben conocer y cumplir todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Corporación CDA, con el fin de garantizar la seguridad de los activos de información y minimizar los riesgos.

ALCANCE

La Política de seguridad de la Información cubre los aspectos de privacidad, acceso, autenticación, mantenimiento y divulgación relacionados con cualquier activo de información, que conlleven a disponer guías y controles que deben ser
Aplicables para todos los aspectos administrativos y de control y deben ser cumplidos por los directivos, funcionarios, contratistas y terceros, que laboren o tengan relación con la Corporación para el desarrollo del norte y oriente amazónico CDA,
Para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad del presente manual. Los usuarios tienen la

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección General.

APLICABILIDAD DE LA POLITICA

Las políticas del Sistema de Seguridad de la Información - SGSI aplican y son de obligatorio cumplimiento para la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, Coordinadores, funcionarios, contratistas, y en general a todos los usuarios que permitan el cumplimiento de los propósitos generales de La corporación para el desarrollo sostenible del norte y oriente amazónico CDA.

REQUISITOS LEGALES

Con el objeto de mitigar los riesgos relacionados con la autenticidad, la integridad, la disponibilidad, el no repudio, la confidencialidad y la trazabilidad de la información, se tiene que cualquier incidente que viole el marco normativo legal vigente en Colombia, en materia de políticas de seguridad de la Información estará sujeto, entre otras, a lo establecido en las siguientes disposiciones legales:

1-Marco normativo de buenas prácticas para el tratamiento de información.

- **DECRETO 555 DEL 9 DE ABRIL 2022:** "Por el cual se adiciona la sección 6 del título 1, parte 2, libro 2 del Decreto 1072 de 2015, único Reglamentario del Sector Trabajo, y se reglamenta el artículo 17 de la Ley 2069 de 2020, y la Ley 2021 de 2021 y se regula el trabajo remoto.
- **RESOLUCIÓN 746 DEL 11 DE MARZO 2022:** "Por el cual establece el Modelo de Seguridad y Privacidad de la información y se definen lineamientos adicionales a los establecidos en la resolución No. 500 de 2021.
- **DECRETO 338 DEL 8 DE MARZO DE 2022:** "Por la cual se adiciona el Título 21 de la parte 2 del Libro del Decreto único 1078 de 2015, reglamentario del sector de tecnologías de la información y las comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea un Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".
- **DIRECTIVA PRESIDENCIAL 02 DEL 24 DE FEBRERO DE 2022:** Reiteración de la política pública en materia de seguridad digital.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **EL DECRETO 767 DE 2022:** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- **DECRETO REGLAMENTARIO 103 DE 2015:** compilado en el Decreto Único Reglamentario 1080 de 2015, por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura. Tiene por objeto: "reglamentar la Ley 1712 de 2014, en lo relativo a la gestión de la información pública".
- **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", la cual tiene por objeto "… regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información".
- **DECRETO REGLAMENTARIO 1377 DE 2013:** "Por el cual se reglamenta parcialmente la Ley 1581 de 2012", Compilado y derogado parcialmente por el Decreto 1081 de 2015. Tiene como objeto: "…reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales".
- **NTC/ISO 27002:2022:** recomendaciones y buenas prácticas para la gestión de seguridad de la información.
- **NTC-ISO-IEC 27001:2022**:"Sistemas de Gestión de Seguridad de la Información".
- **ISO/IEC 27032:2023:** Ciberseguridad– Directrices para la seguridad de Internet. Esta norma se centra en la relación entre la seguridad en Internet, la seguridad web, la seguridad de redes y la ciberseguridad en general.
- **LEY 1581 DE 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales. De conformidad con su artículo 1, tiene por objeto "(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".
- **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".

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

2-Marco normativo sancionatorio.

- **RESOLUCIÓN 500 DEL 2021**: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- **RESOLUCIÓN 1519 DE 2020:** "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".
- **LEY 1952 DE 2019:** "Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario."
- **LEY 1273 DE ENERO 5 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".
- **LEY 734 DE 2002:** "por la cual se expide el Código Disciplinario Único".

TÉRMINO Y DEFINICIONES.

A continuación de definen los términos técnicos.

- **Activo**: Recurso del sistema de información o cualquier elemento que tenga valor para la organización.
- **Activo de información:** Todo aquel elemento lógico o físico que conforme cualquiera de s los sistemas de información de la institución. Ejemplo: base de datos, sistemas operacionales, redes de datos, sistema de información y comunicaciones, documentos impresos, Formularios y recursos humanos.
- **Acción correctiva:** Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.
- **Acción preventiva:** Medida de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Aceptación del Riesgo:** Decisión de aceptar o que puede tolerarse el riesgo asociado a cualquier situación bajo el supuesto de que se cuenta con un plan de acción para afrontarlo.
- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Administrador del Sistema:** Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está dirigida por la Gerencia de informática y se realizará por conducto de las Coordinaciones de la misma.
- **Administrador de Correo:** Persona responsable de solucionar problemas en el correo electrónico, responder preguntas a los usuarios y otros asuntos en un servidor.
- **Análisis de riesgos:** Proceso sistemático que permite identificar y determinar el impacto o grado de vulnerabilidad de los activos de la organización.
- **Administración de riesgos:** Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.
- **Ataque Cibernético:** Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado, por lo general con intenciones insanas y perjudiciales.
- **Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.
- **Brecha de Seguridad:** deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.
- **Buzón:** También conocido como cuenta de correo, es un espacio exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la Corporación CDA.
- **Control:** Mecanismo para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.
- **Control detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
- **Control disuasorio:** Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.
- **Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
- **Chat:** Comunicación simultánea y sincronizada entre dos o más personas a través de Internet.
- **Centro de Cómputo**: También conocido como Centro de Procesamiento de Datos, o Data Center es una instalación que se encarga del procesamiento de datos e información de manera sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras (Hardware) y programas (Software) necesarios para cumplir con dicha tarea.
- **Checklist (Lista de Chequeo):** Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.
- **Confidencialidad:** Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo a las personas autorizadas.
- **Cuentas de Correo**: Son espacios de buzones para la recepción, envió y almacenamiento de mensajes de correo electrónico en internet.
- **Correo Electrónico:** También conocido como E-mail, es un servicio de red que permite a los usuarios enviar y recibir textos, imágenes, videos, audio, programas, a través de internet.
- **Cómputo forense:** También llamado informática forense, computación forense, análisis forense digital o exanimación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

- **Contraseña o Password:** Es una forma de autenticación privada, compuesta por un conjunto de números, letras y caracteres, que permiten al usuario tener acceso a un computador, a un archivo y/o a un programa.
- **Disponibilidad:** Es la garantía de poder acceder a los activos de la información cuando sea necesario, por personal autorizado.
- **Dispositivo móvil:** Elemento electrónico de tamaño pequeño, con capacidades de procesamiento de datos, conexión a Internet y memoria Son ejemplos de estos: celulares inteligentes, tabletas y portátiles.
- **Tecnología:** Es el conjunto de conocimientos técnicos, científicamente ordenados, que permiten diseñar y crear bienes, servicios que facilitan la adaptación al medio ambiente y la satisfacción de las necesidades esenciales y los deseos de la humanidad. Aunque hay muchas tecnologías muy diferentes entre sí, es frecuente usar el término tecnología en singular para referirse al conjunto de todas, o también a una de ellas. La palabra tecnología también se puede referir a la disciplina teórica que estudia los saberes comunes a todas las tecnologías, y en algunos contextos, a la educación.
- **Instalaciones:** son el conjunto de redes y equipos fijos que permiten el suministro y operaciones de los servicios que ayudan a los edificios a cumplir las funciones para las que has sido diseñados.
- **El Tele trabajador:** es la persona que el marco de la relación laboral dependiente utiliza las tecnologías de la información y comunicación como medio o fin para realizar su actividad laboral fuera del local del empleador, en cualquiera de las formas definidas por la ley.
- **Evento de Seguridad de La información:** Ocurrencia identificada de una situación de sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.
- **Firewall:** Dispositivo que permite bloquear o filtrar el acceso en redes de comunicación.
- **Firma Digital**: La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Hacker:** Persona dedicada a realizar entradas no autorizadas a los sistemas, por medio de redes de comunicación como Internet, con el objeto de encontrar vulnerabilidades en los sistemas.
- **Host:** Termino usado en informática para referirse a los computadores conectados a la red, que proveen y/o utilizan servicios de ella. Los usuarios deben utilizar hosts para tener acceso a la red.
- **Incidente de Seguridad de la información:** Es la identificación de la ocurrencia de un hecho que está relacionado con los activos de información, que indica una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.
- **Infraestructura de Procesamiento de Información:** Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.
- **Integridad:** La propiedad de salvaguardar la exactitud y completitud de los activos de información.
- **Internet:** Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.
- Intranet: Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que es de uso interno.
- **LAN:** (Local Area Network). (Red de Área Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.
- **Malware:** Código malicioso o cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.
- **Pasante:** Prácticas profesionales que desarrollan personas que están culminando sus estudios o que recién han egresado de la carrera.
- **Red:** Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.
- **Sistema de Gestión de Seguridad de la información:** SGSI La parte del sistema total de gestión, basada en un enfoque de riesgo de negocios, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. Seguridad: Mecanismos de control que evita el uso no autorizado de recursos.
- **Seguridad de la Información:** Son medidas preventivas que incluyen factores de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, aceptabilidad y confiabilidad de la información.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Servidor:** Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.
- **Servidor de Correo:** Dispositivo y/o aplicación informática, cuya función es gestionar el tráfico de ficheros a través del correo electrónico, su misión es la de almacenar, en su disco duro, los mensajes que envía y que reciben los usuarios.
- **Sistema Operativo:** Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora, servidor o dispositivo móvil.
- **Teletrabajo:** Es una forma de organización laboral, que se efectúa en el marco de un contrato de trabajo o de una relación laboral dependiente, que consiste en el desempeño de actividades remuneradas utilizando como soporte las tecnologías de la información y la comunicación -TIC para el contacto entre el trabajador y empleador sin requerirse la presencia física del trabajador en un sitio específico de trabajo. (LEY 1221 DE 2008).
- **Troyano:** Es un programa con una determinada función o utilidad, pero que contiene código oculto para ejecutar acciones no esperadas por el usuario.
- **Usuario:** en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la corporación CDA, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la corporación CDA y a quienes se les otorga un nombre de usuario y una clave de acceso.
- **Virus:** software malicioso que tiene por objeto alterar el normal funcionamiento de una computadora, reemplazando así programas ejecutados, sin la autorización ni el conocimiento del usuario.
- **VPN (Virtual Private Network):** es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.
- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

COMPROMISO DE LA DIRECCIÓN.

La Alta Dirección de la Corporación para el desarrollo sostenible del norte y oriente amazónico CDA, aprueba el Manual de Políticas de Seguridad de la Información, como muestra de su compromiso y apoyo hacia la gestión de seguridad de la información que se lleva a cabo en la Institución, mediante el SGSI y el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital, antes llamado Gobierno en Línea.

La Alta Dirección de la Corporación CDA demuestra su compromiso de apoyo a la política de seguridad de la información y las comunicaciones destinando los recursos suficientes y adecuados para implementar y mantener las políticas contenidas en este manual y a realizar, entre otras acciones:

- La revisión y aprobación del Manual de Políticas de Seguridad de la Información para la Institución.
- La promoción activa de una cultura de seguridad de la información en los servidores públicos, contratistas, proveedores y ciudadanía en general, que tengan acceso a los sistemas de información, repositorios e instalaciones físicas de la corporación.
- La divulgación de este manual
- La verificación del cumplimiento de las políticas aquí mencionadas.

POLITICAS, PROCEDIMIENTOS Y CONTROLES.

Políticas de seguridad de la información.

Las Políticas de Seguridad de la Información, surge como una herramienta institucional para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la corporación CDA, sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

Directrices.

- Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información, los cuales estarán a cargo de la Oficina de Control Interno.
- Todo aplicativo informático o software que se adquiera e instale debe ser licenciado y debe ser aprobado por el Líder del proceso de Gestión de las TICS en concordancia con la política de adquisición de bienes de la corporación de acuerdo con lo definido en el proceso respectivo.
- La corporación CDA, debe contar con un firewall o dispositivo de seguridad perimetral para la conexión a Internet o para la conexión a otras redes en outsourcing o de terceros.
- La conexión remota a la red de área local de la Corporación CDA, debe realizarse a través de una conexión VPN segura suministrada por la corporación, la cual debe ser aprobada, registrada y auditada, a excepción de los casos que autorice el proceso de Gestión de las TICS.
- Los jefes de área o dependencia (Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, Coordinadores) deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la corporación CDA.
- La corporación CDA, en caso de tener un servicio de transferencia de archivos, deberá realizarlo empleando protocolos seguros. Cuando el origen sea de la corporación CDA hacia entidades externas, la Corporación establecerá los controles necesarios para preservar la seguridad de la información. Cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad. En todo caso se deben revisar y proponer controles en concordancia con las políticas de seguridad de la información de la corporación. Los resultados de la revisión de requerimientos de seguridad se documentarán y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de seguridad de la corporación CDA.
- Se establecerá un Comité de Seguridad Informática y de Sistemas de la Corporación el cual definirá de acuerdo a la clasificación de la información, que datos deben ser cifrados y dará las directrices necesarias para la implementación de los respectivos controles (dispositivos a emplear, mecanismos de administración de claves, políticas de uso de sistemas de cifrado de datos).

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Política de clasificación de la información.

Objetivo: Asegurar que la información recibe el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley.

Directrices:

- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la Corporación CDA como por ejemplo:
- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información transmitida vía oral o por cualquier otro medio de comunicación.
- Los usuarios responsables de la información de la Corporación CDA, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
- Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como “Valiosa” para la Corporación CDA.

Políticas específicas para el proceso de Gestión de las TICS.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información de la corporación CDA, por parte de los funcionarios y contratistas del proceso de Gestión de las TICS de la corporación.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Directrices:

- El personal de la corporación CDA, con acceso a equipos y sistemas de información no debe dar a conocer sus claves y/o usuarios a terceros sin previa autorización del Jefe de Oficina de Planeación o del Profesional Especializado Líder del proceso de Gestión de las TICS.
- Los usuarios y claves de los administradores de sistemas y del personal de Gestión de las TICS son de uso personal e intransferible.
- Los funcionarios y contratistas de Gestión de las TICS deben emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación que posea la corporación de acuerdo al rol asignado.
- Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Jefe de Oficina Asesora de Planeación y el Profesional Especializado Líder del proceso Gestión de las TICS.
- Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la corporación. Ej.: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
- Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
- Los funcionarios del proceso de Gestión de las TICS no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Jefe de la Oficina Asesora de Planeación o del Profesional Especializado de Gestión de las TICS y el registro en el formato correspondiente.
- Los funcionarios del proceso de Gestión de las TICS no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
- Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la corporación. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la corporación.
- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
- Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.

Política de retención y archivo de datos.

Objetivo: Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Directrices.

- La política de retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en la Corporación CDA de acuerdo a las tablas de retención documental – TRD.
- Las reglas y los principios generales que regulan la función archivística del Estado, se encuentran definidos por la Ley, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.
- La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la administración e implantación de programas de gestión de documentos.

Política de disposición de información, medios y equipos.

Objetivo: Contrarrestar las interrupciones en las actividades de la Corporación y proteger sus procesos críticos contra los efectos de fallas importantes en los

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

sistemas de información o contra desastres y propender por su recuperación oportuna.

- Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento; para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

Política de respaldo y restauración de información.

Objetivo: Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla.

Directrices:

- La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como discos duros externos, almacenamiento en la nube, Memorias USB, Servidores de respaldo y DVD.
- Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación) y el administrador del sistema de respaldo, es el responsable de realizar los respaldos periódicos.
- Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.
- Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.
- Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.
- Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones de la sede principal de la Corporación CDA.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información o debe ser requerido por el funcionario que así lo requiera, para poder continuar con su trabajo.
- Semanalmente los administradores de infraestructura de red de la Corporación CDA, verificarán la correcta ejecución de los procesos de backup utilizado.
- El Profesional Especializado Líder del proceso de Gestión de las TICS debe mantener un inventario actualizado de las copias de respaldo de la información, de los aplicativos y los sistemas de información de la Corporación CDA.
- Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada. El borrado seguro se ejecuta cuando al borrar un archivo o formatear un dispositivo de almacenamiento, alguna utilidad de borrado escribe ceros (o) sobre el archivo, no permitiendo que éste se pueda recuperar posteriormente.
- Es responsabilidad de cada dependencia mantener depurada la información de las carpetas de almacenamiento virtuales para la optimización del uso de los recursos de almacenamiento que entrega la corporación CDA, a los usuarios.

Política de gestión de activos de información.

Objetivo: Establecer la forma en que se logra y mantiene la protección adecuada de los activos de información.

Directrices:

- **Inventario de activos de información**: La corporación para el desarrollo sostenible del norte y oriente Amazónico CDA mantendrá un inventario o registro actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el proceso de Gestión de las TICS.
- **Propietarios de los activos de información**: La corporación para el desarrollo sostenible del norte y oriente amazónico CDA, es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la Corporación, que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología de información y comunicaciones (TIC).

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Política de uso de los activos de información.

Objetivo: Lograr y mantener la protección adecuada de los activos de información mediante la asignación de estos, a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Directrices:

- Los activos de información pertenecen a la corporación CDA y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
- Los usuarios deberán utilizar únicamente los programas y equipos autorizados por el Líder del proceso de Gestión de las TICS.
- La corporación para el desarrollo sostenible del norte y oriente amazónico CDA. proporcionará a los usuarios los equipos informáticos y los programas instalados en ellos. Los datos/información creados, almacenados y recibidos, serán propiedad de la Corporación. Los funcionarios solo podrán realizar backup de sus archivos personales o de información pública. Para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por la Corporación CDA. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.
- Periódicamente, Gestión de las TICS efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considera como una violación a las Políticas de Seguridad de la Información de la corporación CDA.
- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados al Profesional Especializado Líder del proceso de Gestión de las TICS, previa autorización del Jefe inmediato, con su correspondiente justificación para su respectiva viabilidad.
- Estarán bajo custodia del Profesional Especializado Líder del proceso Gestión de las TICS los medios magnéticos/óptico/electrónicos (discos, memorias USB, DVD, CD u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso. Adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y las contraseñas de administración de los equipos informáticos, sistemas de información o aplicativos.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- En caso de ser necesario y previa autorización del Comité de Seguridad Informática y de Sistemas de la corporación CDA, los funcionarios podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.
- Los recursos informáticos de la corporación CDA , no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos. Estos actos incluyen: envió de correo electrónico masivo con fines no institucionales y práctica de juegos en línea.
- Los funcionarios no podrán Instalar software en cualquier equipo de la Corporación.
- Los funcionarios no podrán Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo que pertenezca a la corporación CDA.
- Los funcionarios no podrán Modificar, revisar, transformar o adaptar cualquier software propiedad de la corporación CDA.
- Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la corporación CDA.
- Copiar o distribuir cualquier software de propiedad de la corporación CDA.
- El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad o uso indebido que tenga conocimiento y este a su vez al Líder del Proceso de Gestión de las TICS.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.
- Ningún usuario deberá acceder a la red o a los servicios TIC de la Corporación CDA, utilizando una cuenta de usuario o clave de otro usuario. En casos excepcionales deberá mediar una autorización expresa y limitada en el tiempo que permita identificar quien estaba utilizando el usuario y clave.
- Cada usuario es responsable de asegurar que el uso de redes externas, tal como Internet, no comprometa la seguridad de los recursos informáticos de la Corporación CDA . Los funcionarios del proceso de Gestión de las TICS de la corporación CDA, son responsables de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la corporación. Esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Todo archivo o material recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas destructivos antes de ser instalados en cualquier equipo que haga parte de la infraestructura tecnológica de la corporación CDA.
- Todos los archivos provenientes de equipos externos a la corporación CDA, deben ser revisados para detección de virus antes de su utilización dentro de la red de la Corporación.

Política de uso de Internet.

Objetivo: Establecer unos lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

Directrices:

- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
- No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la corporación CDA o que representen peligro para la corporación como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la corporación.
- El acceso a contenidos no permitidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del Comité de Seguridad Informática y de Sistemas de la Corporación CDA.
- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

Política de uso de mensajería instantánea y redes sociales.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información de la corporación CDA, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios que cumplan con los propósitos generales de la Corporación CDA.

Directrices:

- El uso y administración de los servicios de mensajería instantánea y redes sociales como canales oficiales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.
- No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.
- La información que se publique o divulgue por redes sociales o cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la Corporación CDA, que sea creado a nombre personal, como redes sociales, X®, facebook®, youtube® likedink® o blogs, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Política de uso de discos de red o carpetas virtuales.

Objetivo: Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Directrices:

- Para que los usuarios tengan acceso a la información ubicada en los discos de red, se debe registrar la solicitud a través de servicios compartidos especificando el acceso y permisos, correspondientes al rol y funciones a desempeñar, al Líder del proceso Gestión de las TICS de la corporación CDA. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
- La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
- Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la corporación o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en los discos de red.
- Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.
- Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial que atenten contra la integridad e imagen de la corporación CDA.
- La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo del Líder del proceso Gestión de las TICS de la corporación CDA.
- La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de la sede principal de la Corporación, estará a cargo del Líder del proceso Gestión de las TICS de la Corporación CDA.

Política de uso de impresoras y del servicio de Impresión.

Objetivo: Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Directrices:

- Los documentos que se impriman en las impresoras de la corporación CDA deben ser de carácter institucional.
- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Líder del proceso de Gestión de las TICS de la corporación CDA quien revisará y evaluará el estado de la impresora. En caso de que el servicio de impresoras sea prestado por un tercero, es este quien deberá hacer la revisión, mantenimiento y posterior reparación.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Política de uso de puntos de red de datos (red de área local – LAN).

Objetivo: Asegurar la operación correcta y segura de los puntos de red.

Directrices:

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Corporativos estándar. Los equipos de uso personal, que no son de propiedad de la corporación CDA, solo tendrán acceso a servicios limitados destinados al trabajo institucional, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el Líder del proceso Gestión de las TICS.
- La instalación, activación y gestión de los puntos de red es responsabilidad del proceso de Gestión de las TICS.
- Cualquier persona o funcionario que intente conectar un dispositivo electrónico, ya sea pc, Tablet o celular, a la red de la corporación CDA, sin previa Autorización del líder TIC, tendrá sanciones disciplinarias el cual será reportado a los entes de control pertinentes.

Políticas de seguridad del centro de datos y centros de cableado.

Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Directrices:

- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado.
- El Líder del proceso de Gestión de las TICS debe garantizar que el control de acceso al centro de datos de la corporación CDA y contar con dispositivos electrónicos de autenticación o sistema de control biométrico.
- El proceso de Gestión de las TICS deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.
- La limpieza y aseo del centro de datos estará a cargo de la señora de servicios generales y debe efectuarse en presencia de un funcionario o contratista del proceso de Gestión de las TICS de la corporación CDA. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

- En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.
- El centro de datos debe estar provisto por Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
- Pisos elaborados con materiales no combustibles.
- Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por el Comité de Seguridad Informática y de Sistemas y exclusivamente con fines institucionales.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado de la corporación CDA
- Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

Políticas de seguridad de los Equipos.

Objetivo: Asegurar la protección de la información en los equipos.

Directrices:

- **Protecciones en el suministro de energía:** A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el encargado del líder TIC de la corporación CDA.
- **Seguridad del cableado:** Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas. Deben existir planos que describan las conexiones del cableado. El acceso a los centros de cableado (Racks), debe estar protegido.
- **Mantenimiento de los Equipos:** La corporación CDA debe mantener contratos de soporte y mantenimiento de los equipos críticos. Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento. Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.
- Los equipos que requieran salir de las instalaciones de la corporación CDA, para reparación o mantenimiento, deben estar debidamente autorizados y se debe garantizar que en dichos elementos no se encuentra información establecida como crítica en la clasificación de la información de acuerdo a los niveles de clasificación de la información. Para que los equipos puedan salir fuera de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos, teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de la corporación CDA.
- Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información,

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

utilizando herramientas para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

- Ingreso y retiro de activos de información de terceros: El retiro e ingreso de todo activo de información de propiedad de los funcionarios y visitantes de la corporación CDA, utilizados para fines personales y corporativos, se realizará mediante los procedimientos establecidos por la Administración. La corporación CDA no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica pública.
- El retiro e ingreso de todo activo de información de los visitantes y contratistas que presten servicios a la corporación CDA, será registrado y controlado en las porterías del edificio. El personal de vigilancia de recepción verificará y registrará las características de identificación del activo de información. El traslado entre dependencias de la corporación CDA de todo activo de información, está a cargo del área Administrativa, para el control de inventarios.

Política de escritorio y pantalla limpia.

Objetivo: Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Directrices:

- El personal de la corporación CDA debe conservar su escritorio libre de información, propia de la corporación, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- El personal de la corporación CDA debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
- No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Política de uso de correo electrónico.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información de la corporación CDA, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

Directrices:

- Esta política define y distingue el uso de correo electrónico aceptable/apropiado e inaceptable/inapropiado y establece las directrices para el uso seguro del servicio.
- **Servicio de correo electrónico:** Permite a los usuarios de la corporación CDA, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones.
- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
- Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la corporación. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de la corporación CDA se consideran bajo el control de la corporación.
- Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la corporación CDA y no debe utilizarse para ningún otro fin.
- El envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red, no está autorizado.
- No está autorizado, el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la corporación CDA.
- Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de la corporación CDA, su cuenta de correo será desactivada.
- El tamaño del buzón de correo electrónico estará determinado por las capacidades del servicio contratado y por el rol desempeñado por el usuario en la Corporación CDA. En todo caso no podrá ser superior al definido como “tamaño máximo” por el Líder del proceso Gestión de las TICS de la Corporación CDA.
- Cada área deberá solicitar la creación, modificación o cancelación de las cuentas electrónicas de los funcionarios y contratistas.
- Las cuentas de correo electrónico son propiedad de la Corporación CDA, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

la corporación, ya sea como personal de planta, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Corporación CDA y no debe utilizarse para ningún otro fin.

- Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por la Corporación CDA.
- Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Corporación.
- Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe notificar a la oficina de sistemas de la corporación CDA.
- El único servicio de correo electrónico autorizado en la corporación es el correo corporativo con dominio @cda.gov.co asignado por Gestión de las TICS de la Corporación CDA.

Política de control de acceso.

Objetivo: Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática de la corporación CDA, así como el uso de medios de computación móvil**.**

Directrices:

- La corporación CDA proporcionará a los funcionarios y contratistas (personas naturales) todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles personales, tales como: computadores portátiles, tablets, enrutadores, agendas electrónicas, celulares inteligentes, access point, que no sean autorizados por el líder del proceso Gestión de las TICS de la Corporación CDA. En los casos en que se requiera, el jefe inmediato o el supervisor del contratista, solicitará el acceso a la red de datos y/o a los servicios de internet de la corporación.
- La corporación CDA suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Solo usuarios designados por el Líder del proceso Gestión de las TICS de la Corporación CDA estarán autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la corporación.
- Todo trabajo que utilice los servidores de la corporación CDA con información de la corporación, debe ser autorizado por el Líder del proceso Gestión de las TICS de la corporación CDA. No se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del líder TICS.
- La conexión remota a la red de área local de la corporación CDA debe ser hecha a través de una conexión VPN segura suministrada por la corporación CDA, la cual debe ser aprobada, registrada y auditada. En todo, caso, otro tipo de conexión deberá ser aprobada y auditada por el Líder del proceso Gestión de las TICS de la Corporación CDA.

Política de establecimiento, uso y protección de claves de acceso.

Objetivo: Controlar el acceso a la información.

Directrices:

- Se debe concientizar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.
- Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Corporación CDA.
- Las contraseñas de correos y otras plataformas, no se deberán guardar dentro del navegador de los equipos de cómputo que no sean propiedad de la corporación CDA.
- Cuando algún funcionario de planta o contratista solicite el cambio de contraseña del computador, este deberá contar con la aprobación de su jefe inmediato y el líder de TIC, y dichas contraseñas deberán poseer un grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, como fecha de cumpleaños, nombre personal o de familiares, placas de automóviles y gustos de comida o bebidas.
- Las contraseñas deberán tener como mínimo 10 caracteres alfanuméricos ejemplo: GRF#$#%234(/45h

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- El cambio de contraseña deberá hacerse cada 3 meses, y deberá ser aprobada y verificada por el líder TIC de la corporación CDA
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario y este deberá ser informado al líder TIC de la corporación CDA.

Política de adquisición, desarrollo y mantenimiento de sistemas de información.

Objetivo: Garantizar que la seguridad es parte integral de los sistemas de información.

Directrices:

- Asegurar que los sistemas de información o aplicativos informáticos incluyan controles de seguridad y cumplan con las políticas de seguridad de la información.
- En caso de desarrollos propios de la corporación CDA, se debe verificar que están completamente documentados, que las diferentes versiones se preservan adecuadamente en varios medios y se guarda copia de respaldo externa a la corporación y que sean registrados ante la Dirección General de Derechos de autor del ministerio del interior y de justicia.
- Desarrollar estrategias para analizar la seguridad en los sistemas de información.
- Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica de la Corporación CDA, por cualquier dependencia o proyecto, deberá ser gestionado por el Profesional líder TIC de la entidad.
- Al comprar la licencia de un programa, se permitirá a la Corporación CDA realizar una copia de seguridad (a no ser que esté estipulado de manera distinta), para ser utilizada en caso de que el medio se averíe.
- Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
- Los funcionarios del proceso Gestión de las TIC de la Corporación CDA serán los únicos autorizados para realizar copia de seguridad del software original.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- La instalación del software en las máquinas y/o equipos dela Corporación CDA, se realizará únicamente a través de los funcionarios y/o contratistas autorizados por el líder TIC de la corporación CDA.
- El software proporcionado por la Corporación CDA no puede ser copiado o suministrado a terceros.
- En los equipos de la Corporación CDA solo se podrá utilizar software licenciado.
- Para la adquisición y actualización de software, es necesario efectuar la solicitud al Líder del proceso Gestión de las TIC con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
- El software que se adquiera a través de los proyectos o programas, debe quedar a nombre de CDA.
- Se encuentra prohibido el uso e instalación de juegos y programas de ocio en los computadores de la Corporación CDA.
- Cuando un software no se utilice y no sea requerido, se presentará el concepto técnico para ser dado de baja, de acuerdo con los lineamientos dados por la Corporación.

Política de uso de dispositivos móviles.

Objetivo: Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes (Smart phones) tabletas, entre otros) de la Corporación CDA.

Directrices:

- Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes (Smart phones) tabletas, entre otros) de la corporación, son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la corporación CDA.
- Los dispositivos móviles de la corporación podrán estar integrados a las plataformas de administración controlada por el proceso Gestión TIC de la Corporación CDA.
- Los usuarios podrán tener instaladas las aplicaciones distribuidas y autorizadas por el administrador de la CDA.
- Los dispositivos móviles de propiedad de la corporación deben tener configurado la cuenta de correo electrónico de la corporación.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Los usuarios que hagan uso de dispositivos móviles corporativos que requieran configuración, deben hacerlo asociándolos a la cuenta de correo corporativo del usuario o el correo que sea autorizado por el jefe inmediato.
- Ante la pérdida del equipo, ya sea por sustracción o extravío, deberá dar cuenta en forma inmediata al funcionario de Almacén y al profesional líder de las TIC, de la corporación CDA.
- Los teléfonos móviles y/o teléfonos inteligentes de propiedad de la corporación, deben permanecer encendidos y cargados durante las horas laborales o de acuerdo a la responsabilidad y a los requerimientos propios del cargo.
- Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la Corporación CDA, con el fin de realizar actividades propias de su cargo o funciones asignadas.
- En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil se debe solicitar la autorización al Profesional líder TIC de la Corporación para su aprobación.

Política para realización de copias en estaciones de trabajo de usuario final.

Objetivo: Asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

- De acuerdo a lo previsto por el artículo 91 de la Ley 23 de 1982, los derechos de autor sobre las obras creadas por los empleados y funcionarios públicos en cumplimiento de las obligaciones constitucionales y legales de su cargo, serán de propiedad de la entidad pública correspondiente, en este caso son propiedad de la corporación CDA con las excepciones que la misma ley a añadido.
- En el evento de retiro de un funcionario o traslado de dependencia, previa notificación del Área de Talento Humano, el líder de las TIC de la Corporación para el desarrollo sostenible del norte y oriente amazónico CDA, generará una copia de la información contenida en el equipo asignado al perfil del usuario a una unidad de almacenamiento. Si el jefe de la dependencia de la cual se retira el usuario requiere copia de esta información, debe realizar solicitud a Gestión al líder TIC de la Corporación CDA.
- Se debe seguir un procedimiento de Borrado Seguro para equipos Final, a fin garantizar la copia de la información para la entidad y la eliminación de la información almacenada en el disco local.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- En caso de presentarse alguna falla en los equipos de cómputo, se debe reportar al líder de sistemas. En caso de requerirse copia de la información, esta se realizará de manera temporal durante las diferentes labores de reparación o mantenimiento.

Política de uso de Token (Virtual o Físico).

Objetivo: Establecer las directrices de uso del mecanismo de doble autenticación (Token), para los diferentes servicios prestados por la Corporación CDA o entidades externas (Bancos, Ministerios u otros).

Directrices:

- La oficina de sistemas verificará la asignación de los Token a funcionarios de la Corporación CDA por parte de las diferentes entidades, de acuerdo a los accesos a las plataformas que lo requieran.
- La asignación de Token a los funcionarios dependerá del desarrollo de sus funciones, y deberá estar autorizado por el líder de las TIC de la corporación CDA.
- La asignación de Token a los funcionarios para la autenticación del equipo con otras entidades dependerá del tipo de información que maneje y se establezca como información pública reservada o información pública clasificada.
- Es responsabilidad del usuario hacer buen uso del dispositivo entregado, con el fin de realizar actividades propias de su cargo o funciones asignadas.
- La pérdida del Token entregado debe ser reportado de inmediato a la oficina de sistemas y solicitar su debida desactivación y bloqueo.
- En caso de no requerir más el uso del Token o retiro definitivo de la Corporación CDA, el funcionario debe realizar la devolución del mismo en las condiciones que le fue entregado.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

PROCEDIMIENTOS.

Procedimientos que apoyan la Política de Seguridad.

Los procedimientos son uno de los elementos dentro de la documentación del Manual de la Política de Seguridad para las Tecnologías de la Información y las comunicaciones. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso. También es recomendable el uso de instructivos para detallar aún más las tareas y acciones puntuales que se deben desarrollar dentro de un procedimiento, como son los instructivos de trabajo y de operación; los primeros para la ejecución de la tarea por la persona y los segundos para la manipulación o la operación de un equipo.

Procedimiento de control de documentos.

Garantiza que la organización cuente con los documentos estrictamente necesarios a partir de su perfil de actuación en cada momento y maneja la dinámica del mejoramiento, mostrando la realidad que atraviesa la corporación CDA en cada momento, porque incorpora la eficacia de las diferentes acciones, a través de la revisión documental y del cumplimiento de los requisitos idénticos en los diferentes modelos de gestión, sobre el control de documentos. Así mismo, busca garantizar que los documentos en uso son confiables y también se pretende mantenerlos actualizados, una vez se evidencia la eficacia de las acciones correctivas, preventivas y de mejora que hacen que los procesos se ajusten y evolucionen y que los documentos existentes en el momento de la evaluación y comprobación del cambio que se implementó como solución a un problema, riesgo o a una oportunidad se conserven.

Procedimiento de control de registros.

Está definido para evidenciar las acciones realizadas y los resultados obtenidos en la ejecución de las actividades, con el fin de analizar los datos, y lo que es más importante, para la toma de decisiones, de tal forma que registro que no aporta valor o no lleva a una decisión de mejora o de acción, no se debe tener en el sistema, ya que lo único que haría es desgastar a la organización y generar residuos sólidos como papel mal utilizado y espacio de memoria insuficiente.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Procedimiento de auditoría interna.**

La auditoría interna es una herramienta para la alta dirección, en el momento de determinar la eficacia y la eficiencia del sistema de gestión, a través de la identificación de las fortalezas y debilidades. Esta es la razón por la cual se recomienda siempre realizar auditorías internas antes de llevar a cabo la revisión gerencial, ya que para esta última se requiere información sobre el sistema y los procesos, de tal manera que se pueda evaluar la adecuación, la conveniencia y la eficacia del sistema de gestión.

Se hacen auditorias para evaluar la conformidad con las políticas de la organización, para evaluar el nivel de implementación del sistema de gestión, para evaluar el estado de mantenimiento y la capacidad de mejoramiento del sistema de gestión.

- **Procedimiento de acción correctiva.**

El objetivo de este procedimiento es definir los lineamientos para eliminar la causa de no conformidades asociadas con los requisitos de la política de seguridad de la Corporación CDA, así como: definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

- **Procedimiento de acción preventiva.**

El objetivo de este procedimiento es definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones preventivas generadas por la detección de una no conformidad real o potencial en el sistema de gestión de seguridad de la información y eliminar sus causas.

- **Procedimiento de revisión del Manual de la Política de Seguridad.**

El objetivo de este procedimiento es el de revisar, por parte de la dirección o su representante, el Manual de la Política para la Tecnología de Información y Comunicaciones - Tic de la Corporación para el desarrollo sostenible del norte y oriente amazónico CDA en intervalos planificados, para asegurar su conveniencia, eficiencia y eficacia continua.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Requisitos de seguridad de los sistemas de información

Establecer un procedimiento, o lineamientos para el aseguramiento de la calidad en el desarrollo de proyectos de Software, el cual debe ser aplicado a toda solicitud, requerimiento, desarrollo, adquisición de software que serán revisados, validados y liderados por la Oficina de las Tecnologías de la Información y las Comunicaciones de la Corporación CDA.

El desarrollo de tecnologías informáticas se debe orientar sobre herramientas basadas en tecnologías de última generación, que permitan la portabilidad y escalabilidad de las aplicaciones con el fin de estar a vanguardia con los últimos avances tecnológicos.

Todos los desarrollos de software, adquisición de sistemas de información y adquisición de equipos de cómputo, deberán ser aprobados por la Oficina de las Tecnologías de la Información y las Comunicaciones de la corporación CDA.

Seguridad en los procesos de desarrollo y de soporte.

La Oficina de Tecnologías de la Información y las Comunicaciones – TIC define los procedimientos y reglas básicas para tener en cuenta en el desarrollo seguro de software dentro de la Corporación CDA, estableciendo lineamientos para realizar una programación segura en los nuevos desarrollos y actualizaciones de software, acorde a la necesidad de las partes interesadas.

La Corporación debe establecer e implementar procedimientos para el control de cambios, para requerimientos de actualización, modificación o nuevas funcionalidades a los sistemas de información en producción.

Para el control de cambio se debe tener en cuenta.

- Establecer un proceso técnico documentado para llevar o realizar los cambios.
- Realizar las diferentes pruebas de calidad sobre los cambios establecidos.
- Realizar la correspondiente evaluación de riesgos antes de realizar los cambios.
- Verificar los requisitos de seguridad a los diferentes sistemas al implementar los cambios en las plataformas o software de la corporación CDA.
- Aprobación de los cambios realizados a los sistemas de información.
- Determinar controles y restricciones de acceso a los sistemas de información.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Desarrollo contratado externamente.

- La Oficina de Tecnologías de la Información y las Comunicaciones, será quien defina y/o aprueba los requerimientos de desarrollos tercerizados.
- La Oficina de Tecnologías de la Información y las Comunicaciones apoyará la supervisión de los desarrollos contratados externamente conforme a los requerimientos de la Corporación CDA.

Pruebas de seguridad de sistemas

- Todos los desarrollos de software deben surtir una fase de pruebas de funcionalidad en la cual se evidencien los controles establecidos en relación con la integridad de la información que será ingresada una vez se lleve a cabo su implementación.
- No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información. Así mismo, en los ambientes de desarrollo y calidad si se llegaran a utilizar datos reales del ambiente de producción, se debe definir el protocolo de seguridad que permita salvaguardar la integridad de la información.
- La actualización e incorporación de nuevos sistemas o nuevo software debe estar sujeto a un proceso de pruebas funcionales y de seguridad, con el fin de establecer el cumplimiento y aceptación de lo requerido.

RELACIÓN CON LOS PROVEEDORES.

Seguridad de la información en las relaciones con los proveedores.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la Entidad.

Los proveedores que dejen de prestar sus servicios a la corporación CDA, deberán entregar toda información del producto del trabajo realizado y hacer entrega de los equipos y recursos tecnológicos en perfecto estado, de acuerdo con las condiciones establecidas en el contrato o convenio. Una vez terminada la relación contractual, debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante la gestión en la Corporación CDA.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

En los procesos contractuales se deben incluir los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de las tecnología de la información y comunicaciones.

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL SERVICIO.

La Oficina de Tecnologías de la Información y las Comunicaciones debe establecer el análisis de los requisitos de seguridad de la información, incluyendo las necesidades de la seguridad de la información en las situaciones de emergencia o desastres.

Se debe desarrollar e implantar un plan de continuidad para asegurar que los procesos misionales de TI de la Corporación CDA puedan ser restaurados dentro de escalas de tiempo razonables.
La Corporación, deberá tener definido un plan que permita mantener la continuidad de servicios de TI teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI de la Corporación CDA, de acuerdo con su impacto en el cumplimiento de la misión de la Entidad.
- Documentación del plan de recuperación de TI de acuerdo con la estrategia definida anteriormente.
- Realizar las pruebas de recuperación de los elementos físicos, de software y backups, con el fin de que cuando ocurran los desastres, se sepa responder de manera oportuna para corregir el error o restaurar la recuperación del sistema en el menor tiempo posible.
- La Corporación CDA, debe asegurar que la información y los sistemas de información se encuentren respaldados y almacenados en diferentes sitios, con el fin de garantizar que no haya pérdida o daño de los datos.
- Se debe realizar la revisión y/o actualización periódica del sistema de gestión de seguridad, con el fin de mantener los controles y asegurar la eficacia en la seguridad de la información.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

CUMPLIMIENTO.

Cumplimiento de los requisitos legales y contractuales.

Derechos de propiedad intelectual.

La Corporación, respeta y acata las normas legales existentes relacionadas con protección de derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.
La Oficina de Tecnologías de la Información y las Comunicaciones – TIC, garantizará que todo el software que se ejecute en los activos de información de la Corporación CDA, esté protegido por derechos de autor y requiera licencia de uso o sea software de libre distribución y uso.

Protección de registros.

Realizar y conservar un análisis de los registros (bases de datos, registros de auditoría, registros documentales, y todos los registros generados por la entidad), para proteger y evitar la pérdida, destrucción, adulteración, y acceso no autorizado, de acuerdo con los requisitos contractuales y legales, y los contemplados por la Corporación CDA.
La Corporación se obliga a proteger todos los registros que revelen la evidencia del cumplimiento de los requisitos contractuales y legales contra la pérdida de Confidencialidad, Integridad y Disponibilidad, siguiendo los lineamientos del manual de Gestión de Activos de la corporación CDA.

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: www.cda.gov.co e-mail: cda@cda.gov.co