CSC
CORPORACIÓN SOCIAL DE CUNDINAMARCA

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN V1.1
11/08/2021

REALIZÓ	**REVISÓ**	**APROBÓ**
JOSÉ RAIMUNDO PABÓN JIMÉNEZ **CONTRATISTA DE LA CSC**	OMAR GERARDO DÍAZ ESPINOSA **ASESOR DE GERENCIA**	ADRIANA CAROLINA SERRANO TRUJILLO **GERENTE**

Tabla de contenido

1. INTRODUCCION

Las Entidades públicas tienen la necesidad de implementar un sistema de gestión de seguridad de la información (SGSI), y además debe definir las necesidades de sus grupos de trabajo, y la valoración de los controles precisos para mantener la seguridad de la información y tener en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, y sus procesos misionales.

Teniendo en cuenta lo anterior la Corporación Social de Cundinamarca actualiza la política de Seguridad y privacidad de la información a través de la oficina de sistemas donde define los lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo por el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la Entidad.

2. GLOSARIO

termino	Definición
Política	Declaración de alto nivel que describe la posición de la entidad sobre un tema específico
Estándar	Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.
Mejor Práctica	Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.
Guía	Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
Procedimiento	Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.
Información	está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto

	fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.
Información Pública	Un grupo de datos puros o procesados, hechos, noticias, DOCUMENTOS Toda información (informes, copias, reproducciones, datos electrónicos, imágenes etc.) que, independientemente del sujeto que la genere, obtenga, adquiera, transforme o controle, sea considerada de interés público.
Información reservada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.
Seguridad de la Información	La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos
Confidencialidad	es asegurar que la información es accesible sólo para las personas autorizadas para ello.
Integridad	es salvaguardar la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.
Personal	es toda persona a la cual se le da autorización para acceder a la información y a los sistemas de CSC. El personal puede ser interno o externo a la Entidad.

3. OBJETIVO GENERAL

Determinar, actualizar y socializar la política general y las directrices que se requieren para garantizar la protección de la información de la Corporación Social de Cundinamarca, cumpliendo con la integridad, disponibilidad y confidencialidad de la información y además como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

3.1. Objetivos Específicos

- Establecer las actividades que se desarrollarán como parte de la política de Seguridad y Privacidad de la Información.
- Producir una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la información por parte de los funcionarios de la Corporación Social de Cundinamarca.
- Definir los lineamientos para la implementación de la política de seguridad digital en la Corporación Social de Cundinamarca.

4. ALCANCE

La política debe ser socializada y aprobada por el comité de desempeño institucional y debe ser acatada por todos los funcionarios y ciudadanos que tengan acceso a las instalaciones y/o servicios tecnológicos de la Corporación Social de Cundinamarca.

Se debe asegurar el correcto funcionamiento, confiabilidad, confidencialidad, integridad en los servicios tecnológicos de la CSC, ofreciendo un nivel óptimo de Seguridad que permitan:

- Minimizar los riesgos de pérdida, integridad, disponibilidad y confidencialidad de la información y garantizar la continuidad de la información.
- Realizar campaña de cultura en seguridad y privacidad de la información en el año 2021 para los funcionarios, contratistas, terceros, aprendices, practicantes y proveedores de la Entidad.
- Realizar seguimiento al cumplimiento de la política de seguridad, privacidad de información y la protección de datos.
- Mantener un seguimiento al plan de manejo y acceso a la información de la atención al ciudadano.
- Capacitar y socializar los controles de política de seguridad, privacidad de información y la protección de datos.
- Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
- Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital de manera integral.
- Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información de la corporación
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL (Política General de la SPI Guía No.2, 2016)

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

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

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Corporación Social de Cundinamarca.
- Garantizar la continuidad del negocio frente a incidentes.
- La CSC ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI, Principios de seguridad que soporta el SGSI de la CSC:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, o terceros.
- La CSC protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La CSC protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La CSC protegerá su información de las amenazas originadas por parte del personal.
- La CSC protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La CSC controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La CSC implementará control de acceso a la información, sistemas y recursos de red.
- La CSC garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La CSC garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La CSC garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La CSC garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1. Seguridad de la Información

Según ISO 27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: Electrónicos, En papel o Audio y vídeo, etc.
La Corporación Social de Cundinamarca estableció a través del Comité de Desempeño Institucional el Comité directivo de la seguridad y Privacidad de la información con el propósito de planear, verificar y mejorar los programas y las actividades de SPI, revisión de documentos de la política, avances en los proyectos de SPI, etc., este comité está en cabeza del profesional de área de sistemas de la entidad.

6.2. Roles y responsabilidades (Roles y responsabilidades guia No. 4, 2016)

La Corporación Social de Cundinamarca para obtener un buen desarrollo de la política de seguridad y Privacidad de la Información - MSPI, establecerá las responsabilidades y el personal de las dependencias encargadas de desarrollar las actividades del modelo de seguridad digital. Para la asignación de los roles, la Entidad signara los roles de acuerdo a las funciones específicas dentro del manual de funciones de CSC. A continuación, se definen algunos roles y responsabilidades que se deben tener en cuenta en la implantación y seguimiento de la política SPI.

Funcionarios de la CSC	Rol	Responsabilidad
Gerente de CSC	Alta Dirección	Direccionamiento y apoyo en la implementación MSPI
Grupo de Trabajo de Seguridad de la Información (Asesor de Planeación)	Toma de decisiones en la Planeación, implementación y evaluación.	Toma de decisiones frente a la seguridad de la Información de la Entidad.
Líder de la Información (Oficina de Sistemas)	Líder y Responsable MSPI	Liderazgo y responsabilidad del MSPI.
Líder y dueño del Riesgo (Oficina de Sistemas)	Plan de tratamientos de riesgos de la seguridad	Gestión riesgos de seguridad de la información

	digital.	del proceso
Grupo Interesado (equipo de trabajo de la CSC).	Dar cumplimiento MSPI.	Mediante un informe dar estricto cumplimiento a lo estipulado en el MSPI.
Grupo de la oficina de sistemas de la CSC.	Planeación e implementación de la transición y migración IPv4 a IPv6, actividades dentro del MPSI	Llevar a cabo la implementación del protocolo IPv6 en la entidad.

6.3. Control de acceso

La Corporación Social de Cundinamarca determina mecanismos de protección, relacionado con los accesos a la información sin importar si estos accesos sean electrónicos o físicos, actualmente la Entidad contempla los siguientes controles:

- Control de acceso con usuario y contraseña. (La CSC cuenta con un documento de Usuarios y contraseñas de todos los funcionarios. (planta y contratistas) para acceder a los computadores y a los sistemas de información. (La CSC cuenta con el documento)
- Suministro del control de acceso. (La CSC cuenta con el documento)
- Gestión de Perímetros de Seguridad. (La CSC cuenta con el documento)
- Áreas de Carga. (La CSC cuenta con el documento)

6.4. Controles criptográficos

Los controles criptográficos pueden alcanzar diferentes objetivos de seguridad como, por ejemplo, la confidencialidad utilizando cifrado de información para proteger información sensible o crítica, así sea transmitida o almacenada dentro de esta política la Corporación Social de Cundinamarca incorpora lo siguiente:

- Se establece el enfoque de la dirección general con relación al uso de controles criptográficos en CSC, incluyendo los principios generales bajo los cuales se deben proteger la información de la entidad.
- Se realizo la valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido.

- Se protege la información enviada por dispositivos móviles encriptados mediante líneas de comunicación.
- Se estableció la oficina de sistemas de la CSC con rol y responsabilidades: la implementación de la política.
- Se definió en el matriz de riesgos el impacto de usar información encriptada en los controles que dependen de la inspección del contenido.
- Se genero llaves para diferentes sistemas criptográficos y diferentes aplicaciones, además con las certificaciones requeridas por las entidades relacionadas con la entidad.

6.5. Escritorio limpio y pantalla limpia

Consiste en la protección de los papeles y dispositivos removibles de almacenamiento de información, almacenados y manipulados en estaciones de trabajo, de accesos no autorizados, perdida o daño de la información.
De acuerdo a lo anterior la Corporación Social de Cundinamarca cumple con las siguientes directrices:

- Se considera que la información sensible o crítica de la CSC, ya sea en físico o electrónico, se guarda en caja fuerte cuando no se requiera, especialmente cuando la oficina esté desocupada.
- Se definió un manual para la gestión de equipos desatendidos, los computadores y terminales deben estar fuera del sistema y estar protegidos con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña y deben estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso.
- Evitar el mal uso y no autorizado de fotocopiadoras y otras tecnologías de reproducción.

6.6. Protección de datos personales

La información es el activo más importante de la CSC, La ley (Estatutaria 1581 de 2012) busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación (tratamiento) por parte de entidades de naturaleza pública y privada. La Corporación social de Cundinamarca cuenta con una política de protección de datos la cual está aprobada y publicada en el Portal WEB.

6.7. Inventario de activos (Clasificación de activos guía No. 5, 2016)

La Corporación Social de Cundinamarca a través de un inventario bien identificado tiene la relación de todos los activos de la información, y se puede identificar, las características de cada equipo o sistema de información, su rol, ubicación, clasificación, justificación, criticidad, custodio, fecha de ingreso, identificador, nombre, etc., estas actividades se encuentran reflejadas documentalmente en la Matriz de Inventario y Clasificación de Activos de Información.

6.8. Uso de correo electrónico

La Corporación Social de Cundinamarca establece las políticas del buen uso del correo electrónico y define unas reglas para tal uso:

- Los correos electrónicos son exclusivamente para actividades y funciones de la Corporación Social de Cundinamarca, y no deben ser utilizados para actividades o asuntos personales o ajenos a la entidad.
- La utilización del correo debe hacerse de manera ética y responsable, y sin generar traumatismos ni riesgos para la operación de los equipos de cómputo y sistemas de información de la CSC.
- Las personas clientes y contratistas de la Corporación deben dar cumplimiento a la ley, 1273 de 2009 "de la protección de la información y de los datos", igualmente evitar prácticas o usos que puedan afectar la SPI de la Corporación.
- La información generada en los correos electrónicos, buzones y copias de seguridad son propiedad de la CSC, igualmente poder ser revisadas en caso de algún incidente de seguridad de la información.
- Cuando la CSC, a través de una dependencia, generen información institucional para divulgar debe realizarse a través de la subgerencia administrativa quien es la encargada del área de sistemas.
- El único Correo electrónico autorizado por CSC es el que directamente la oficina de sistemas genera, el cual cumple con los requisitos de seguridad y privacidad de la información.
- La capacidad el buzón del correo electrónico se asigna de manera igual para todos los funcionarios, la capacidad específica es definida y administrada por la Oficina de Sistemas.
- El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado

- o no solicitado, correos de dudosa procedencia o con virus a la Oficina de Tecnologías de
- Los funcionarios usuarios de los correos institucionales debe reportar a la oficina de Sistemas, cuando llegan correo desconocidos o maliciosos, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos.
- Cuando los funcionarios de la CSC son retirados de la entidad, la oficina de Sistema inactiva el correo electrónico y demás claves de ese usuario.
- Las personas responsables de los correos institucionales deben realizar depuración del buzón periódicamente
- Si una cuenta de correo es interceptada por personas ajenas y mal intencionadas (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), la Oficina de Sistemas hará un barrido y tomara medidas.
- Ningún usuario debe inscribirse por el correo institucional a promociones o televentas, o actividades ajenas a la CSC.
- Los correos electrónicos de los funcionarios de la CSC, tienen un tamaño máximo para recibir o enviar mensajes de 25 MB.

6.9. Uso del Internet

6.9.1. Buen uso del servicio del internet

- La Corporación Social de Cundinamarca mediante la política del buen uso del internet establece una protección de la Seguridad y Privacidad de la Información.
- El servicio de internet debe ser exclusivo para el desarrollo de las funciones y actividades desarrolladas por la entidad.
- Los funcionarios autorizados para hacer uso del internet, son responsables de prevenir prácticas que puedan causar daños tecnológicos en la Entidad o que afecte la Seguridad y Privacidad de la información.
- La oficina de Sistemas revisa y monitorea todas las comunicaciones establecidas como administrador del servicio.
- La oficina de Sistemas maneja el navegador de internet autorizado por esta oficina, y así prevenir ataques cibernéticos.
- Los funcionarios de la Corporación Social de Cundinamarca tienen bloqueadas ciertas paginas como son Facebook, páginas pornográficas, etc.
- No se permite conexiones externas o ajenas de la CSC de aparatos tecnológicos sin que esta sea autorizada por la Corporación.

- Todos los funcionarios son responsables del uso de sus credenciales de acceso a las cuales les fue otorgado el acceso a internet.
- La oficina de sistemas de la Entidad se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios.
- Todos los usuarios autorizados son responsables del uso adecuado del internet y no podrá usarlo para prácticas ilícitas o mal intencionadas que afecten la seguridad y privacidad de la información.

6.9.2. Mal uso del servicio de internet

- Por enviar o descargar información de tamaño grande o pesado que congestione el ancho de banda, a no ser que sea funcional para la entidad.
- Los usuarios no podrán acceder a páginas indebidas como pornografía y ajenas a las funciones de la entidad que afecten la integridad moral de las personas.
- Prohibida el intercambio o descargas de videos, juegos, música, imágenes, etc., que afecten la propiedad intelectual, los archivos ejecutables y comprometan la seguridad y privacidad de la información de la Corporación Social de Cundinamarca.
- Los usuarios invitados de la entidad que deseen tener acceso al servicio de internet deben de cumplir las políticas de seguridad y privacidad de la información.

6.10. Uso de redes sociales

- El servicio de las redes sociales debe ser exclusivo de la Corporación Social de Cundinamarca.
- El administrador de las cuentas de las redes sociales debe mantenerlas en modo privado y la comunidad podrá seguir las redes de la empresa si el administrador da el acceso y permisos.
- En caso de recibir mensajes ofensivos el administrados no debe contestar, deberá denunciar la cuenta y bloquéala.
- No deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.
- Comprobar la configuración de la privacidad, en la cual puedes decidir que la información privada solo la vea la entidad.
- La Oficina de sistemas, es el encargado de configurar las directrices y permisos para el buen uso de las diferentes redes sociales de la CSC.

- No se permite las descargas de material inapropiado como pornografía desde las plataformas o herramientas de redes sociales de la entidad.

6.11. **Integridad** (Política General de la SPI Guía No.2, 2016)

El objetivo de la integridad es prevenir modificaciones no autorizadas de la información. Los funcionarios de la Corporación Social de Cundinamarca reconocen y aceptan el manejo integral de la información producida por la entidad, igualmente la recibida por la comunidad, esta información se procesa y mediante la gestión del conocimiento se intercambia exclusivamente con las persona interesadas de dicha información, igualmente, la información (verbal, física o electrónica) es enviada o recibida por los diferentes medios de comunicación sin ninguna modificación, ni alteraciones, a no ser que sea necesario la modificación o alteración y esto solo lo puede decidir o autorizar el responsable de la información o del proceso.

En la suscripción del contrato de los funcionarios de la CSC de planta como contratistas existe una cláusula denominada Cláusula de integridad de la información, donde la persona pacta con la entidad que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

6.12. Uso adecuado del Software

En la Corporación Social de Cundinamarca en los computadores de trabajo no se pueden instalar aplicaciones, ni programas, que no se encuentren licenciados y hayan sido adquiridos por la entidad.

La oficina de sistemas de la entidad, es la encargada de la coordinación y mantenimiento de programas y aplicaciones para las distintas labores de cada funcionario.
Los computadores de la Corporación Social de Cundinamarca deben ser utilizados por los empleados, proveedores y contratistas solamente para el desarrollo de las funciones normales del trabajo.

6.13. Protección de virus

Los equipos de trabajo personales deben mantener activo un Sistema operativo, software antivirus, y una herramienta de editor de documentos como lo es Microsoft Office, que se

encuentren licenciados los programas y o aplicaciones que no sean de software libre. Que el uso de estos equipos debe estar autorizados por el área encargada del buen uso como es la Oficina de Sistemas de la CSC.

Los servidores de archivos, terminales y correos electrónicos entre otros deben mantener activo y actualizado un software de protección de virus
La oficina de sistemas debe realizar periódicamente un análisis de virus tanto en las estaciones de trabajo como en los servidores de datos y de aplicaciones.
Toda información recibida electrónicamente tanto por correo electrónico como en medio magnético debe ser examinada por un antivirus para garantizar la protección de la información suministrada.
La oficina de Sistemas de entidad es la encargada de la actualización oportuna del software antivirus.
Es responsabilidad de los usuarios:

- Reportar todos los incidentes de virus a las áreas encargadas.
- Realizar copias de la información y verificar que esté libre de cualquier infección de virus.
- El usuario debe asegurar que toda la información provenga de fuentes confiables.
- Ningún usuario puede instalar o distribuir software no confiable.

6.14. Backup

La Corporación Social de Cundinamarca cuenta con un sistema automático para realizar las copias de respaldo de la información, las copias tienen el mismo nivel de protección de la información que poseen en su fuente original.

Los medios magnéticos que contienen información de respaldo se encuentran almacenados en lugares seguros.
La oficina de sistemas de CSC son responsables de respaldar la información producida por la entidad, igualmente, son responsables de realizar la oportuna restauración de la información requerida.

Se realizan más de una copia de respaldo para que en caso de contingencia se pueda recuperar la información oportunamente.

Los funcionarios de la CSC deben exigir el acuse de recibo en caso de enviar o suministrar información clasificada, restringida o confidencial a terceros.

La oficina de sistemas de la CSC realizar programación diaria y en horas diferentes automatizadas para las copias de respaldo de la información y así tener eficacia y seguridad de la información cuando sea requerida o necesaria por la entidad.

6.15. Manejo integral de la gestión documental

La Corporación Social de Cundinamarca establece requisitos para el manejo de documentos electrónicos entre los cuales tenemos:

- Procesos de transparencia en la gestión y el mejoramiento de los servicios a los ciudadanos.
- La CSC a través del área de talento humano realiza capacitaciones para fortalecer la gestión de los documentos electrónicos.
- La CSC cuenta con servicio permanente de Internet y servicios de correo electrónico, la oficina de sistemas de la entidad reglamenta la utilización de acuerdo a las políticas y a las responsabilidades asignadas a cada uno de los funcionarios y estos a su vez tendrán un control sobre los documentos enviados y recibidos.
- De acuerdo a la ley 594 del 14 de julio del 2000 donde "***Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014 Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones El Congreso de Colombia"***

  Las entidades que están en la obligación de generar mecanismos para administrar las comunicaciones oficiales que se reciben y se envían mediante el correo electrónico. (Ley 594 del 2000, 2000).
- La CSC 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 de acuerdo a la ley 527 de agosto de 1999. (Ley 527 de 1999., 1999).

6.16. Registro y auditoría

La Corporación Social de Cundinamarca establece políticas para el mantenimiento de las evidencias, actividades y acciones que afectan los activos de información y contiene lo siguiente:

- La oficina de control interno como responsable de las auditorías trimestralmente a las actividades de los sistemas de información de la entidad y dar a conocer los resultados a la oficina de sistemas como a la gerencia general.
- La oficina de sistemas de la CSC es la encargada de las copias de seguridad de acuerdo a la política de Backup y el buen funcionamiento del mismo. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.
- La oficina de sistemas elabora controles para determinar la eficiencia de los sistemas de la información.
- La Entidad mediante el plan de riesgos de la seguridad y privacidad de la información evalúa los niveles de riesgo al que está expuesta la información y así mismo poder establecer controles sobre esos riesgos detectados.

7. BIBLIOGRAFÍA

Clasificación de activos guía No. 5. (2016). *MINTICS*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Ley 527 de 1999. (08 de 1999). *Secretaria distrital de hábitat*. Obtenido de https://www.habitatbogota.gov.co/transparencia/normatividad/normatividad/ley-527-1999

Ley 594 del 2000. (14 de 07 de 2000). *Archivo general de la Nación*. Obtenido de https://normativa.archivogeneral.gov.co/ley-594-de-2000/

Política General de la SPI Guía No.2. (2016). *MInisterio de la Tic y Comunicaciones*. Obtenido de MINTIC: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Porcedimientos de SPI guía no. 3. (2016). *Ministerio de Tics*. Obtenido de MINTIC: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Roles y responsabilidades guia No. 4. (2016). *Ministerio de Tics y Comunicaciones*. Obtenido de MINTICS: https://gobiernodigital.mintic.gov.co/692/articles-150523_G4_Roles_responsabilidades.pdf