Plan de Seguridad y Privacidad de la Información

Corporación Social de Cundinamarca

2023

CONTENIDO

TABLAS

REALIZÓ	REVISÓ	APROBÓ
Diana Milena Reina Profesional de Gerencia	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño

1. INTRODUCCION

Los lineamientos de nivel de seguridad y privacidad de la información establecidos por el gobierno nacional en cabeza del Ministerio de Tecnologías de Información y las Comunicaciones – MINTIC para las entidades públicas en su nueva RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 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” están cada vez más expuestas a sufrir incidentes de seguridad digital, lo cual, puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Es por eso que MINTIC establece lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en las Entidades Públicas.

La política de Seguridad y privacidad de la información tiene como objetivo promover 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.

Teniendo en cuenta lo anterior la Corporación Social de Cundinamarca actualiza el modelo de Seguridad y Privacidad de la Información a través de la oficina de sistemas y define los lineamientos para la implementación de la estrategia de seguridad digital el cual contempla la operación mediante el ciclo de PHVA (planear, hacer, verificar y actuar), esta actualización de modelo de seguridad consta de cinco (5) fases: Diagnostico, Planificación, Operación, Evaluación de Desempeño, Mejoramiento continuo.

2. MARCO JURÍDICO

Conforme con lo establecido en la normatividad vigente La Corporación Social de Cundinamarca, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la Entidad:

- ✓ Constitución Política de Colombia. Artículos 15, 209 y 269.
- ✓ Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- ✓ Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- ✓ Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- ✓ Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- ✓ Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- ✓ Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- ✓ Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- ✓ Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- ✓ Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- ✓ Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- ✓ Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- ✓ CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- ✓ Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- ✓ Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- ✓ Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- ✓ Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.
- ✓ Resolución número 00500 de marzo 10 de 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.

3. TERMINOS Y DEFINICIONES

Tabla No. 1. Términos y definiciones

termino	Definición
AJAX	Acrónimo de Asynchronous JavaScript And XML (JavaScript asíncrono y XML), es una técnica de desarrollo web para crear aplicaciones interactivas o RIA (Rich Internet Applications). Estas aplicaciones se ejecutan en el cliente, es decir, en el navegador de los usuarios mientras se mantiene la comunicación asíncrona con el servidor en segundo plano. De esta forma es posible realizar cambios sobre las páginas sin necesidad de recargarlas, mejorando la interactividad, velocidad y usabilidad en las aplicaciones.
Base de datos SQL	(Por sus siglas en inglés Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas. Una de sus características es el manejo del álgebra y el cálculo relacional que permiten efectuar consultas con el fin de recuperar, de forma sencilla, información de bases de datos, así como hacer cambios en ellas.
Bitvise	Es un cliente para administrar y modificar código fuente en programas web.
Copia de seguridad:	Una copia de seguridad, copia de respaldo o backup (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales.
DATADOC	Software desarrollado para el control, la administración y la gestión documental de una entidad.

Direccionamiento IP	Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP).
Directorio Activo	Es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red. Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.
Firewall – Trunk	Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. La opción “trunk” – “baúl” canaliza ciertas amenazas a un sitio seguro para después ser analizadas.
Firewall Fortinet	Es un producto que ofrece soluciones de servicios a nivel de seguridad informática con mecanismos de software y hardware. Solución adquirida por la Corporación Social de Cundinamarca.
ISOLUCION	Compañía de tecnología relacionada con el diseño, desarrollo, implementación y soporte de soluciones tecnológicas para los sistemas integrados de gestión y los sistemas de gestión de la Calidad, basados en modelos normativos ISO y sus complementarios.

Lenguaje PHP	Es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico. Fue uno de los primeros lenguajes de programación del lado del servidor que se podían incorporar directamente en el documento HTML en lugar de llamar a un archivo externo que procese los datos. El código es interpretado por un servidor web con un módulo de procesador de PHP que genera la página Web resultante. Puede ser usado en la mayoría de los servidores web al igual que en casi todos los sistemas operativos y plataformas. PHP se considera uno de los lenguajes más flexibles, potentes y de alto rendimiento conocidos hasta el día de hoy.
LITISOFT	Es un sistema que controla los procesos judiciales, desde la presentación de la demanda hasta la terminación del proceso judicial. Tiene parametrizados todos los tipos de proceso y sus respectivos trámites por cada jurisdicción: civil, administrativa, penal, laboral y constitucional. Está compuesto por los módulos de: Información jurídica y financiera, control de términos y módulo de reportes.
Modo batch	Se conoce como sistema por lotes (en inglés batch processing), o modo batch, a la ejecución de un programa sin el control o supervisión directa del usuario (que se denomina procesamiento interactivo). Este tipo de programas se caracterizan porque su ejecución no precisa ningún tipo de interacción con el usuario.
Permisos SQL server	Asignar por parte de un administrador de la base de datos, derechos de acceso o restricción a las opciones o información contenida en las tablas de almacenamiento, administración y estructura de los datos contenidos en los servidores de información de la Organización.
Segmento DMZ	Llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.
Segmentos de red	Es un conjunto de equipos (computadoras y periféricos) conectados en red. Una red de una organización puede estar compuesta por varios segmentos de red conectados a la LAN principal llamada backbone, que existe para comunicar los segmentos entre sí.

Servidor DHCP	(siglas en inglés de Dynamic Host Configuration Protocol, en español «protocolo de configuración dinámica de host») es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Los servidores DHCP administran de forma centralizada direcciones IP e información relacionada y la ofrecen a los clientes automáticamente. Esto permite configurar la red de cliente en un servidor en lugar de hacerlo en cada equipo cliente.
Servidor DNS:	Domain Name System o DNS (en español «Sistema de Nombres de Dominio») es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.
Servidor NTP	Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable. Una solución completa para sincronizar redes de gran tamaño. El servidor de hora combina un reloj de radio basado en GPS con un ordenador de estado sólido Linux incorporado y ofrece una configuración y administración sencillas a través de una interfaz

	de navegador.
Sistema Operativo Linux	Es un sistema operativo, una gran pieza de software que controla un computador. Es parecido a Microsoft Windows, pero completamente libre. El nombre correcto es GNU/Linux pero "Linux" se usa más. Linux no es el producto de una sola compañía, es el resultado de la contribución de un gran número de compañías y grupos de personas. De hecho, el sistema GNU/Linux es un componente central, el cual se transforma en muchos productos diferentes: las llamadas distribuciones.
Software:	Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación. Se considera que el software es el equipamiento lógico e intangible de un ordenador. En otras palabras, el concepto de software abarca a todas las aplicaciones informáticas, como los procesadores de textos, las planillas de cálculo y los editores de imágenes.
SQL Server Management Studio (SSMS):	Es una aplicación de software de Microsoft que se utiliza para configurar, gestionar y administrar todos los componentes dentro de Microsoft SQL Server. La herramienta incluye tanto los editores de scripts y herramientas de gráficos que trabajan con objetos y características del servidor. Una característica central de SSMS es el explorador de objetos, lo que permite al usuario navegar, seleccionar y actuar sobre alguno de los objetos dentro del servidor.
Switch:	Conmutador (Switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta. Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

Tiempo real	Un sistema en tiempo real (STR) es aquel sistema digital que interactúa activamente con un entorno con dinámica conocida en relación con sus entradas, salidas y restricciones temporales, para darle un correcto funcionamiento de acuerdo con los conceptos de predictibilidad, estabilidad, controlabilidad y alcanzabilidad. La palabra tiempo significa que el correcto funcionamiento de un sistema depende no sólo del resultado lógico que devuelve la computadora, también depende del tiempo en que se produce ese resultado. La palabra real quiere decir que la reacción de un sistema a eventos externos debe ocurrir durante su evolución. Como una consecuencia, el tiempo del sistema (tiempo interno) debe ser medido usando la misma escala con que se mide el tiempo del ambiente controlado (tiempo externo).
Topología de red	Se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que una curva se intercepta a sí misma. En algunos casos, se puede usar la palabra arquitectura en un sentido relajado para hablar a la vez de la disposición física del cableado y de cómo el protocolo considera dicho cableado. Así, en un anillo con un concentrador (unidad de acceso a múltiples estaciones, MAU) podemos decir que tenemos una topología en anillo, o de que se trata de un anillo con topología en estrella. La topología de red la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.
Usuarios de dominio	Es una cuenta compuesta por nombre y contraseña con el fin de acceder a los diferentes servicios de un servidor o grupo de servidores, redes, carpetas, archivos, información y recursos compartidos para compartir, editar o transferir la gestión digital de la Organización. La cuenta de un usuario del dominio registra toda la información necesaria para su definición, los grupos a los que pertenece el usuario, los derechos y permisos que tiene el usuario para utilizar el equipo y la red, así como para tener acceso a sus recursos. En los controladores de dominio de

	Windows Server, las cuentas de usuario se administran con usuarios y equipos de Active Directory.
VLAN	Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4). Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware, lo que las hace extremadamente fuertes.
ZIMBRA:	La suite de colaboración Zimbra (en inglés Zimbra Collaboration Suite o ZCS) es un programa informático colaborativo o Groupware que consta de un servicio de correo electrónico creado por Zimbra Inc. compañía ubicada en San Mateo, California. Posee tanto el componente de servidor como su respectivo cliente.
Información pública	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.
Internet:	Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.
Intranet:	Es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.
Vulnerabilidad o riesgo de seguridad de la información	Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener

	en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

4. OBJETIVOS

4.1. General

Actualizar el plan de seguridad y privacidad de la información de acuerdo a la normativa vigente, que permitan implementar procesos transversales para el mejoramiento del sistema de gestión de seguridad de la información y buscar el aprovechamiento de los servicios tecnológicos y de comunicaciones brindando confiabilidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso con el fin de asegurar su correcta funcionalidad, ofreciendo un nivel de seguridad óptimo que contribuyan al cumplimiento misional de la Corporación Social de Cundinamarca.

4.2 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.
- ✓ Implantar un cronograma basado en el ciclo de mejora continua para la adopción integral del Modelo de Seguridad y Privacidad de la Información.
- ✓ Desarrollar el modelo de seguridad mediante sus cinco (5) las fases.

- ✓ Definir los lineamientos para la implementación de la estrategia de seguridad digital en la Corporación Social de Cundinamarca.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

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 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.

En la Corporación social de Cundinamarca mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada ciudadano.

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.

5.1. Objetivos específicos de la política de seguridad y privacidad de la información y seguridad digital

- ✓ 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 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.

5.2. Identificación de los activos de seguridad y privacidad de información de la CSC

La clasificación de activos hace parte de la política de la seguridad y privacidad de la información de la entidad y contribuye al cumplimiento del control del Anexo A del estándar ISO/IEC 27001:2013 (inventario de activos, propiedad de activos, clasificación de la información, etiquetado y manipulado de la información).

Tabla No. 2. Clasificación de activos

Tipo de activo	Descripción
Elementos de Red	Son todos aquellos los elementos y medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, hub y demás.
Hardware	Equipos físicos de cómputo, impresoras, gabinetes, y de comunicaciones como, servidores, etc.
Información	Toda la producida por la CSC como: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros. Esta información es almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores).

Instalaciones	Cuarto de datos o espacio o área asignada para alojar y salvaguardar los servidores considerados como activos críticos para la CSC.
Intangibles	Son aquellos activos inmateriales que otorgan a la CSC una ventaja competitiva relevante, uno de ellos: es la imagen corporativa, reputación o el Good Will, entre otros.
Humanos	Profesionales que, por su conocimiento, experiencia son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
Software	Relaciona a todos los sistemas de información de la CSC como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.

6. PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Corporación Social de Cundinamarca tomo como referencia la norma ISO/IEC 27001, para definir los procedimientos de seguridad necesarios de la seguridad y privacidad de la información.

Tabla No. 3. Procedimientos de seguridad de la SPI

Controles de seguridad	Procedimientos
Seguridad del recurso humano	Está relacionado con tanto con los funcionarios como contratistas que trabajan en la Entidad. La CSC cuenta con los siguientes procedimientos. ▪ Metodología para la capacitación de los funcionarios en temas de seguridad digital. ▪ Procedimientos documentados de vinculaciones y desvinculaciones laborales.

Gestión de activos	La CSC tiene un documento donde posee todo el inventario de los activos de información.
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. ▪ Suministro del control de acceso. ▪ Gestión de Perímetros de Seguridad. ▪ Áreas de Carga
Seguridad física y entorno	La corporación Social de Cundinamarca maneja una restricción favorable al cuarto de datos y a los sistemas de información, además maneja formatos del control de calidad para dar de baja e ingresar equipos de cómputo o de comunicaciones a los activos de la CSC.
Seguridad de las comunicaciones	Está protegida a través de Firewall, protección del cableado estructura, antivirus y licencia MPKI de sitio seguro para la página web.
Relaciones con los proveedores	La entidad a través de los procesos de contratación selecciona su proveedor y estos a su vez tienen que cumplir con unos métodos de confiabilidad y protección de datos.
Adquisición, desarrollo y mantenimiento de sistemas de información	La CSC realiza procesos para la actualización y mantenimiento de los sistemas de información que maneja, como son NOVASOFT Y DATADOC.

7. INVENTARIO DE ACTIVOS

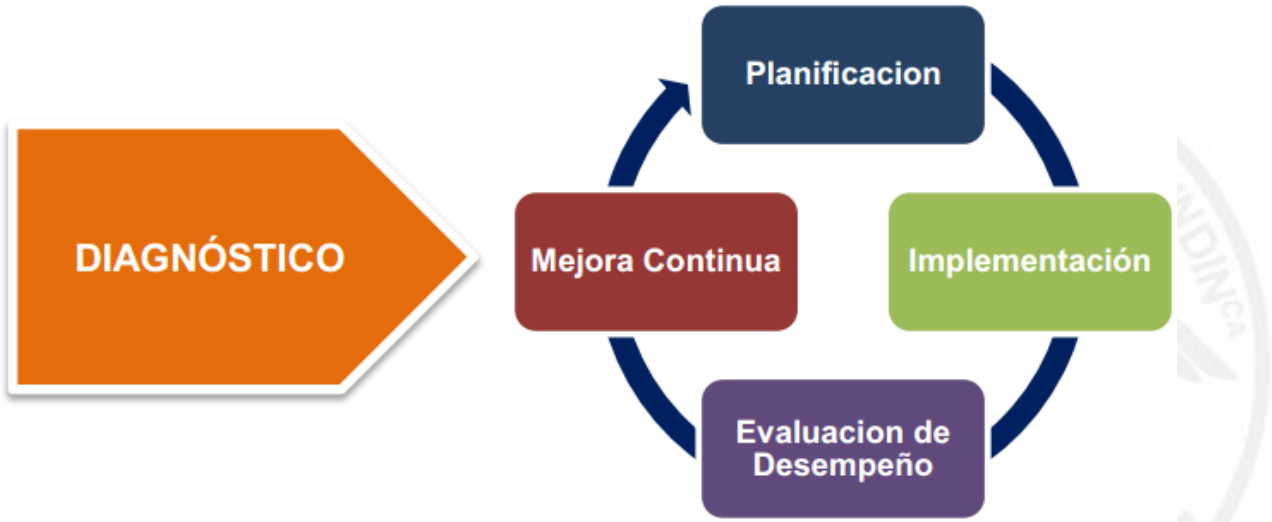
La Corporación Social de Cundinamarca a través de un inventario de todos los activos de la información puede identificar, las características de cada activo de información, su rol, ubicación, clasificación, custodia, fecha de ingreso e

identificador, estas actividades se encuentran reflejadas documentalmente en la Matriz de Inventario y Clasificación de Activos de Información.

8. CICLO DE OPERACIONES

Definir el plan de seguridad y privacidad de la Información en el marco de la implementación y mejora del Subsistema de Gestión de Seguridad de la Información (SGSI) para la Corporación Social de Cundinamarca, utilizando como guía la norma ISO-IEC- 27001:2013 y Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC para proteger la confidencialidad, integridad y disponibilidad de la información contenida en los activos de la entidad.

El modelo consta de 5 ciclos: (Ciclos de MSPI, 2021)



8.1. Diagnóstico

En esta fase se identifica el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Tabla No. 4. Etapa de diagnostico

Actividades	Descripción	Área interesada **(Responsable)**	Periodo de ejecución
Diagnóstico Modelo de Seguridad y Privacidad de la Información (MSPI).	Realizar diagnóstico de seguridad y privacidad de la información para la vigencia, construido a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI)	TIC-Subgerencia Administrativa	Primer trimestre del 2023.
Determinar el nivel de madurez de los controles de seguridad de la información.	Se registra en la herramienta de instrumento de evaluación MSPI del ministerio de las Tic.	TIC-Subgerencia Administrativa	Segundo trimestre del 2023.
Identificar el avance de la implementación del ciclo de operación al interior de la entidad.	Se registra en la herramienta de instrumento de evaluación MSPI del ministerio de las Tic.	TIC-Subgerencia Administrativa	Segundo trimestre del 2023.
Identificación del uso de buenas prácticas en ciberseguridad.	Se registra en la herramienta de instrumento de evaluación MSPI del ministerio de las Tic.	TIC-Subgerencia Administrativa	Segundo trimestre del 2023.
Actualización de inventario de computadores,	Documento de oficina de sistemas	TIC-Subgerencia Administrativa	Tercer trimestre del 2023

revisión de Software instalado en servidores y sistemas de información			

8.2. Planificación

La Corporación social de Cundinamarca construyó este documento teniendo cuenta los resultados de la fase diagnóstico, con el fin de determinar las actividades que estén encaminadas y alineadas a los objetivos misionales de la entidad:

Tabla No. 5. Planificación de actividades CSC

Actividades	Descripción	Área interesada **(Responsable)**	Periodo de ejecución
Política de Seguridad y Privacidad de la Información.	Revisar y actualizar el documento de la política de seguridad de la información, aprobado por Comité Institucional de Gestión y Desempeño	TIC-Subgerencia Administrativa	Primer trimestre 2023.
Procedimientos de seguridad de la información.	Revisar y actualizar dentro del documento Política de seguridad y privacidad de la información	TIC-Subgerencia Administrativa	Primer trimestre 2023.
Roles y responsabilidades de seguridad y privacidad de la información.	Revisar y actualizar dentro del documento Política de seguridad y privacidad de la información	TIC-Subgerencia Administrativa	Tercer trimestre 2023.
Inventario de	Actualización del	TIC-Subgerencia	Cuarto trimestre

activos de información.	Documento.	Administrativa-Archivo	2023.
Integración del MSPI con el Sistema de Gestión documental	Documento desarrollado y aprobado.	TIC-Subgerencia Administrativa.	Tercer trimestre 2023.
Identificación, Valoración y tratamiento de riesgo.	Documento desarrollado y aprobado. Plan de riesgos de la SPI	TIC-Subgerencia Administrativa	Tercer trimestre 2023.
Revisión, ajuste e implementación de controles para el teletrabajo	Documento desarrollado y aprobado.	TIC-Subgerencia Administrativa	Segundo trimestre 2023.
Revisión y mejoramiento de acuerdos contractuales de funcionarios y contratistas para la inclusión de responsabilidades en cuanto a la seguridad de la información (acuerdos de confidencialidad)	Documento desarrollado y aprobado.	Tic-Contratación	Segundo trimestre 2023.

8.3. Implementación

La Corporación Social de Cundinamarca en esta etapa concluirá con la planificación anteriormente expresa, mediante desarrollo de procesos y controles necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos. Se establecerán procesos con criterios que permitan medir

la efectividad, eficiencia y eficacia de las acciones implementadas en el Modelo de Seguridad y Privacidad de la Información.

Tabla No. 6. Etapa de implementación CSC

Actividades	Descripción	Área interesada **(Responsable)**	Periodo de ejecución
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	TIC-Subgerencia Administrativa	Segundo trimestre 2023.
Capacitación en Seguridad de la información a funcionarios acorde a su función	Incentivar la cultura de seguridad mediante capacitaciones a los funcionarios de la CSC.	TIC-Subgerencia Administrativa	Tercer trimestre 2023.
Implementación del plan de tratamiento de riesgos.	Actualización del Plan de riesgos de SPI.	TIC-Subgerencia Administrativa	Último trimestre 2023.
Revisión y mejoramiento del procedimiento de copias de seguridad de información	Documento actualizado del procedimiento.	TIC-Subgerencia Administrativa	Segundo trimestre 2023.
Revisión de usuarios activos en las plataformas tecnológicas de la CSC.	Documento actualizado de usuarios activos.	TIC-Subgerencia Administrativa	Tercer trimestre 2023.
Implementación de mejoras y controles para solucionar vulnerabilidades técnicas	Documento de la oficina de sistemas.	TIC-Subgerencia Administrativa	Cuarto trimestre 2023.
Implementación	Documento con el	TIC-Subgerencia	Tercer trimestre

IPv6	informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la Oficina de TI.	Administrativa	2023.

8.4. Evaluación de desempeño

La Corporación Social de Cundinamarca realizara el proceso de seguimiento y monitoreo del MSPI con base a los resultados que arrojen las acciones implementadas, igualmente las auditorías realizadas.

Tabla No. 7. Evaluación de desempeño CSC.

Actividades	Descripción	Área interesada **(Responsable)**	Periodo de ejecución
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección. Guía No 16 – Evaluación del desempeño.	TIC-Subgerencia Administrativa	Cuarto trimestre 2023.
Plan de Ejecución de Auditorias.	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección. Guía No 15 – Guía de Auditoría.	TIC-Subgerencia Administrativa	Cuarto trimestre 2023.
Plan de pruebas de funcionalidad de IPv4 a IPv6.	Documento con los cambios detallados de las configuraciones realizadas, previo al	TIC, Subgerencia Administrativo.	Cuarto trimestre 2023.

	análisis de funcionalidad realizado en la fase II de Implementación. Acta de cumplimiento a satisfacción de la Entidad con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II de la implementación. Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6. Guía No 20 – Guía Transición de IPv4 a IPv6 para Colombia. Guía No 19 - Guía de Aseguramiento del Protocolo IPv6.		

8.5. Mejora Continua

En esta etapa la Corporación Social de Cundinamarca debe consolidar los resultados obtenidos en la fase de evaluación de desempeño, para diseñar el plan de mejoramiento dirigido a la seguridad y privacidad de la información.

Tabla No. 8. Plan de mejora continua en la CSC

Actividades	Descripción	Área interesada **(Responsable)**	Periodo de ejecución
Plan de mejora continua.	Documento con el plan de mejoramiento. Documento con el	TIC, Planeación, Subgerencia Administrativo.	Cuarto trimestre 2023.

	plan de comunicación de resultados.		

9. BIBLIOGRAFIA

Ciclos de MSPI. (2021). *Ministerio de las Tics*. Obtenido de https://www.mintic.gov.co/: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

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

Fases del protocolo IPv4 a IPv6. (2021). *Ministerios de las Tic*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

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

Pruebas de funcionalidad IPv4 a IPv6. (2021). *Ministerio de Tic*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.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