



**PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN**

ENERO 2022

REALIZÓ	REVISÓ	APROBÓ
JOSÉ RAIMUNDO PABÓN J CONTRATISTA DE LA CSC	COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO



Calle 39A #18-05 Bogotá D.C.
Sede Administrativa.
Código Postal: 111321 – Teléfono: 339 0150

f /Corporación Social de Cundinamarca
t @csc_corsocun www.csc.gov.co

Tabla de Contenido

1. INTRODUCCIÓN	5
2. OBJETIVO GENERAL.....	6
2.1. Objetivos específicos.....	6
3. GLOSARIO	7
4. GENERALIDADES.....	10
4.1. Entorno institucional.....	10
4.2. Misión Visión	10
4.2.1. Misión.....	10
4.2.2. Visión	10
4.3. Estructura Organizacional	11
4.4. Mapa de procesos de la CSC	11
5. POLITICA DE ADMINISTRACIÓN DEL RIESGO	13
6. METODOLOGÍA DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.....	14
6.1. Identificación de los activos de seguridad de la información	14
6.2. Identificación del Riesgo	16
6.3. Valoración del Riesgo	18
6.3.1. Criterios para definir la probabilidad	18
6.3.2. Criterios para definir el impacto	18
6.3.3. Niveles de severidad del riesgo.....	19
6.3.4. Controles asociados a la seguridad de la información.....	19
7. CRONOGRAMA.....	21
8. MAPA DE RIESGOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA CSC.....	22
9. BIBLIOGRAFIA	1



Tablas

Tabla 1. Términos y Siglas	7
Tabla 2. Activos de Información de la CSC	14
Tabla 3. Activos de procesos de la CSC	15
Tabla 4. Amenazas y vulnerabilidades	16
Tabla 5. Criterios para definir probabilidad	18
Tabla 6. Criterios para definir el impacto	18
Tabla 7. Algunos controles de MSPI	19
Tabla 8. Cronograma de actividades	21
Tabla 9. Mapa de riesgos SPI	22



Figuras

Ilustración 1. Organigrama CSC.....	11
Ilustración 2. Mapa de Procesos CSC	11
Ilustración 3. Niveles de severidad del riesgo.....	19



	PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: CSC-GI-FR-18 PÁGINA: 5 DE 27
--	--	---

1. INTRODUCCIÓN

La información que genera constantemente la Corporación Social de Cundinamarca es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales, es por ello que la seguridad y privacidad de la información se convierte en atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puede significar una alteración para el normal desarrollo en la prestación del servicio de la entidad.

De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Es por esto que Corporación Social de Cundinamarca adopta la metodología “del anexo 4 Lineamientos para la gestión del riesgo de seguridad Digital en Entidades públicas año 2018” del Departamento Administrativo de la Función Pública.

La corporación social de Cundinamarca implementa la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para mitigar, reducir, transferir o asumir el riesgo con medidas preventivas o correctivas de los riesgos informáticos.



	PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: CSC-GI-FR-18 PÁGINA: 6 DE 27
---	--	---

2. OBJETIVO GENERAL

Implementar una herramienta con un proceso sistemático que permita mitigar y reducir los riesgos Informáticos, en relación a los todos los procesos TIC de la CSC, a través de estrategias y procedimientos que faciliten la identificación, análisis, evaluación, valoración, y tratamiento de los riesgos, así como el seguimiento y monitoreo permanente focalizado a su cumplimiento y mejoramiento continuo para mitigar los riesgos de la Seguridad y privacidad de la Información.

2.1. Objetivos específicos

- Proporcionar una estrategia que permita a la CSC diligenciar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso.
- Presentar herramientas para identificar, analizar, evaluar y valorar los riesgos y determinar roles y responsabilidades de cada uno de los funcionarios de la entidad en los riesgos de gestión.
- Orientar una metodología fundamentado en una adecuada gestión del riesgo y controles de los mismos, que permitan a la dependencia encargada tener una seguridad en el logro de sus metas.
- Implementar el proceso de identificación y análisis de riesgos en la entidad enfocado en la Seguridad y Privacidad de la Información con la metodología de riesgos de la Función Pública.
- Anuar esfuerzos en la orientación de los aspectos comunes de las metodologías para la administración de todo tipo de riesgos informático y reforzar el enfoque preventivo con el fin de facilitar a la Corporación, la identificación, análisis y tratamiento de cada uno de los riesgos.



3. GLOSARIO

Tabla 1. Términos y Siglas

Términos y Siglas	Significado
Acceso a la Información Pública:	conjunto de elementos interrelacionados que brindan a la entidad la capacidad para ejecutar acciones necesarias que le permitan el manejo de actividades que puedan afectar negativamente el logro de los objetivos y protegerla de los efectos ocasionados por su funcionamiento diario
Análisis de riesgos:	Procedimiento sistemático de identificación, evaluación, registro y divulgación de información necesaria para formular sugerencias orientadas a la adopción de una posición o medidas en respuesta a un peligro.
Amenazas:	Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización
Apetito del Riesgo:	Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
Consecuencia:	Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
CICCI:	Comité Institucional de Coordinación de Control Interno.
Contingencia:	Posible evento futuro, condición o eventualidad.



Sede Administrativa.

Código Postal: 111321 – Teléfono: 339 0150



/Corporación Social de Cundinamarca



@csc_corsocun

www.csc.gov.co

Continuidad:	Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
Crisis (Emergencia):	Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
CGDI:	Comité de Gestión y Desempeño Institucional.
Datos Abiertos:	Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
Datos Personales:	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Datos Personales:	Públicos Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.
Mapa de Riesgos:	Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
MIPG:	Modelo Integrado de Planeación y Gestión
MECI:	Modelo Estándar de Control Interno.
OTIC:	Oficina de las Tecnologías de la Información y las Comunicaciones.
OAP:	Oficina Asesora de Planeación Bogotá D.C.

Restablecimiento:	Capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.
SIGI:	Sistema Gestión Institucional.
TIC:	Tecnologías de la Información y las Comunicaciones.
Vulnerabilidad:	Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.



	PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: CSC-GI-FR-18 PÁGINA: 10 DE 27
--	--	--

4. GENERALIDADES

4.1. Entorno institucional

La Corporación Social de Cundinamarca es un establecimiento público del orden departamental descentralizado, con personería jurídica, con autonomía administrativa, financiera y patrimonio independiente, que presta servicios de crédito y bienestar a sus afiliados y fue creada mediante la Ordenanza No. 5 del 17 de enero 1972, bajo la administración del Gobernador Diego Uribe Vargas y quien fuera su primer gerente Víctor Vega Gómez. La dirección y administración de la Corporación, está a cargo de la Junta Directiva y el Gerente, quien es el Representante Legal. La entidad que inició con 10 afiliados, en la actualidad cuenta con 15.350.

La principal función de la Corporación es la colocación de créditos bajo un amplio portafolio que busca dar soluciones a sus afiliados a fin de contribuir al mejoramiento de su calidad de vida.

En el 2015, dando cumplimiento a la ley 1527 de 2012 y por una recomendación de la Superintendencia Financiera, la Corporación decidió realizar la devolución de los aportes de ahorro recaudados hasta esa fecha. En febrero de 2016, como meta clara respecto al direccionamiento del Gobernador se desarrolló un Plan de devoluciones, el cual se ha cumplido según lo establecido. Además, en este año se obtuvo la recertificación bajo las Normas ISO 9001:2008 y NTCGP 1000:2009.

4.2. Misión Visión

4.2.1. Misión

La Corporación Social de Cundinamarca tiene como misión mejorar la calidad de vida de sus afiliados a través de planes y programas tendientes a captar su vinculación fomentar el crédito generar la cultura del ahorro buscar su felicidad y bienestar social y económico.

4.2.2. Visión

En el 2024 la Corporación Social de Cundinamarca, será posicionada como una entidad modelo en la oferta de soluciones crediticias, reconocida en el Departamento de Cundinamarca, con personal idóneo y un Sistema de Gestión de Calidad certificado, que

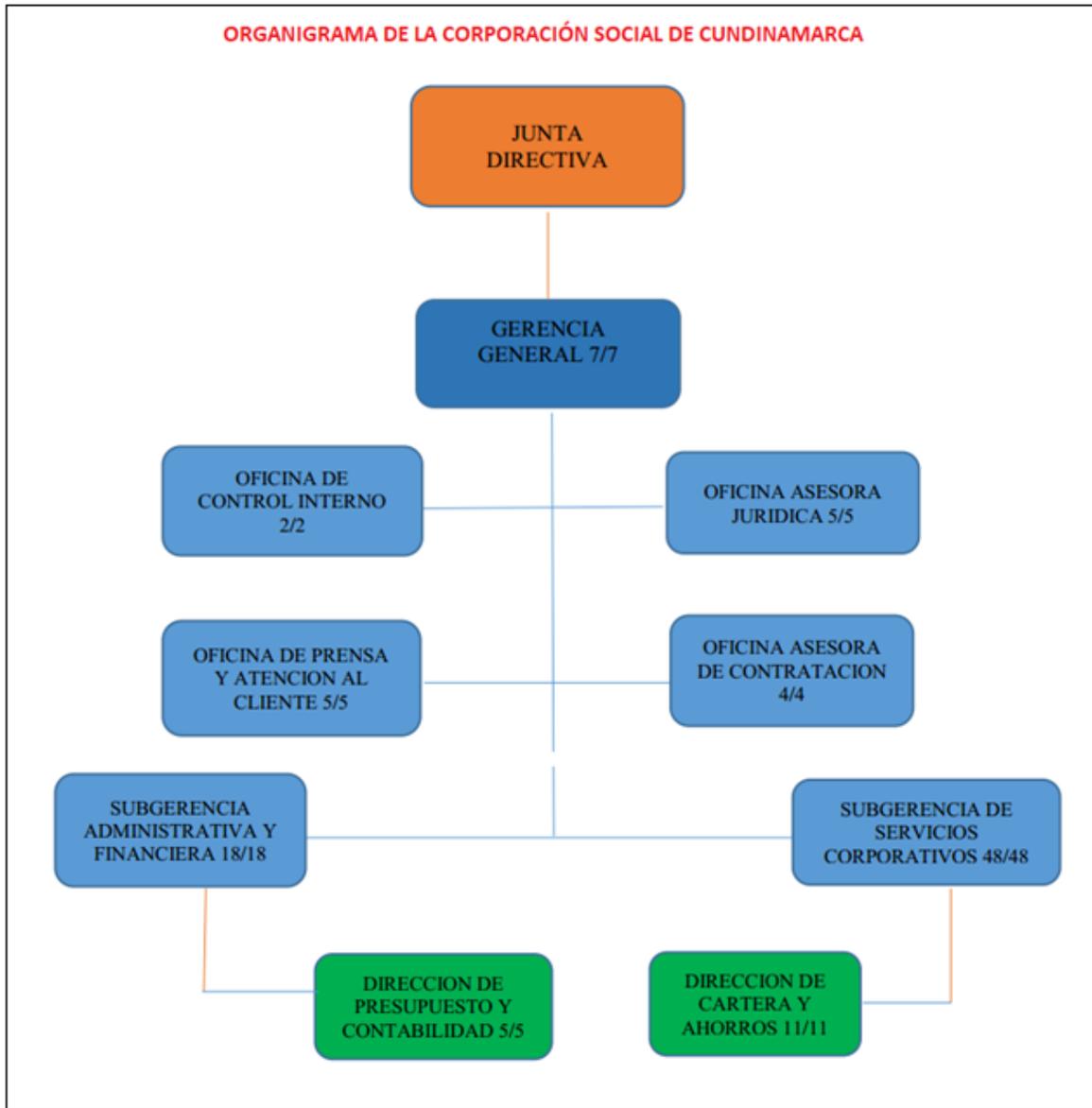


Calle 39A #18-05 Bogotá D.C.
Sede Administrativa.
Código Postal: 111321 – Teléfono: 339 0150
 /Corporación Social de Cundinamarca
 @csc_corsocun www.csc.gov.co

ofrezca créditos de manera ágil y eficiente con el fin de mejorar la calidad de vida de todos sus afiliados.

4.3. Estructura Organizacional

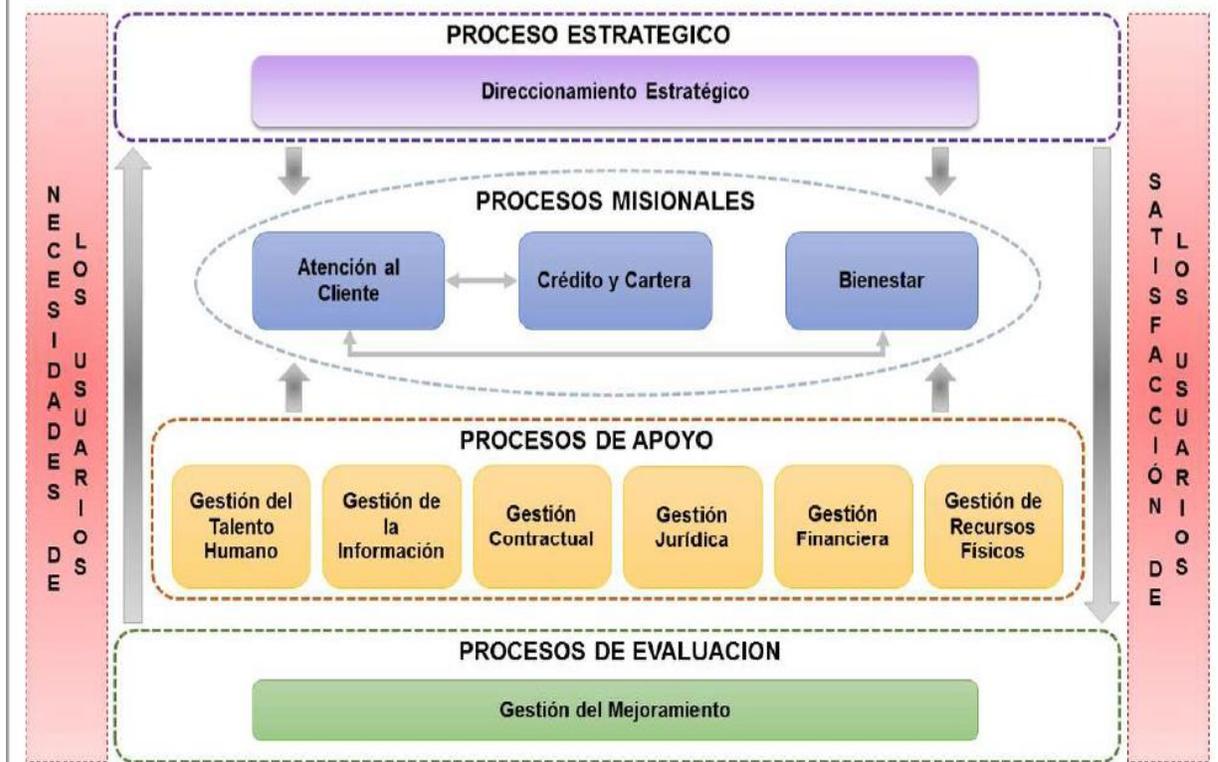
Ilustración 1. Organigrama CSC



4.4. Mapa de procesos de la CSC

Ilustración 2. Mapa de Procesos CSC





		PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: CSC-GI-FR-18
			PÁGINA: 13 DE 27

5. POLITICA DE ADMINISTRACIÓN DEL RIESGO

La Corporación Social de Cundinamarca, mediante el Modelo Integrado de Planeación y Gestión MIPG y la implementación del proceso de administración del riesgo asociados al desarrollo de los procesos y cumplimientos de las metas, en aras de cumplir con la obligación de diseñar, adoptar y divulgar las políticas, proyectos y programas de la tecnologías de la información que contribuyen al desarrollo social, económico y sobre todo al desarrollo integral de los afiliados a la CSC y a los ciudadanos en general.

El objetivo de esta política es implantar los parámetros necesarios para una adecuada gestión de riesgos de seguridad de la información y su tratamiento, donde podrá ser aplicada sobre cualquier proceso de la Corporación Social de Cundinamarca, a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- + Aceptar el riesgo: Ningún riesgo de corrupción es aceptado en la CSC. De pronto para los riesgos bajos, y para los riesgos que no se les puedan aplicar controles. Igualmente, para ambos casos se le debe realizar un seguimiento continuo.
- + Reducir el riesgo: se reduce la probabilidad o el impacto del riesgo mediante la implementación y seguimientos de los controles apropiados.
- + Evitar el riesgo: no se tienen en cuenta, ni se inicia, mucho menos se continua con las actividades que provocan los riesgos.
- + Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.



6. METODOLOGÍA DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

6.1. Identificación de los activos de seguridad de la información

El primer punto es identificar los activos vinculados a la información del proceso, en la Corporación Social de Cundinamarca agruparemos los activos de la siguiente manera:

Tabla 2. Activos de Información de la CSC

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



Sede Administrativa.

Código Postal: 111321 – Teléfono: 339 0150



/Corporación Social de Cundinamarca



@csc_corsocun

www.csc.gov.co

	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.

Tabla 3. Activos de procesos de la CSC

Proceso	Activo	Descripción	Responsable	Tipo de activo	Nivel de criticidad
Contabilidad	Bases de datos y aplicativo	Maneja la parte contable de la CSC	Subdirector de servicios administrativos	De información y de software	Media
Propiedad, Planta Y Equipo	Bases de datos y aplicativo	Los activos de infraestructura de la CSC	Subdirector de servicios administrativos	De información y de software	Media
Presupuesto De Gastos	Bases de datos y aplicativo	Gastos de la CSC	Subdirector de servicios administrativos	De información y de software	Media
Compras	Bases de datos y aplicativo	Registra las compras realizadas por la CSC	Subdirector de servicios administrativos	De información y de software	Media
Almacén Oficial	Bases de datos y aplicativo	Inventario de todas las compras realizadas por la CSC	Subdirector de servicios administrativos	De información y de software	Media
Activos Fijos	Bases de datos y aplicativo	Se registra y genera todos los activos fijos	Subdirector de servicios administrativos	De información y de software	Media
Contratación	Bases de datos y aplicativo	Maneja la información de las contrataciones realizadas por	Subdirector de servicios administrativos	De información y de software	Alta



la CSC					
Cuentas Por Pagar	Bases de datos y aplicativo	Cuentas por pagar	Subdirector de servicios administrativos	De información y de software	Media
Nomina	Bases de datos y aplicativo	Base de datos de la nómina de la CSC	Subdirector de servicios administrativos	De información y de software	Alta
Tesorería	Bases de datos y aplicativo	Registra todas las transacciones que realiza la CSC	Subdirector de servicios administrativos	De información y de software	Alta
Presupuesto de ingresos	Bases de datos y aplicativo	Transacciones de presupuestos de ingresos	Subdirector de servicios administrativos	De información y de software	Alta
Cartera financiera	Bases de datos y aplicativo	Transacciones y informes de la cartera	Subdirector de servicios administrativos	De información y de software	Alta
Información general	Bases de datos y aplicativo	Información general	Subdirector de servicios administrativos	De información y de software	Media
Contabilidad local	Bases de datos y aplicativo	Transacciones de contabilidad local	Subdirector de servicios administrativos	De información y de software	Media

6.2. Identificación del Riesgo

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Tabla 4. Amenazas y vulnerabilidades

Tipo de activo	Vulnerabilidad	Amenazas
  		Sede Administrativa. Código Postal: 111321 – Teléfono: 339 0150  /Corporación Social de Cundinamarca  @csc_corsocun www.csc.gov.co

Elementos de Red	Daños de Cableado y demás, y comunicación sin protección	Hurto de elementos, fallas técnicas, fenómenos sísmicos
Hardware	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad), Almacenamiento sin protección	Hurto de los equipos de cómputo, daño general, mal funcionamiento
Información	Falta de controles, falta de copias de seguridad	Hurto de la Información, fallas geológicas, fenómenos naturales.
Instalaciones	Red eléctrica inestable, humedad y falta de aire. Ausencia de protección en puertas o ventanas.	Fallas geológicas, fenómenos naturales, fallas técnicas, Acciones no autorizadas.
Intangibles	Suplantaciones	Hurto de identidad
Humanos	Ausencia del personal, falta de conocimiento, trabajo no supervisado por los funcionarios de la CSC	Funcionarios deshonestos, deficientes en conocimientos.
Servicios	Ausencia de procedimientos y/o de políticas que la CSC no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros.	Plataformas digitales piratas, hurto de información y de equipos técnicos.
Software	Ausencia o insuficiencia de pruebas de software, Ausencia de terminación de sesión, Ausencia de registros de auditoría, Asignación errada de los derechos de acceso, Interfaz de usuario compleja, Ausencia de documentación, Fechas incorrectas, Ausencia de mecanismos	Acciones no autorizadas, daño físico, fallas técnicas, compromisos de las funciones.

identificación y autenticación de usuarios, Contraseñas sin protección, Software nuevo o inmaduro.

6.3. Valoración del Riesgo

6.3.1. Criterios para definir la probabilidad

Tabla 5. Criterios para definir probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

(Guía para la administración del riesgo versión 5, 2020)

6.3.2. Criterios para definir el impacto

Tabla 6. Criterios para definir el impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.



Calle 39A #18-05 Bogotá D.C.

Sede Administrativa.

Código Postal: 111321 – Teléfono: 339 0150

 /Corporación Social de Cundinamarca

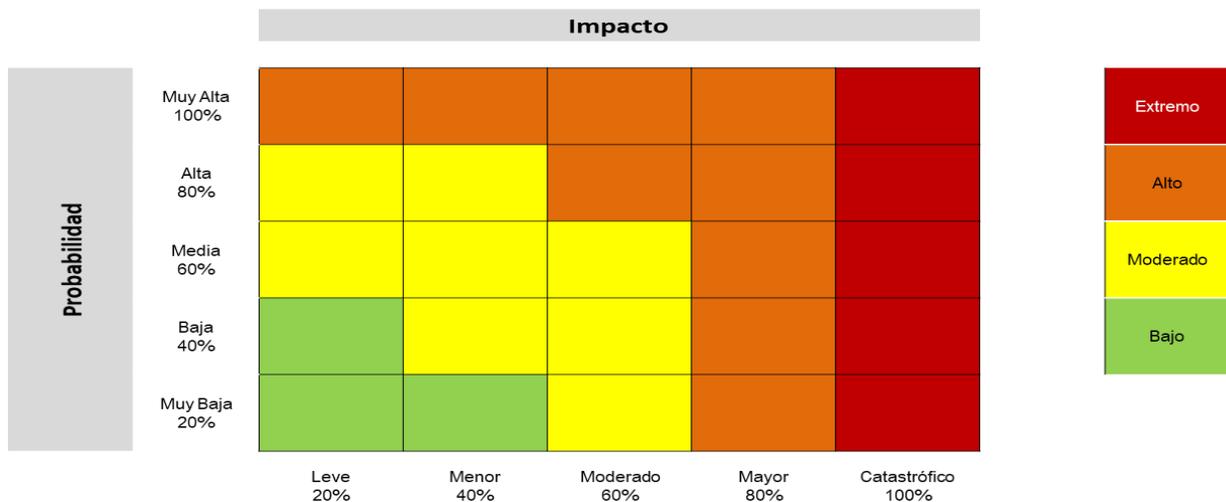
 @csc_corsocun www.csc.gov.co

Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país
-----------------------------	-------------------	---

(Guía para la administración del riesgo y diseños de controles versión 5, 2020)

6.3.3. Niveles de severidad del riesgo

Ilustración 3. Niveles de severidad del riesgo



(Guía para la administración del riesgo y diseños de controles versión 5, 2020)

6.3.4. Controles asociados a la seguridad de la información

La Corporación Social de Cundinamarca podrán reducir y atacar los riesgos de seguridad de la información empleando controles de SPI, se tomará como referencia Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos, a continuación, se muestra algunos ejemplos utilizados en la MSPI.

Tabla 7. Algunos controles de MSPI

Procedimientos operacionales y responsabilidades	Control
Procedimientos de operación documentados	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten
Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos, en las instalaciones y en los sistemas de



Calle 39A #18-05 Bogotá D.C.

Sede Administrativa.

Código Postal: 111321 – Teléfono: 339 0150

 /Corporación Social de Cundinamarca

 @csc_corsocun www.csc.gov.co

	procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Hay que asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Se debe separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos
Controles contra códigos maliciosos	Se debe implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Proteger la información contra la pérdida de datos
Respaldo de información	Se deben realizar copias de respaldo de la información, del software y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

(Guía para la administración del riesgo y diseños de controles versión 5, 2020)



7. CRONOGRAMA

Tabla 8. Cronograma de actividades

Actividades	2022			
	1er Trimestre	2do Trimestre	3er Trimestre	4to Trimestre
Identificar los activos de información de la entidad para gestionar los riesgos de seguridad de la información.				
Identificar las amenazas y la valoración de los daños que pueden producir.				
Revisar las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la CSC.				
las consecuencias operativas de los escenarios de incidentes en términos de: <ul style="list-style-type: none"> + Tiempo de investigación y reparación. + Pérdida de tiempo operacional. + Pérdida de oportunidad. + Salud y seguridad. 				
Generar la matriz integral de riesgos, con sus respectivos análisis, evaluación y tratamiento del riesgo.				
Socializar y comprometer a los funcionarios de CSC, en la formulación e implementación de controles y acciones encaminadas mitigar y administrar los riesgos.				
Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional				
Seguimiento al control del Plan de riesgos digitales				



8. MAPA DE RIESGOS DE LA

SEGURIDAD Y

PRIVACIDAD DE LA INFORMACIÓN DE LA CSC

Tabla 9. Mapa de riesgos SPI

No.	Riesgo	Activo	Tipo de riesgo	Amenazas	Tipo de Vulnerabilidad	Probabilidad	Impacto	Riesgo Residual	Opción de Tratamiento	Actividad de control	Tipo de control	Soporte	Responsable	Tiempo	Indicador %
1	Acceso a los sistemas de información por personas no autorizadas	Software	Seguridad digital	-Destrución de la información. -Divulgación ilegal de la información.	Ausencia de mecanismos de identificación y autenticación de usuarios. Contraseñas sin protección	Media	Alto	Media	Reducir	Acceso restringido a los códigos fuentes. Configurar restricciones en el servidor Firewall y consola de antivirus para cada uno de los equipos de la entidad. Implementación de mecanismos de control de navegación en internet a sitios potencialmente peligrosos.	Preventivo Preventivo Preventivo	El área de sistemas estará documentando todas las acciones de control de seguridad digital	Oficina de Sistemas de la corporación social de Cundinamarca.	cuatrimestre	No. de Intentos fallidos * Numero de sistemas de información / 365 días

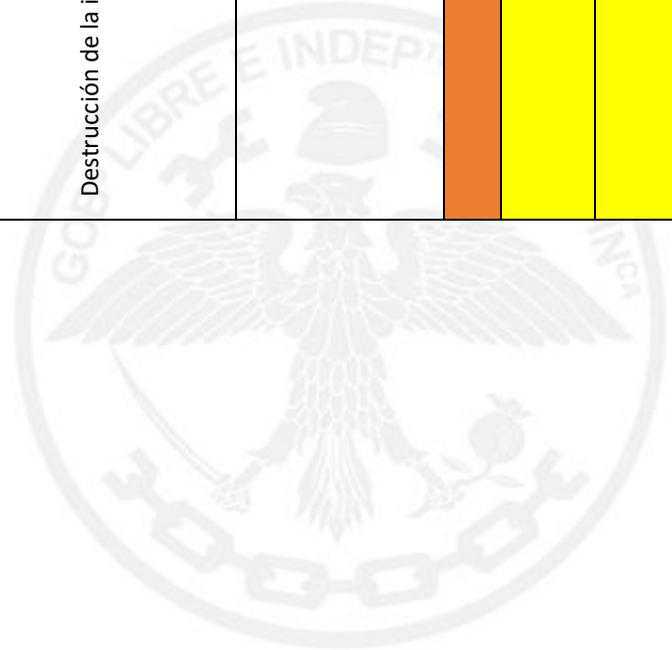


									Si hay acceso de información por parte de personas no autorizadas, se eliminará los permisos a los usuarios no autorizados.	Preventivo													
2	Mal funcionamiento de las redes LAN y WAN de la CSC	Elementos de Red	Seguridad digital	-Daño físico -Fallas técnicas -Intrusos	Ausencia de pruebas de envío o recepción de mensajes	Líneas de comunicación sin protección	Conexión deficiente de cableado	Tráfico sensible sin protección	Baja	Moderado	Medio	Reducir	Cambiar la arquitectura de la red para que el dispositivo de seguridad UTM monitoree tanto el tráfico interno como el tráfico de la VLAN de servidores.	Preventivo	Mantenimientos preventivos de la Red	Preventivo	La CSC cuenta con funcionalidades de Firewall, IDS, IPS, antivirus, restricción de contenido.	Preventivo	Las redes Wi-Fi están protegidas mediante una contraseña WPA2.	Documentado las actividades de mantenimiento y demás con un organigrama actualizado de las actividades.	Oficina de Sistemas de la corporación social de Cundinamarca.	Semestral	No de fallas sobre los 365 días de año

					Punto único de falla				El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño	Preventivo					
3	No tener disponibles los servicios de TI de la CSC/ No garantizar que la información sea accesible y usable bajo demanda de los usuarios autorizados, que, en todo momento debido a interrupciones del servicio por cortes de electricidad, fallos de hardware, daño de los sistemas de información etc.	Hardware	Seguridad digital	Falla o manipulación de la infraestructura de equipos de cómputo, electricidad, de protección, etc.	Baja capacidad tecnológica	Muy Alta	Mayor	Alta	Reducir	Manual de Políticas de seguridad y privacidad de la información (Código: - D103M01)	Preventivo	Se tiene documentado	Oficina de Sistemas de la corporación social de Cundinamarca	Semestrales	No. de sucesos sobre 365 días del año

4	El inadecuado uso o falta del Respaldo de información de la CSC	Software	Seguridad Digital	-Pérdida de la información	Ausencia del procedimiento de la programación de las copias de seguridad	Alta	Mayor	Moderado	Reducir	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	Preventivo	Programación de copias programadas a realizarse diariamente	Oficina de Sistemas de la corporación social de Cundinamarca	Diarias	No. de acciones sobre No. total, de copias de seguridad programadas en el año
5	Daño de hardware y software de los servidores de aplicaciones y demás plataformas.	Hardware y Software	Seguridad digital	Fallas del equipo, Mal funcionamiento del equipo, Saturación del sistema de información, Mal funcionamiento del software, Incumplimiento en el mantenimiento del sistema de información.	Mantenimiento o insuficiente	Alta	Moderado	Moderado	Reducir	Ejecución del Plan de mantenimiento, cumpliendo con el cronograma de actividades por parte del Auxiliar Administrativo de Gestión de la Información.	Preventivo	Cronograma de actividades de los mantenimientos previstos	Oficina de Sistemas de la corporación social de Cundinamarca	Cuatrimestrales	N° mantenimientos programados cuatrimestralmente sobre N° Total de mantenimientos ejecutados
	Ausencia de documentación														
	Software nuevo o inmaduro														

6	Intrusión y falta de integridad informática (hackers)	Software	Seguridad digital	Destrucción de la información Divulgación ilegal de la información	Perdida de información	Alta	Moderada	Moderada	Reducir	Seguridad permanente perimetral en la red CSC (FIREWALL)	Preventivo	Contrato de actualización del Firewall	Oficina de Sistemas de la corporación social de Cundinamarca	Anual	Actualización anual
---	---	----------	-------------------	--	------------------------	------	----------	----------	---------	--	------------	--	--	-------	---------------------



9. BIBLIOGRAFIA

Guía para la administración del riesgo versión 5. (2020). *Función Pública*. Obtenido de

[https://www.funcionpublica.gov.co:](https://www.funcionpublica.gov.co)

https://www.funcionpublica.gov.co/documents/28587410/38054865/2021-01-20_Guia_administracion_riesgos_f.pdf/6351b4f1-2299-8b6e-70b7-f99f6dd4c59a?t=1611257075079

Guía para la administración del riesgo y diseños de controles versión 5. (Diciembre de 2020).

Función pública. Obtenido de

https://www.funcionpublica.gov.co/documents/28587410/38054865/2021-01-20_Guia_administracion_riesgos_f.pdf/6351b4f1-2299-8b6e-70b7-f99f6dd4c59a?t=1611257075079

Guía para la administración del riesgo y diseños de controles versión 5. (Diciembre de 2020).

Función pública. Obtenido de

https://www.funcionpublica.gov.co/documents/28587410/38054865/2021-01-20_Guia_administracion_riesgos_f.pdf/6351b4f1-2299-8b6e-70b7-f99f6dd4c59a?t=1611257075079

Guía 7 gestiones de riegos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

Guía 8 controles de seguridad y privacidad de la información. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS del Ministerio de las tecnologías de la información TICs