POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

CORPOCESAR
CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR

SUBDIRECCIÓN GENERAL ÁREA DE PLANEACIÓN
OFICINA DE SISTEMAS Y TICS

TABLA DE CONTENIDO

1. OBJETIVO 3
2. DEFINICIONES/GLOSARIO 3
3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 5
4. COMPROMISO DE LA ALTA DIRECCIÓN 6
5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 7
6. APLICABILIDAD 7
7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES) 7
8. SANCIONES 9
9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI 10
10. APROBACIÓN Y REVISIONES A LA POLÍTICA 10

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR
CORPOCESAR

2023

1. OBJETIVO

Establecer los lineamientos definidos por la Alta Dirección de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.

2. DEFINICIONES/GLOSARIO

- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Seguridad Lógica:** Establece e integra los mecanismos y procedimientos, que permiten monitorear el acceso a los activos de información lógicos, que incluyen los controles de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a los sistemas de información de acuerdo a las necesidades y funciones del usuario, análisis de incidentes de seguridad lógica y lecciones aprendidas de los mismos, monitoreo de aplicaciones críticas, análisis forense, documentación sobre sistemas, software malicioso, y además, participa en la definición de la arquitectura de las soluciones para garantizar el

cumplimiento específico en los términos de seguridad de la información requeridos.

- **Seguridad Física:** Identifica los límites mínimos que se deben cumplir en cuanto a zonas seguras y perímetros de seguridad física, accesos físicos, control de ingreso y salida de activos, administración infraestructura locativa, entre otros, de forma que se puedan establecer controles que garanticen la seguridad de la información y del personal.
- **Activos de información:** Los activos de información en la compañía se clasifican de la siguiente manera: Software (incluye parametrizaciones, licencias, software genérico y a la medida, entre otros), hardware tecnológico, hardware no tecnológico (muebles, activos físicos, instalaciones, maestro de llaves, entre otros), información digital, documentación física, personas, intangibles (reputación, imagen, marca, good will, activos financieros, entre otros).
- **Continuidad de negocio:** La continuidad representa una serie de procesos coherentes encaminados a asegurar que la Entidad no experimente interrupciones inaceptables en cualquiera de sus operaciones esenciales, las cuales acarreen consecuencias financieras y operacionales e impacten negativamente a las partes interesadas.
- **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 de buenas

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.
- **SGSI:** Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

La **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Minimizar el riesgo de todos los procesos de la entidad.
- Mejorar continuamente el sistema de gestión de seguridad de la información.
- Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información conforme a los requisitos normativos comprende a todos los procesos de la entidad.

6. APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la entidad, servidores públicos, contratistas y terceros de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR**.

El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc....):

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Alta Dirección	• Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
	información (Recursos económicos, formación y recursos tecnológicos).
Comité de Gestión y Desempeño	• Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información.
Grupo TIC	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
Oficial de Seguridad Digital	• Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. • Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad.
Talento Humano	• Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
Control Interno	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Prensa / Comunicación Interna	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Oficina de Contratación	• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Líderes de Proceso	• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
Todos los funcionarios y contratistas	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.

8. SANCIONES

a. Cualquier violación a las políticas de seguridad de la información de la **CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR** debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

b. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de la misma.

9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR - CORPOCESAR indica que realizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

10. APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la Alta Dirección. La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la entidad (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran que la política requiera cambios.

11. CONTROL DE CAMBIOS

Responsable	Versión	Fecha	Cambios
AITE SOLUTIONS SAS	1	01-04-2014	Creación del documento.
Mauricio Garcés Ordoñez	2	31-01-2019	Ajustes de acuerdo con los lineamientos establecidos por el MinTIC.
Mauricio Garcés -Ordoñez	3	25-08-2023	Ajustes de la política general de acuerdo con los nuevos lineamientos de MinTIC

Elaborado por	Revisado por	Aprobado por
Nombre y Cargo		
MAURICIO GARCES ORDÓÑEZ Profesional Especializado de Sistemas y TICs	**YOHASKY FIORELLA CABALLERO OSPINO** Profesional de Apoyo SGAP. SIG-C	**WILMEN JOSE VASQUEZ**– Coord. GIT para la Gestión del Área de Sistemas y TICS. **MÓNICA INÉS GONZÁLEZ THOMAS** Subdirectora General Área Planeación (e)