1. Objetivo del documento y alcance

La presente política establece los **principios, compromisos y lineamientos estratégicos** para la protección de la información en todos los procesos, servicios y activos tecnológicos de la organización. **Aplica** a todas las personas, recursos y sistemas que participan en la operación, gestión y soporte de la información corporativa, y constituye la base del Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con los lineamientos de la norma ISO/IEC 27001.

2. Alcance del SGSI y estructura de soporte

La definición del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) se encuentra documentada formalmente en el documento **"Alcance, Misión, Visión" del SIG**, el cual ha sido establecido con base en el contexto organizacional, los requisitos de las partes interesadas y las necesidades de protección de los activos críticos de información.

Dicho alcance contempla los **procesos, servicios, activos y sede** que hacen parte del sistema, así como los elementos que permiten su operación y sostenibilidad, entre los cuales se destacan:

- Infraestructura crítica de tecnología e información, que soporta los servicios y operaciones incluidas en el SGSI.
- Interfaces y dependencias con terceros, como proveedores de servicios tecnológicos, aliados estratégicos y plataformas externas, cuya gestión y control son considerados dentro del sistema.

El documento de alcance debe ser consultado como referencia oficial para entender los límites, aplicabilidad, exclusiones justificadas y estructura técnica que respalda el SGSI.

3. Objetivos de Seguridad de la Información

1. Garantizar la protección de los activos críticos de la empresa
2. Velar por la disponibilidad de los servicios
3. Asegurar la continuidad del negocio
4. Mantener el cumplimiento de los requerimientos contractuales para los proyectos
5. Alcanzar la conformidad del SGSI según los requisitos de la ISO 27001
6. Incluir tecnología que provea apoyo a la gestión del sistema de seguridad de la información.

4. Política de Seguridad de la Información

La empresa establece su compromiso de implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI), reconociendo la importancia de una gestión eficaz de los activos y de la información como base para generar confianza en el desarrollo de sus actividades internas y en la prestación de servicios.

Este compromiso se enmarca en el cumplimiento estricto de la legislación aplicable y en coherencia con la misión y visión organizacional, promoviendo una cultura orientada a la protección de los activos de información.

La organización adopta y sostiene los principios fundamentales de la seguridad de la información:

- Confidencialidad: acceso solo por personas autorizadas.
- Integridad: exactitud y completitud de la información.
- Disponibilidad: acceso oportuno a la información cuando se requiera.

En concordancia con estos principios, la empresa se compromete a:

- Proteger la información y los sistemas ante riesgos que puedan afectar la operación, la reputación y el cumplimiento normativo.
- Implementar mecanismos que permitan mantener un nivel de exposición al riesgo tolerable, alineado con las expectativas de los grupos de interés.
- Cumplir con los requisitos legales, regulatorios y contractuales relacionados con la seguridad de la información.
- Promover la innovación tecnológica como medio para fortalecer la protección de la información.
- Desarrollar, mantener y divulgar políticas, procedimientos y lineamientos relacionados con la seguridad de la información.
- Gestionar la seguridad de la información conforme a los estándares establecidos por la norma ISO/IEC 27001, mediante objetivos de control y dominios definidos en dicho marco.

5. Políticas complementarias de Seguridad de la Información

Dentro de las políticas establecidas y requeridas para la gestión correcta de la Seguridad de la Información, se han definido e implementado las siguientes:

- POLITICA DE DISPOSITIVOS MOVILES
- POLITICA DE CONTROL DE ACCESO LOGICO
- POLITICA DE CLASIFICACION ETIQUETADO Y MANEJO DE INFORMACION
- POLITICA DE CONTROLES CRIPTOGRÁFICOS Y GESTION DE LLAVES
- POLITICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA
- POLITICA DE SEGURIDAD EN LAS RELACIONES CON PROVEEDORES
- POLITICA DE DESARROLLO SEGURO
- LINEAMIENTOS DE SEGURIDAD DE LA INFORMACION PARA EL DESARROLLO DE SOFTWARE
- LINEAMIENTOS PARA LE GESTION DE CONTRASEÑAS

- POLÍTICA DE CALIDAD OPERATIVA
- POLITICA DE CONTROL DE ACCESO FISICO
- POLITICA DE USO ACEPTABLE DE ACTIVOS
- POLITICA DE BACK UP DE LA INFORMACION
- POLITICA DE TELETRABAJO
- IMPLEMENTACION Y OPERACION DE SERVICIOS BPO
- POLITICA DEL SISTEMA INTEGRADO DE GESTIÓN
- POLITICA DE TRANSFERENCIA DE INFORMACION
- POLITICA PARA EL TRATAMIENTO DE DATOS PERSONALES
- LINEAMIENTOS PARA LA GOBERNANZA, SEGURIDAD Y USO CONFIABLE DE LA INTELIGENCIA ARTIFICIAL

Nota: El contenido específico de cada una está indicado en la política particular a cada tema.

6. Roles y Responsabilidades en Seguridad de la Información

Gerencia General

La Gerencia General lidera estratégicamente el Sistema de Gestión de Seguridad de la Información (SGSI), asegurando su alineación con los objetivos institucionales. Sus principales responsabilidades son:

- Definir y aprobar los objetivos estratégicos en materia de seguridad de la información.
- Asignar los recursos necesarios para el funcionamiento y mejora del SGSI.
- Aprobar las políticas y lineamientos clave del sistema.
- Impulsar la implementación y la cultura de seguridad de la información en toda la organización.
- Supervisar el cumplimiento de las obligaciones regulatorias.
- Evaluar y aprobar proyectos estratégicos asociados a la seguridad de la información.

Comité Directivo

El Comité Directivo opera como una instancia de decisión táctica y estratégica que apoya la gestión del SGSI, asegurando su alineación con los objetivos organizacionales y facilitando la implementación efectiva de los lineamientos institucionales en materia de seguridad de la información.

Sus principales responsabilidades son:

- Revisar periódicamente el estado del SGSI y proponer acciones para su mejora continua.
- Analizar los riesgos relevantes y las recomendaciones derivadas de los análisis de impacto (BIA) y evaluación de vulnerabilidades.
- Validar la pertinencia de controles y medidas implementadas, y proponer ajustes cuando sea necesario.
- Supervisar el cumplimiento de los planes y proyectos de seguridad de la información aprobados por la Gerencia General.
- Apoyar la integración de la seguridad de la información en todos los procesos organizacionales.

- Coordinar acciones con las diferentes áreas para asegurar el cumplimiento normativo y contractual en materia de seguridad.
- Facilitar la toma de decisiones cuando se presenten incidentes de seguridad de alto impacto.

Gerentes de Area

Son responsables de asegurar que las actividades bajo su gestión se desarrollen conforme a los lineamientos establecidos por el SGSI, actuando como puente entre la política de seguridad de la información y su aplicación práctica en el entorno operativo.

Sus responsabilidades incluyen:

- Implementar y mantener los controles de seguridad definidos para su proceso.
- Asegurar la correcta clasificación, uso y protección de la información que gestionan.
- Identificar y reportar riesgos o incidentes relacionados con la seguridad de la información.
- Promover la cultura de seguridad dentro de sus equipos de trabajo.
- Participar activamente en actividades de sensibilización, formación y auditorías internas.
- Colaborar con el Comité Directivo y el Oficial de Seguridad de la Información en la actualización de políticas, procedimientos o controles cuando se identifiquen brechas o cambios relevantes.

Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información (OSI) es el responsable designado para coordinar, asesorar y monitorear la implementación del SGSI. Actúa como punto focal entre la estrategia organizacional y la aplicación de las medidas de seguridad, asegurando el cumplimiento de los requisitos normativos, contractuales y técnicos.

Sus responsabilidades incluyen:

- Coordinar la implementación y mantenimiento del SGSI.
- Gestionar la documentación del sistema y asegurar su actualización.
- Coordinar la identificación, análisis y tratamiento de riesgos de seguridad de la información.
- Hacer seguimiento a los controles establecidos y proponer ajustes cuando sea necesario.
- Consolidar información para la revisión por la dirección y auditorías internas o externas.
- Promover acciones de sensibilización, formación y cultura de seguridad.
- Actuar como enlace con entes de control, autoridades competentes y grupos de interés cuando se presenten incidentes relevantes.

Colaboradores

Todos los colaboradores de la organización tienen la responsabilidad de **cumplir y aplicar los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI)**, actuando de forma consciente, ética y diligente frente al uso, manejo y protección de los activos de información.

Sus responsabilidades incluyen:

- Respetar las políticas, procedimientos e instructivos relacionados con la seguridad de la información.
- Garantizar la confidencialidad, integridad y disponibilidad de la información que manipulan o gestionan.
- Reportar de manera oportuna cualquier incidente, vulnerabilidad o anomalía que pueda afectar la seguridad de la información.
- Participar activamente en los procesos de capacitación y sensibilización en materia de seguridad.
- Utilizar los recursos tecnológicos de acuerdo con los lineamientos establecidos por la organización.

Contratistas y Terceros

Los contratistas, proveedores y terceros que acceden a la infraestructura tecnológica, sistemas o información de la organización están sujetos al cumplimiento de los lineamientos del SGSI, los acuerdos de confidencialidad y los compromisos establecidos en los contratos o convenios correspondientes.

Sus responsabilidades incluyen:

- Cumplir con los acuerdos de confidencialidad y niveles de acceso autorizados.
- Asegurar el tratamiento adecuado de la información a la que tengan acceso en el marco de sus funciones o servicios.
- Atender las instrucciones de la organización respecto al uso de los recursos tecnológicos y procedimientos de seguridad.
- Reportar de inmediato cualquier incidente, filtración o situación anómala que afecte los activos o la información.
- Participar, cuando se requiera, en actividades de inducción o formación relacionadas con la seguridad de la información.

7. Implementación y mantenimiento del SGSI

La implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI) se realiza mediante un conjunto de actividades estructuradas que permiten asegurar su eficacia, alineación con los objetivos institucionales y mejora continua.
Las principales actividades que conforman el ciclo de implementación y mantenimiento del SGSI incluyen:

- Definición y actualización del alcance del SGSI, considerando los procesos, servicios, activos y sedes relevantes.
- Análisis del contexto organizacional y de las partes interesadas, conforme a los numerales 4.1 y 4.2 de la norma.

- Identificación, evaluación y tratamiento de riesgos que puedan afectar la seguridad de la información.
- Determinación de controles aplicables y elaboración de la Declaración de Aplicabilidad (SoA).
- Despliegue de controles técnicos, administrativos y físicos, alineados con el Anexo A de la norma ISO/IEC 27001.
- Ejecución de auditorías internas, revisión por la dirección y acciones de mejora continua.
- Promoción de la cultura de seguridad, mediante campañas de sensibilización y formación.
- Documentación, control y revisión periódica de los procedimientos, políticas e instructivos asociados.

8. Contacto con autoridades y grupos de interés especial

Autoridades

Situación	Entidad	Contacto	Responsable de informar
Acceso abusivo a sistemas de información, phishing, suplantación de sitios web, violación de datos personales, uso de software malicioso, transferencia no consentida de activos, hurto por medios informáticos, ingeniería social	Centro Cibernético Policial (CCP)	Tel: (601) 515 9700 ext. 30428 Correo: dijin.cecip-jef@policia.gov.co https://www.policia.gov.co/contenido/centro-cibernetico-policial	Gerente Tecnología e Infraestructura
Emergencias cibernéticas	ColCERT	https://www.colcert.gov.co/	Representante Legal
Incidentes de seguridad informática	CSIRT-CCIT	http://www.csirt-ccit.org.co	Gerente Tecnología e Infraestructura
Emergencias por incendio	Bomberos de Bogotá	Línea de emergencia: 123 Tel: (601) 382 2500 ext. 40101 – 40102 Cel: 316 473 9599 WhatsApp: 317 404 3709 https://www.bomberosbogota.gov.co/	Gerente Administrativo y Financiero
Robo, emergencias generales	Policía Nacional	Línea de emergencia: 123/112 Tel: (601) 515 9000 https://www.policia.gov.co/	Gerente Administrativo y Financiero
Antisecuestro / Antiextorsión	GAULA Policía Nacional	Línea gratuita: 165 Tel: 317 896 5468 Correo: gabog@policia.gov.co https://www.policia.gov.co/contenido/gaula-metropolitana-bogota-0	Subgerente
Siniestros ambientales	Defensa Civil Colombiana	Línea de emergencia: 144 / 123 Tel: 601 319 9000 ext 124 Correo: orientacionciudadana@defensacivil.gov.co https://www.defensacivil.gov.co/	Gerente Control Mejora Innovación

Situación	Entidad	Contacto	Responsable de informar
Incidentes laborales, primeros auxilios	Cruz Roja Colombiana	Línea de emergencia: 112 Línea nacional gratuita: 01 8000 110 002 Correo: cruzrojateescucha@cruzrojacolombiana.org https://www.cruzrojacolombiana.org/	Gerente Talento Humano
Intoxicaciones, emergencias toxicológicas	Línea Nacional de Toxicología (MinSalud)	Línea gratuita: 01 8000 916 012 Tel: (601) 288 6012 https://www.minsalud.gov.co/salud/PServicios/paginas/linea-nacional-de-toxicologia.aspx	Gerente Talento Humano
Delitos complejos, investigaciones	DIJIN – Dirección de Investigación Criminal e INTERPOL	Tel: (601) 515 9700 ext. 30409 Correo: dijin.jefat@policia.gov.co https://www.policia.gov.co/contenido/direccion	Subgerente

Grupos de especial interés

Los grupos de interés son importantes para compartir conocimientos, identificar oportunidades de mejora, mejores prácticas, recibir capacitación y conocer cambios en el sector de SI. A continuación, se mencionan los relevantes:

Fuente de referencia técnica / Entidad	Aporte al SGSI
Asociación Colombiana de Contact Center y BPO (BPRO)	Monitorea tendencias, cambios regulatorios y avances del sector; útil para anticipar riesgos y oportunidades.
Asociación Colombiana de Inteligencia Artificial (ACIA)	Aporta en la identificación de tendencias tecnológicas y riesgos emergentes vinculados con IA.
ISO /IEC y sus comités técnicos	Referente oficial para los estándares internacionales en seguridad. Evolución de normas aplicables como ISO 27001, 27002.
CONPES o Gobierno Digital (MinTIC)	Normativa nacional, guías sobre IA responsable y transformación digital.
NIST (National Institute of Standards and Technology)	Profundización técnica, referencia internacional. Fuente confiable y global de marcos como NIST CSF, guías de gestión de riesgos, guías para IA segura.
IT Service	Fuente de formación y buenas prácticas en tecnología de la información, útil para mantener competencias técnicas actualizadas.
CQR	Provee servicios de certificación y auditoría en temas de seguridad; aporta en verificación de controles.
Microsoft	Proveedor de tecnología utilizada internamente (Office, Azure, etc.); clave para gestión de vulnerabilidades y parches.
Fortinet	Fabricante de soluciones de ciberseguridad; fuente de referencia para controles y actualizaciones.
ESET / WeLiveSecurity	Fuente confiable de alertas, formación y campañas de cultura de seguridad de la información.

Anexo - Términos y Definiciones

Activo
Cualquier recurso que tiene valor para la organización, como hardware, software, documentos, infraestructura, servicios o información.

Amenaza
Evento o condición que podría causar daño a los activos de información o afectar su seguridad.

Confidencialidad
Propiedad de la información que asegura que solo las personas autorizadas pueden acceder a ella.

Disponibilidad
Capacidad de la información o los sistemas para estar accesibles y utilizables cuando se requieran.

Incidente de seguridad de la información
Evento inesperado que puede comprometer la confidencialidad, integridad o disponibilidad de la información.

Integridad
Propiedad que asegura que la información es exacta, completa y no ha sido modificada de forma no autorizada.

Política
Declaración, intenciones y directrices de la compañía, expresadas por la dirección general.

Riesgo
Posibilidad de que una amenaza explote una vulnerabilidad, causando un impacto negativo en la organización.

Seguridad de la información
Protección de la confidencialidad, integridad y disponibilidad de la información, así como de otros aspectos como la autenticidad y la trazabilidad.

Sistema de gestión de seguridad de la información (SGSI)
Conjunto de políticas, procesos y recursos utilizados para gestionar la seguridad de la información en la organización y mejorarla continuamente.

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA DE APROBACIÓN**	**DESCRIPCION**
01	16-02-2022	Creación del documento.
02	17-05-2022	Se adiciona listado de partes interesadas. Se describe brevemente la intensión de cada política que hace parte del sistema.
03	27-06-2023	Se ajustó la declaración de la política, se adicionan los objetivos y el responsable, se actualizan los ítems de las políticas que hay de seguridad.
04	02/01/2024	Cambio de la clasificación del documento, de Privado a Público.
05	06/03/2024	Actualización de los siguientes elementos: • Objetivo de la política general • Objetivos de Seguridad de la Información conforme revisión por la Dirección. • Exclusión de los textos detallados para cada política indicada en el documento. • Inclusión del listado de las políticas que aplican para el Sistema de Seguridad de la Información
06	07/05/2024	Actualización del capítulo Políticas complementarias Seguridad de la Información: • Exclusión de las políticas relacionadas con medio ambiente, seguridad y salud en el trabajo, diversidad, equidad e inclusión y desconexión laboral, dado que sus alcances no incluyen la seguridad de la información. • Inclusión del documento Lineamientos de seguridad de la información para el desarrollo de software
07	06/12/2024	Inclusión de: ***"Lineamientos para la gestión de contraseñas",*** en el capítulo "Políticas complementarias Seguridad de la Información".
08	16/04/2025	• Actualización del nombre del documento teniendo en cuenta su contenido. • Actualización de la estructura del documento por capítulos, para un mejor entendimiento. • Ajuste en las responsabilidades de los roles, para alinearlos con el SGSI. • Actualización de los contactos de las autoridades y grupos de interés especial • Ajustes de redacción en todo el documento para aportar información de fácil entendimiento para las partes interesadas.