GRUPO COLPATRIA

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Grupo Empresarial Colpatria • Versión 01

INFORMACIÓN SEGURA, UN FUTURO MÁS FUERTE

## 01 OBJETIVO

Proteger la confidencialidad, integridad, disponibilidad, privacidad, autenticidad y no repudio de la información y sus sistemas. Enmarcar el Sistema de Gestión de Seguridad de la Información (SGSI) y gestionar sus riesgos dentro del SIAR.

## 02 COMPROMISOS

- Proteger la información como activo estratégico.
- Asignar recursos al SGSI.
- Cumplir requisitos legales, regulatorios y contractuales.
- Mejorar continuamente la eficacia de los controles.

## 03 PRINCIPIOS

- Enfoque basado en riesgos.
- Necesidad de saber y mínimo privilegio.
- Seguridad y privacidad desde el diseño y por defecto.
- Defensa en profundidad.
- Responsabilidad individual, trazabilidad y no repudio.
- Seguridad extendida a terceros.
- Mejora continua.

## 04 MODELO DE GOBIERNO

Se integra a la estructura existente, con segregación de funciones. La Junta Directiva aprueba la política y el apetito de riesgo. El Comité Estratégico autoriza excepciones; el Comité Ejecutivo asegura recursos, aprueba el plan anual y decide tratamientos de riesgo según sus competencias. El Subcomité de Riesgos y Auditoría supervisa y recomienda, sin facultad de aprobación. Transformación y Datos dirige el SGSI; la segunda linea ejerce contrapeso y Auditoría Interna evalúa independientemente.

## 05 RESPONSABILIDADES DE TODA LA PLANTILLA

La seguridad es responsabilidad de todas las personas, sin importar cargo, vinculación o ubicación. Cada colaborador debe aceptar la política y la confidencialidad; proteger y compartir información según su clasificación; no compartir credenciales; usar autenticación multifactor cuando corresponda y herramientas autorizadas; completar la formación; reportar de inmediato sin investigar ni borrar evidencia; devolver activos y mantener la confidencialidad tras el retiro. Los líderes revisan accesos y los usuarios privilegiados registran sus actividades.

## 06 INTEGRIDAD Y PROTECCIÓN DE LOS DATOS

Protegar la información durante todo su ciclo de vida: inventario y clasificación; accesos autorizados y mínimo privilegio; cifrado de información confidencial en reposo y tránsito; validación de datos, segregación de funciones y registros protegidos; gestión formal de cambios; respaldos cifrados con pruebas de restauración; prevención de fugas y eliminación segura. Los datos personales se tratan con base legal, finalidad autorizada, minimización y seguridad proporcional.

## 07 GESTIÓN DE RIESGOS

Dentro del SIAR: identificar → medir → controlar → monitorear. Actualizar la evaluación al menos anualmente y ante cambios significativos o incidentes relevantes. Evaluar proyectos y nuevas tecnologías antes de producción; gestionar los riesgos conforme al apetito aprobado.

## 08 MONITORIZACIÓN Y RESPUESTA A AMENAZAS

Correlacionar y analizar registros protegidos de sistemas críticos para detectar anomalías y atender alertas; consultar fuentes reconocidas de amenazas. Reportar inmediatamente incidentes o sospechas. El Encargado de Seguridad valida, clasifica y escala según severidad. La respuesta comprende contención → erradicación → recuperación → lecciones aprendidas, preservando evidencia. Los incidentes que puedan involucrar datos personales se informan de inmediato al área competente. El monitoreo del uso corporativo es proporcional, con aviso previo y respeto de la privacidad.

## 09 ANÁLISIS DE VULNERABILIDADES

Proceso continuo de identificación, analisis, priorización y remediación. Analizar infraestructura, aplicaciones y servicios críticos al menos anualmente y tras cambios significativos. Realizar pruebas de penetración anuales en servicios expuestos a internet y sistemas críticos por personal calificado e independiente. Corregir según severidad y verificar; si procede, aplicar controles compensatorios temporales aprobados.

## 10 REQUISITOS PARA TERCEROS Y PROVEEDORES

Exigir protección equivalente a la propia, proporcional a la criticidad y clasificación de los datos. Evaluar antes de contratar; pactar confidencialidad, seguridad, protección de datos, continuidad, auditoría o evidencias, cooperación y devolución o eliminación segura. Los contratos prevén notificación de incidentes en 24 horas desde su detección. Trasladar requisitos a subcontratistas tecnológicos; limitar y retirar accesos; reevaluar terceros críticos al menos anualmente o ante cambios significativos.

## 11 CONTINUIDAD DEL NEGOCIO

Integrar seguridad al Plan de Continuidad del Negocio (PCN) y al Plan de Recuperación ante Desastres (DRP). El análisis de impacto define procesos críticos y objetivos de recuperación. Mantener controles equivalentes durante contingencias y verificar un retorno seguro. Probar planes, restauración y simulacros de ciberincidentes al menos anualmente; actualizar con resultados. El Comité de Continuidad del Negocio y Gestión de Crisis activa los planes.

## 12 FORMACIÓN Y CONCIENTIZACIÓN

Inducción al ingreso y formación anual obligatoria con evaluación para todos los colaboradores; simulacros periódicos de phishing y refuerzo; capacitación por rol. Medir cobertura y resultados para mejorar el programa. Informar a proveedores y contratistas sobre sus obligaciones.

## 13 AUDITORÍA, CERTIFICACIONES Y MEJORA CONTINUA

Auditoría Interna evalúa independientemente el SGSI dentro de su plan anual basado en riesgos. Cada empresa puede adoptar evaluaciones externas o certificaciones según sus necesidades, con referencias como ISO/IEC 27001, ISO 22301, ISO/IEC 27701 y SOC 2. Mejorar continuamente los sistemas y controles de seguridad mediante Planear → Hacer → Verificar → Actuar: medir, probar y actualizar con incidentes, auditorías y evolución de amenazas. Revisar el SGSI al menos anualmente; asignar responsables y fechas a los hallazgos; eliminar causas raíz y verificar la eficacia de acciones correctivas.

## PROCEDIMIENTO ANTE INCUMPLIMIENTOS

La política establece el tratamiento de incumplimientos mediante el Reglamento Interno de Trabajo, el procedimiento disciplinario, el Código de Ética y los contratos, con debido proceso y proporcionalidad. Las faltas propias de la política son sancionables tras incorporarse al reglamento; entretanto aplican las ya previstas. Para terceros rigen consecuencias contractuales. Las denuncias pueden presentarse por el Canal de Integridad.

## APROBADA POR LA JUNTA DIRECTIVA



**Fuente:** Política Seguridad de la Información y Ciberseguridad, versión 01. Síntesis informativa; no sustituye la política.