

# Plan de seguridad y privacidad de la información

Versión 1  
Fecha: 9/12/2024



### Hoja de aprobación y control de cambios

<b>ELABORÓ / ACTUALIZÓ</b>	<b>Jaiber Ortíz Valdez</b> Profesional de TI	Fecha: 9/12/2024 Firma
<b>ELABORÓ/REVISÓ</b>	<b>Sebastián Marín Loaiza</b> Líder de infraestructura y TI	Fecha: 9/12/2024 Firma
<b>APROBÓ</b>	<b>Virmar Yessid David Valle</b> Subdirector administrativo y financiero	Fecha: 11/12/2024 Firma

<b>VERSIÓN</b>	<b>DESCRIPCIÓN / CONTROL DE CAMBIOS</b>	<b>FECHA DE APROBACIÓN</b>
1	Primera versión del documento	9/12/2024



## ÍNDICE

1. Introducción: .....	4
2. Alcance:.....	4
3. Estrategias y acciones: .....	4
4. Roles y responsabilidades:.....	5
5. Indicadores de desempeño:.....	6
6. Cronograma:.....	6





## 1. Introducción:

Establecer mecanismos de seguridad y privacidad para proteger la confidencialidad, integridad y disponibilidad de los activos de información, de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la normatividad internacional.

## 2. Alcance:

El plan aplicará a todos los niveles organizacionales de la Corporación Ruta N, dando alcance a nivel de procesos, activos de información y usuarios tanto internos como externos.

## 3. Estrategias y acciones:

### Sensibilización y Capacitación

#### 1. Capacitación:

- Capacitar a los empleados sobre las políticas de seguridad y privacidad de la información.
- Incluir módulos específicos sobre protección de datos y prevención de incidentes digitales.

#### 2. Comunicación interna:

- Difundir boletines informativos y cápsulas sobre ciberseguridad.
- Realizar simulaciones de ciberataques (phishing, ransomware) para evaluar y mejorar la preparación del personal.

### B. Gestión de Riesgos

#### 1. Evaluación continua:

- Monitorear los activos críticos y los riesgos asociados.
- Actualizar periódicamente la matriz de riesgos.

#### 2. Implementación de controles técnicos:

- Realizar cifrado de datos sensibles en tránsito y almacenamiento.
- Implementar sistemas de detección de intrusos (IDS) y herramientas de monitoreo continuo.





## C. Protección de datos

### 1. Control de acceso:

- Usar autenticación multifactor (MFA) en sistemas clave.
- Implementar políticas de privilegio para usuarios.

### 2. Gestión de datos personales:

- Garantizar el cumplimiento de la Ley 1581 de 2012 sobre protección de datos.
- Establecer un proceso para manejar solicitudes de acceso, corrección o eliminación de datos.

## D. Respuesta y recuperación ante incidentes

### 1. Plan de continuidad del negocio:

- Diseñar un protocolo para asegurar la disponibilidad de sistemas críticos durante incidentes.

### 2. Gestión de incidentes:

- Crear un equipo de respuesta rápida.
- Documentar y analizar cada incidente para prevenir recurrencias.

## E. Auditoría y mejora continua

### 1. Evaluaciones internas:

- Verificar el cumplimiento de los controles establecidos.

### 2. Indicadores de desempeño:

- Porcentaje de controles implementados.
- Reducción en incidentes de seguridad reportados.

## 4. Roles y responsabilidades:

- **Líder de Infraestructura TI:** Coordinar la implementación y supervisión del plan.
- **Profesional TI:** Ejecutar las medidas técnicas y dar soporte.
- **Todos los empleados:** Cumplir con las políticas y participar en las capacitaciones.





## 5. Indicadores de desempeño:

- **Porcentaje de activos protegidos:** Número de activos con controles implementados respecto al total identificado.
- **Tasa de incidentes detectados vs. mitigados:** Relación entre eventos reportados y solucionados.

## 6. Cronograma:

Actividad Principal	Descripción	Meses
Diagnóstico y sensibilización inicial	Realizar un análisis inicial de riesgos y vulnerabilidades.	<b>3-6 meses</b>
	Capacitar al personal en políticas de seguridad y privacidad.	
Implementación de controles iniciales y capacitación	Implementar controles técnicos prioritarios como cifrado de datos y autenticación multifactor (MFA).	<b>6-9 meses</b>
	Realizar talleres prácticos sobre buenas prácticas de seguridad.	
Auditorías internas y ajustes según resultados	Ejecutar auditorías internas para evaluar el cumplimiento.	<b>9-12 meses</b>
	Ajustar medidas y procesos según los hallazgos de las auditorías.	

