



## Política de Seguridad de la Información

### 1. Introducción

La presente Política de Seguridad de la Información establece las directrices y procedimientos necesarios para proteger la confidencialidad, integridad y disponibilidad de la información en VIP SERVICIOS INTELIGENTES S.A.S. Esta política aplica a todos los empleados, contratistas, proveedores y cualquier otra parte con acceso a la información y sistemas de la organización.

### 2. Objetivo

El objetivo de esta política es definir y regular las medidas y prácticas para proteger la información sensible y garantizar que la organización cumpla con los requisitos legales, regulatorios y contractuales relacionados con la seguridad de la información.

### 3. Alcance

Esta política se aplica a todos los activos de información y sistemas, incluyendo hardware, software, datos, redes y procesos asociados, dentro de VIP SERVICIOS INTELIGENTES S.A.S.

### 4. Principios de Seguridad de la Información

- **Confidencialidad:** La información debe ser accesible solo para aquellas personas autorizadas y debe protegerse contra el acceso no autorizado.
- **Integridad:** La información debe ser precisa y completa, y debe protegerse contra modificaciones no autorizadas.
- **Disponibilidad:** La información y los sistemas deben estar disponibles para los usuarios autorizados cuando los necesiten.

### 5. Responsabilidades

- **Dirección de Seguridad de la Información:** Es responsable de la implementación, revisión y mantenimiento de esta política.
- **Usuarios:** Todos los usuarios de los sistemas de información deben cumplir con esta política y reportar cualquier incidente de seguridad.
- **Administradores de Sistemas:** Deben implementar medidas técnicas y operativas para proteger la información y garantizar el cumplimiento de esta política.



## 6. Gestión de Riesgos

La organización llevará a cabo evaluaciones de riesgos periódicas para identificar y evaluar las amenazas y vulnerabilidades a los activos de información. Basado en estas evaluaciones, se implementarán controles adecuados para mitigar los riesgos.

## 7. Control de Acceso

- **Autenticación:** Todos los usuarios deben autenticarse mediante métodos seguros antes de acceder a los sistemas de información.
- **Autorización:** El acceso a la información se basará en el principio de necesidad de conocer, y se otorgará de acuerdo con los roles y responsabilidades.

## 8. Protección de la Información

- **Cifrado:** La información sensible debe ser cifrada tanto en tránsito como en reposo.
- **Copias de Seguridad:** Se deben realizar copias de seguridad regulares de la información crítica para garantizar la recuperación en caso de pérdida o corrupción de datos.

## 9. Seguridad Física y Ambiental

Se deben implementar medidas físicas para proteger los activos de información contra el acceso no autorizado, daño o interferencia. Esto incluye el control de acceso a las instalaciones y la protección contra desastres naturales.

## 10. Gestión de Incidentes de Seguridad

Todos los incidentes de seguridad de la información deben ser reportados inmediatamente a la Dirección de Seguridad de la Información. La organización mantendrá un plan de respuesta a incidentes para manejar y mitigar los efectos de los incidentes de seguridad.

## 11. Formación y Conciencia

Se debe proporcionar formación periódica sobre seguridad de la información a todos los empleados y usuarios para asegurar que estén informados sobre las políticas, procedimientos y mejores prácticas de seguridad.



## **12. Cumplimiento y Auditoría**

La organización llevará a cabo auditorías internas y externas para asegurar el cumplimiento de esta política y las normativas aplicables. Cualquier incumplimiento será investigado y se tomarán las medidas correctivas necesarias.

## **13. Revisión y Actualización**

Esta política será revisada al menos anualmente y actualizada según sea necesario para reflejar cambios en la normativa, tecnología o riesgos de seguridad.

## **14. Aprobación y Enmiendas**

Esta política ha sido aprobada por la Dirección de VIP SERVICIOS INTELIGENTES S.A.S. Cualquier enmienda o modificación a esta política debe ser revisada y aprobada por el mismo.

## **15. Contacto**

Para cualquier consulta relacionada con esta política, contactar a la Dirección de Seguridad de la Información en [seguridad@vipserviciosinteligentes.com](mailto:seguridad@vipserviciosinteligentes.com)

---

**Firma del Responsable de Seguridad de la Información:**

---

SERGIO IVAN ISIDRO CELIS  
Ingeniero de la Red  
06/06/2024

Este documento debe ser distribuido a todos los empleados y partes interesadas para su conocimiento y cumplimiento.