Vita Wallet

POLÍTICA · VITA WALLET

Seguridad de la Información y **Ciberseguridad**

Política

Lineamientos de seguridad de la información en Vita Wallet

Confidencialidad · Integridad · Disponibilidad

Marzo 2025

Marzo 2025

Documento de uso interno · vitawallet.io

ÍNDICE

Contenido de la **política**

1 Objetivo
2 Alcance
3 Principios de Seguridad de la Información
4 Gestión de Seguridad en Accesos y Contraseñas
5 Gestión de Seguridad en Sistemas y Aplicaciones
6 Gestión de Registros y Monitoreo de Actividades (Logs)
7 Gestión de Vulnerabilidades y Actualizaciones
8 Gestión de Incidentes de Seguridad
9 Continuidad del Negocio y Recuperación ante Desastres
10 Cumplimiento Normativo y Mejora Continua

1. Objetivo

El objetivo de esta declaración es establecer los lineamientos de seguridad de la información en Vita Wallet, garantizando la confidencialidad, integridad y disponibilidad de los datos y activos digitales.

Como empresa fintech, entendemos la importancia de proteger la información de nuestros clientes, proveedores, colaboradores y terceros relacionados, asegurando que nuestras operaciones cumplan con los más altos estándares de seguridad.

2. Alcance

Esta política es aplicable a todos los procesos, sistemas, plataformas y colaboradores de Vita Wallet, incluyendo:

- La gestión y protección de la información desde su creación hasta su eliminación.
- Los accesos y permisos en sistemas digitales.
- La seguridad en transacciones y comunicaciones.
- La protección ante ciberataques y vulnerabilidades.
- La continuidad del negocio y recuperación ante incidentes.

Nuestra infraestructura y protocolos están alineados con las mejores prácticas de la industria y con los estándares de ISO 27001, asegurando un entorno seguro y confiable para nuestros usuarios.

3. Principios de Seguridad de la Información

Vita Wallet adopta un enfoque integral de seguridad basado en los siguientes principios:

- **Confidencialidad:** Protegemos la información sensible para evitar accesos no autorizados.
- **Integridad:** Aseguramos que los datos sean precisos y no sean modificados de manera indebida.
- **Disponibilidad:** Garantizamos que la información y los sistemas estén accesibles cuando se necesiten.

4. Gestión de Seguridad en Accesos y Contraseñas

Para proteger la información dentro de nuestros sistemas, implementamos:

- Accesos con autenticación multifactor (2FA) para todas las cuentas críticas.
- Uso de contraseñas robustas, con una longitud mínima y combinación de caracteres.
- Prohibición del uso compartido de credenciales y almacenamiento inseguro de claves.
- Control de accesos basado en roles (RBAC), limitando los permisos según la necesidad operativa.
- Revisión y auditoría periódica de los accesos y privilegios de los usuarios.

5. **Gestión** de Seguridad en Sistemas y Aplicaciones

Los sistemas y plataformas de Vita Wallet están protegidos mediante:

- Monitoreo constante de actividad y detección de amenazas.
- Implementación de firewalls, WAF y antivirus en nuestros entornos.
- Aplicación de cifrado de datos en reposo y en tránsito, asegurando la protección de la información.
- Pruebas de seguridad periódicas, incluyendo análisis de vulnerabilidades y ethical hacking.

6. **Gestión** de Registros y Monitoreo de Actividades (Logs)

Para garantizar la trazabilidad y seguridad de la información, registramos y analizamos eventos en nuestros sistemas:

- Registro automático de accesos, cambios y transacciones en la plataforma.
- Identificación de actividad inusual o intentos de acceso no autorizados.
- Análisis de eventos para la detección temprana de amenazas.

7. **Gestión** de Vulnerabilidades y Actualizaciones

Vita Wallet mantiene un enfoque proactivo para identificar y mitigar vulnerabilidades:

- Evaluaciones periódicas de seguridad en sistemas y aplicaciones.
- Instalación oportuna de actualizaciones y parches de seguridad.
- Implementación de procesos de revisión y pruebas antes de cambios en producción.

8. **Gestión** de Incidentes de Seguridad

Ante cualquier incidente de seguridad, Vita Wallet cuenta con un Plan de Respuesta a Incidentes, que incluye:

- Detección y análisis inmediato de amenazas.
- Mitigación y contención de impactos.
- Notificación a las partes afectadas, en caso de incidentes relevantes.
- Registro y análisis forense para prevenir futuros incidentes.

9. **Continuidad** del Negocio y Recuperación ante Desastres

Para garantizar la operación ininterrumpida de nuestros servicios, contamos con:

- Planes de recuperación ante desastres (DRP), asegurando la restauración de sistemas.
- Backups regulares y seguros, almacenados en múltiples ubicaciones.
- Pruebas de continuidad y simulacros periódicos.

10. Cumplimiento Normativo y Mejora Continua

Vita Wallet cumple con todas las normativas aplicables en materia de seguridad de la información, incluyendo las mejores prácticas de la industria y estándares como ISO 27001. Nuestra política de seguridad se revisa y actualiza periódicamente para adaptarse a nuevas amenazas y regulaciones.

La seguridad de la información es una responsabilidad compartida en Vita Wallet. Todos nuestros colaboradores, proveedores y clientes deben seguir los lineamientos establecidos para mantener un entorno seguro y confiable.