POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN WPOSS

2026

Powered by WPOSS WORLD POS SOLUTIONS

Información de contacto
World POS Solutions LLC
168 SE 1ST Street, Suite 1204,
FL 33131
+1 786 299 5294
Miami Florida
USA

REVISIONES

Versión	Fase	Responsable	Cargo	Fecha
1.0	Elaboración	Área de seguridad de la información	Oficial de seguridad de la información. Oficial de cumplimiento Analista de seguridad de la información	02 de mayo, 2026
	Revisión / aprobación	Responsable del proceso del SGSI	Jefe de información y tecnología	11 de junio, 2026
Cambios realizados	Elaboración del documento			

PROPÓSITO Y DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

World POS Solutions (WPOSS) reconoce que la información constituye uno de sus activos más críticos para la continuidad del negocio, la confianza de sus clientes y el cumplimiento regulatorio en las jurisdicciones donde opera. En WPOSS, la seguridad de la información se define como la preservación de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información en todos sus formatos y repositorios.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Todas las actividades en WPOSS se guiarán por los siguientes principios:

- **Protección integral:** Implementación de controles desde el diseño para proteger la información generada, procesada y transmitida.
- **Responsabilidad compartida:** La seguridad es responsabilidad de cada colaborador y tercero; todos deben cumplir con los controles establecidos que les corresponda.
- **Gestión del riesgo:** Toma de decisiones basada en la identificación, análisis y tratamiento de riesgos tecnológicos y de ciberseguridad.

ALCANCE Y APLICABILIDAD

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de WPOSS abarca los procesos estratégicos, misionales y de apoyo de la organización, incluyendo:

- **Procesos estratégicos:** Estrategia corporativa.
- **Procesos misionales:** Gestión comercial, gestión de proyectos (PMO), gestión de infraestructura tecnológica, desarrollo de software, QA y gestión de mesa de ayuda.
- **Procesos de apoyo:** Gestión de talento humano, seguridad de la información, soporte técnico interno, gestión financiera y operaciones.

Estos procesos están asociados a la prestación de servicios de diseño, desarrollo, comercialización, instalación, soporte técnico y mantenimiento de soluciones especializadas para los sectores bancarios, transaccionales y de medios de pago, incluyendo la gestión de infraestructura tecnológica, plataformas y servicios de soporte.

El alcance aplica a todos los activos de información, recursos tecnológicos, procesos y personal involucrado en la operación, incluyendo la Alta Dirección, colaboradores y terceros con acceso a la información de la organización, en las sedes y operaciones ubicadas en Ecuador y Colombia.

DECLARACIÓN Y COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de WPOSS asume el liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información (SGSI) mediante las siguientes declaraciones obligatorias:

- **Cumplimiento de requisitos:** El compromiso absoluto de satisfacer todos los requisitos legales, reglamentarios, estatutarios y contractuales aplicables a la seguridad de la información, incluyendo normativas financieras, y la legislación de protección de datos personales.
- **Mejora Continua:** El compromiso inquebrantable con la revisión, el mantenimiento y la mejora continua del SGSI para asegurar su idoneidad, adecuación y eficacia frente al cambiante panorama de riesgos y amenazas.

OBJETIVOS

Para garantizar la alineación con la estrategia del negocio, WPOSS establece el siguiente marco para la definición y evaluación de sus objetivos de seguridad de la información:

- Identificar, evaluar y gestionar proactivamente los riesgos de seguridad de la información para reducir su probabilidad e impacto.
- Fortalecer el conocimiento y la concienciación en seguridad de la información mediante la ejecución de planes de formación y sensibilización.
- Asegurar la resiliencia operativa y la continuidad de los servicios y procesos críticos del negocio ante cualquier eventualidad.
- Garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables mediante la gestión y actualización de la matriz de requisitos legales.
- Asegurar la confidencialidad y la integridad de la información transaccional y los datos procesados en las soluciones de medios de pago, e-commerce y sector bancario, previniendo incidentes de fuga o alteración.
- Garantizar una respuesta ágil y oportuna frente a los incidentes de seguridad de la información para minimizar su impacto en la operación tecnológica y en los clientes.

LINEAMIENTOS GENERALES DEL SGSI

Para ejecutar esta política, WPOSS implementará controles organizacionales, físicos, de personas y tecnológicos que garanticen:

- **Gestión de Activos y Control de Acceso:** Identificación, clasificación y asignación de propietarios para todos los activos de información, garantizando que su acceso se restrinja según el rol y el principio de necesidad de saber.
- **Seguridad Física y de Comunicaciones:** Protección contra accesos físicos no autorizados y aseguramiento de las redes y la información en tránsito.

- **Desarrollo y Adquisición Segura:** Separación de los entornos de desarrollo, pruebas y producción, y la incorporación de requisitos de seguridad desde la fase de diseño de todo software.
- **Gestión de Proveedores:** Exigencia, evaluación y seguimiento de acuerdos de nivel de servicio (SLA) y requisitos de seguridad contractuales en la cadena de suministro.
- **Gestión de Incidentes y Continuidad:** Identificación, reporte y respuesta oportuna ante eventos de seguridad, así como el mantenimiento y prueba periódica de los Planes de Continuidad (BCP) y Recuperación (DRP).

ROLES Y RESPONSABILIDADES

- **Alta Dirección:** Aprobar la política, asignar los recursos y garantizar la alineación con la estrategia del negocio.
- **Seguridad de la Información:** Definir, implementar, mantener el SGSI, evaluar riesgos y coordinar la respuesta a incidentes.
- **Dirección de Tecnología:** Garantizar la implementación de la arquitectura y los controles técnicos.
- **Colaboradores y Terceros:** Conocer, comprender y cumplir estrictamente los lineamientos, protegiendo los activos bajo su responsabilidad.

EXENCIONES Y EXCEPCIONES A LA POLÍTICA

Cualquier desviación, exención o excepción a los controles establecidos en esta política o en sus directrices específicas, deberá ser formalmente justificada por el riesgo de negocio, documentada y aprobada explícitamente por el área de Seguridad de la Información y la Alta Dirección antes de su implementación.

REVISIÓN Y ACTUALIZACIÓN

Esta política, junto con las políticas específicas por tema, será revisada a intervalos planificados (mínimo anualmente) o cuando se produzcan cambios significativos en el entorno regulatorio, la tecnología, o los riesgos del negocio, asegurando su idoneidad, adecuación y eficacia continua.