Política de Desarrollo Seguro de Software

Fecha: 07/10/2025

Versión: 2.0

Control de versiones

Fecha	Versión	Descripción	Autor
20/03/2023	0.1	Creación del Documento	PMO SGSI
20/03/2023	1.0	Revisión del Documento	Comité de Seguridad de la Información
28/03/2024	1.1	Revisión del Documento	Comité de Seguridad de la Información
07/10/2025	2.0	Actualización de Política según alcance e implementación de SGSI	Comité de Seguridad de la Información

Contenido

1 Objetivo

El objetivo de esta política es establecer los lineamientos que garanticen la incorporación de prácticas de desarrollo seguro en el ciclo de vida de los sistemas y aplicaciones de Interfase ISA, asegurando que la seguridad de la información sea considerada desde la fase de planificación hasta la puesta en producción.

Esta política busca reducir los riesgos de vulnerabilidades, proteger los activos de información y promover una cultura de "seguridad por diseño" en todas las etapas del desarrollo, en concordancia con los principios y controles definidos en el Sistema de Gestión de Seguridad de la Información (SGSI).

Esta política aplica un enfoque basado en riesgos y se integra con el análisis de riesgos del SGSI, garantizando que las decisiones de diseño, desarrollo, pruebas y despliegue consideren los riesgos de seguridad identificados y su impacto potencial en los activos de información.

2 Alcance

Aplica a todas las sedes de Interfase ISA, y a todos los colaboradores, contratistas, desarrolladores y proveedores que participen en actividades de análisis, diseño, construcción, pruebas, implementación o mantenimiento de software desarrollado o mantenido por la organización.

Abarca tanto los desarrollos internos como los servicios de desarrollo contratados a terceros, las integraciones con sistemas externos, y los proyectos ejecutados bajo cualquier metodología (ágil, tradicional o híbrida).

3 Roles y responsabilidades

El desarrollo seguro es una responsabilidad compartida entre las áreas de desarrollo, seguridad, proyectos y tecnología.

- Directorio: aprueba esta política, asigna los recursos necesarios y supervisa su cumplimiento mediante la Revisión por la Dirección.
- Comité de Seguridad: supervisa la aplicación de esta política, valida excepciones, revisa resultados de auditorías y eleva informes al Directorio.

- PM del SGSI: coordina la actualización y difusión de esta política, asegura su integración con las demás normas del SGSI y promueve la mejora continua de los controles de desarrollo.
- Jefatura de Desarrollo / Líder Técnico: garantiza que los equipos de desarrollo implementen prácticas seguras, definan los controles necesarios y mantengan la documentación de soporte (guías, estándares, revisiones de código, etc.).
- Equipo de Desarrollo: aplica las buenas prácticas definidas, utiliza componentes verificados y mantiene la confidencialidad del código fuente y de la información procesada.
- Responsable de Seguridad de la Información: apoya al equipo de desarrollo en la identificación y mitigación de riesgos, revisa vulnerabilidades y valida la seguridad antes de la liberación de los sistemas.

Las responsabilidades específicas y la segregación de funciones están definidas en la Matriz RACI del SGSI, que complementa esta política y constituye evidencia formal de auditoría.

4 Principios de desarrollo seguro

Interfase ISA promueve el desarrollo seguro bajo los siguientes principios rectores:

- Seguridad por diseño: la seguridad debe integrarse desde las fases iniciales de análisis y diseño del software.
- Mínimo privilegio: los sistemas deben otorgar únicamente los permisos necesarios para cada función o usuario.
- Separación de entornos: los ambientes de desarrollo, prueba y producción deben mantenerse completamente aislados.
- Validación continua: los controles de seguridad deben verificarse en cada etapa del ciclo de vida del desarrollo.
- Cumplimiento normativo: todo desarrollo debe alinearse con los requisitos de la Política General de Seguridad de la Información, las leyes de protección de datos y los contratos con clientes.

- Todos los desarrollos de software deberán ajustarse a los requerimientos de seguridad establecidos en los contratos con clientes, licitaciones o acuerdos de nivel de servicio (SLA), así como a las leyes de protección de datos y propiedad intelectual aplicables.

5 Seguridad en la planificación de proyectos

Durante la planificación de cada proyecto de desarrollo o mantenimiento de software deberán:

- Definirse los requerimientos de seguridad, roles, permisos, autenticación, auditoría y controles de acceso aplicables.
- Incorporarse hitos de validación en seguridad, que incluyan revisiones de código, pruebas de vulnerabilidad y reportes de resultados.
- Preverse la implementación de comunicaciones seguras (SSL/TLS) y cifrado de información sensible, tanto en tránsito como en reposo.
- Incluir en la planificación los controles de gestión de identidades, registro de eventos, trazabilidad y monitoreo de accesos.

6 Seguridad en el entorno de desarrollo

El entorno de desarrollo deberá mantenerse bajo estrictas medidas de control físico y lógico:

- Los accesos al código fuente y repositorios estarán restringidos a personal autorizado, con autenticación individual y registro de actividad.
- Los entornos de desarrollo, pruebas y producción deberán mantenerse separados y protegidos, evitando el uso de datos reales en ambientes no productivos.
- Se deberá utilizar software licenciado y actualizado, con mecanismos de validación de integridad para librerías y componentes de terceros.
- El almacenamiento del código y la gestión de versiones deberán realizarse en repositorios corporativos bajo control del Área de TI y Seguridad.
- Todo acceso a los repositorios de código y entornos de desarrollo deberá registrarse en un Registro de Accesos y Cambios de Código, conservado por el Área de TI como evidencia auditable dentro del SGSI. Además, los repositorios deberán someterse a

revisiones periódicas de integridad, verificando que no existan componentes obsoletos, vulnerabilidades conocidas o dependencias sin mantenimiento.

- Las herramientas utilizadas para el control de versiones y los entornos de prueba deberán documentarse en el inventario de activos del SGSI.

7 Pruebas y validaciones de seguridad

- Las pruebas de seguridad deberán planificarse desde la fase de diseño y realizarse en todas las etapas del desarrollo. Estas incluirán revisiones de código fuente, análisis estático y dinámico, pruebas de vulnerabilidad, pruebas de penetración (cuando aplique) y validación del cumplimiento de las guías OWASP Top 10. Los resultados de las pruebas deberán documentarse y conservarse como evidencia de cumplimiento dentro del SGSI, registrando las acciones correctivas derivadas.
- Cualquier hallazgo crítico deberá resolverse antes de la liberación del software o documentarse con una justificación aprobada por el Comité de Seguridad
- Los entornos de desarrollo, pruebas y producción deberán mantenerse separados y protegidos, evitando el uso de datos reales en ambientes no productivos.
- Se deberá utilizar software licenciado y actualizado, con mecanismos de validación de integridad para librerías y componentes de terceros.
- El almacenamiento del código y la gestión de versiones deberán realizarse en repositorios corporativos bajo control del Área de TI y Seguridad.

8 Capacitación y concientización

- El Comité de Seguridad y la Jefatura de Desarrollo deberán asegurar capacitaciones periódicas al personal técnico en buenas prácticas de desarrollo seguro, OWASP y técnicas de revisión de código.
- Los desarrolladores deberán estar familiarizados con las vulnerabilidades más comunes (por ejemplo, OWASP Top 10) y con los mecanismos de mitigación aplicables.
- Todo nuevo integrante del equipo de desarrollo deberá recibir inducción formal en seguridad de la información antes de incorporarse a proyectos activos.

9 Control de versiones y cambios

- Todo sistema deberá contar con un control de versiones formal que garantice la trazabilidad de los cambios, aprobaciones y despliegues.
- Cualquier modificación deberá seguir el Procedimiento de Control de Cambios de TI, con registros de revisión, aprobación y validación previa por parte de Seguridad.
- El código fuente deberá mantenerse bajo resguardo y copia de seguridad periódica, conservando evidencias de acceso y modificaciones.

10 Lecciones aprendidas

El Comité de Seguridad y la Jefatura de Desarrollo deberán analizar los incidentes o vulnerabilidades detectadas durante las pruebas o en producción, con el fin de identificar causas raíz y aplicar medidas preventivas.

Los resultados de estas revisiones se documentarán como Lecciones Aprendidas del Proceso de Desarrollo Seguro, y serán consideradas en futuras versiones del software o actualizaciones de la política.

Este enfoque garantiza la aplicación del ciclo PDCA (Planificar–Hacer–Verificar–Actuar) dentro del proceso de desarrollo.

11 Indicadores y revisión de eficacia

El Comité de Seguridad y el PM del SGSI medirán la eficacia de esta política mediante los siguientes indicadores:

- Porcentaje de proyectos con revisión de código completada.
- Número de vulnerabilidades críticas corregidas antes de liberación.
- Porcentaje de desarrolladores capacitados en OWASP o seguridad de software.
- Tiempo medio de resolución de vulnerabilidades detectadas.

Los resultados se presentarán al Directorio durante la Revisión por la Dirección y servirán de base para el plan anual de mejora del SGSI.

12 Cumplimiento y mejora continua

El cumplimiento de esta política es obligatorio para todos los colaboradores, contratistas y proveedores que participen en actividades de desarrollo de software bajo el ámbito del SGSI.

El Comité de Seguridad, junto con el PM del SGSI y la Jefatura de Desarrollo, supervisará la aplicación de los controles definidos, revisará la eficacia de las medidas implementadas y consolidará los resultados en un informe anual de cumplimiento presentado al Directorio durante la Revisión por la Dirección.

Los hallazgos detectados en auditorías o revisiones deberán gestionarse mediante acciones correctivas y preventivas, garantizando la mejora continua del proceso de desarrollo seguro.

13 Vigencia y Publicación

Esta política entra en vigencia a partir de su aprobación por el Directorio de Interfase ISA. La versión vigente será comunicada a todos los colaboradores mediante los canales institucionales oficiales y permanecerá disponible en la intranet corporativa, dentro del repositorio del SGSI.

El Comité de Seguridad es responsable de garantizar que solo la versión aprobada esté publicada y accesible, así como de coordinar su revisión anual o antes si se producen cambios tecnológicos, normativos u organizacionales relevantes.

Toda modificación deberá contar con la aprobación formal del Directorio antes de su aplicación, asegurando que la versión actualizada sea debidamente comunicada y registrada bajo control documental.

Versión	Fecha de aprobación	Próxima revisión	Aprobado por:
2.0	DD/MM/AAAA	DD/MM/AAAA	Directorio – Interfase ISA

tuid
FIRMA DIGITAL
Leonardo Adrian Noach Meierovich