



Política de Gestión de Activos de Información

Fecha: 18/09/2025
Versión: 2.0

 	Política de Gestión de Activos de Información	C-1 Información Pública
Versión: 2.0 Fecha: 18/09/2025		Página: 2 de 9

Control de versiones

Fecha	Versión	Descripción	Autor
15/11/2024	0.9	Creación del Documento	Comité de Seguridad de la Información
29/11/2024	1.0	Revisión del Documento	Comité de Seguridad de la Información
18/09/2025	2.0	Actualización de Política según alcance e implementación de SGSI	Comité de Seguridad de la Información

Contenido

Control de versiones	2
1 Objetivo	4
2 Alcance	4
3 Roles y responsabilidades	4
4 Identificación e inventario de activos	5
5 Propiedad de los activos	6
6 Uso y protección de activos	6
7 Ciclo de vida de los activos.....	7
8 Integración con otras políticas	8
9 Cumplimiento y seguimiento	8
10 Vigencia y Publicación	9

	Política de Gestión de Activos de Información	C-1 Información Pública
Versión: 2.0 Fecha: 18/09/2025		Página: 4 de 9

1 Objetivo

El propósito de esta política es garantizar la gestión adecuada de todos los activos de información de Interfase ISA durante todo su ciclo de vida, desde su identificación y registro hasta su disposición final. Busca asegurar que dichos activos estén protegidos frente a amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento legal y contractual.

Esta política se encuentra alineada con los requisitos de ISO/IEC 27001:2022 e ISO/IEC 27002:2022 y aplica en todas las sedes de Interfase ISA.

2 Alcance

La presente política aplica a todos los activos de información de Interfase ISA en todas sus sedes, incluyendo datos, aplicaciones, documentación física, infraestructura tecnológica, servicios en la nube, dispositivos móviles, estaciones de trabajo y entornos de teletrabajo autorizados. Su cumplimiento es obligatorio para todos los colaboradores, contratistas y terceros que administren, procesen o tengan acceso a dichos activos.

3 Roles y responsabilidades

La gestión de activos de información en Interfase ISA es una responsabilidad compartida que involucra a todas las áreas de la organización:

- **Directorio:** aprueba esta política, asigna los recursos necesarios para su implementación y asegura que la gestión de activos se integre en los procesos de negocio.
- **Comité de Seguridad:** supervisa la aplicación de esta política, valida excepciones, revisa periódicamente el inventario de activos y eleva reportes de cumplimiento al Directorio.
- **PM del SGSI:** coordina la aplicación de esta política, asegura la actualización del inventario de activos y su integración con la matriz de riesgos del SGSI.
- **Responsables de Área / Propietarios de Activos:** mantienen actualizado el inventario de los activos bajo su control, autorizan cambios de estado en el ciclo de vida (altas, bajas, transferencias) y garantizan que se cumplan las medidas de seguridad definidas.
- **Área de TI:** administra los activos tecnológicos, mantiene registros de configuración, aplica controles de seguridad, realiza respaldos y asegura que se respeten los lineamientos definidos en el SGSI.

 	Política de Gestión de Activos de Información	C-1 Información Pública
Versión: 2.0 Fecha: 18/09/2025		Página: 5 de 9

- Colaboradores: utilizan los activos de manera responsable, protegen los recursos bajo su control y reportan cualquier incidente o uso indebido.

Adicionalmente, los responsables de área deberán coordinar con Recursos Humanos y TI para asegurar que, en los procesos de ingreso, cambio de rol o egreso de colaboradores, los activos asignados sean inventariados, transferidos o devueltos de manera formal. Toda entrega o devolución deberá quedar registrada en el inventario oficial del SGSI como evidencia de cumplimiento.

Las responsabilidades específicas y la segregación de funciones se encuentran documentadas en la Matriz RACI del SGSI, la cual complementa esta política y constituye evidencia verificable en auditorías internas y externas.

4 Identificación e inventario de activos

La gestión de activos de información en Interfase ISA es una responsabilidad compartida que involucra a todas las áreas de la organización:

- Directorio aprueba esta política, asigna los recursos necesarios para su implementación y asegura que la gestión de activos se integre en los procesos de negocio.
- Comité de Seguridad: supervisa la aplicación de esta política, valida excepciones, revisa periódicamente el inventario de activos y eleva reportes de cumplimiento al Directorio.
- PM del SGSI: coordina la aplicación de esta política, asegura la actualización del inventario de activos y su integración con la matriz de riesgos del SGSI.
- Responsables de Área / Propietarios de Activos: mantienen actualizado el inventario de los activos bajo su control, autorizan cambios de estado en el ciclo de vida (altas, bajas, transferencias) y garantizan que se cumplan las medidas de seguridad definidas.
- Área de TI: administra los activos tecnológicos, mantiene registros de configuración, aplica controles de seguridad, realiza respaldos y asegura que se respeten los lineamientos definidos en el SGSI.
- Colaboradores: utilizan los activos de manera responsable, protegen los recursos bajo su control y reportan cualquier incidente o uso indebido.

Adicionalmente, los responsables de área deberán coordinar con Recursos Humanos y TI para asegurar que, en los procesos de ingreso, cambio de rol o egreso de colaboradores, los activos asignados sean inventariados, transferidos o devueltos de manera formal. Toda entrega o devolución deberá quedar registrada en el inventario oficial del SGSI como evidencia de cumplimiento.

 	Política de Gestión de Activos de Información	C-1 Información Pública
Versión: 2.0 Fecha: 18/09/2025		Página: 6 de 9

El inventario deberá contemplar, además de activos físicos y locales, los activos en la nube (instancias, buckets, configuraciones, claves/secretos) y las licencias/suscripciones SaaS, incluyendo propietario, clasificación, criticidad, ubicación lógica, dependencias y controles aplicados, garantizando cobertura integral y trazabilidad en el SGSI.

Las responsabilidades específicas y la segregación de funciones se encuentran documentadas en la Matriz RACI del SGSI, la cual complementa esta política y constituye evidencia verificable en auditorías internas y externas.

5 Propiedad de los activos

- Cada activo de información deberá tener un propietario claramente designado, quien será responsable de su uso, protección y mantenimiento durante todo su ciclo de vida.
- Las responsabilidades del propietario de activo incluyen:
- Garantizar que el activo esté correctamente registrado e incluido en el inventario.
- Definir y autorizar los niveles de acceso, asegurando el cumplimiento del principio de mínimo privilegio.
- Coordinar con TI y el Comité de Seguridad cualquier cambio en el estado del activo (alta, transferencia o baja).
- Validar anualmente la vigencia de los accesos y controles aplicados a los activos bajo su responsabilidad, documentando dicha revisión en el inventario oficial del SGSI.
- La ausencia de propietario asignado será tratada como una no conformidad y deberá ser subsanada en un plazo definido por el Comité de Seguridad.

6 Uso y protección de activos

Los activos de información de Interfase ISA deberán ser utilizados exclusivamente para fines corporativos y en estricto cumplimiento de las políticas del SGSI. Su uso indebido, negligente o no autorizado será considerado una violación de esta política y se gestionará conforme a la Política General de Seguridad de la Información y al procedimiento de Gestión de Incidentes.

El uso y protección de activos deberá cumplir con los siguientes lineamientos:

- Principio de mínimo privilegio: el acceso a los activos estará restringido únicamente a los colaboradores, contratistas o terceros que lo requieran para el desempeño de sus funciones.

	Política de Gestión de Activos de Información	C-1 Información Pública
Versión: 2.0 Fecha: 18/09/2025		Página: 7 de 9

- Autenticación y credenciales: todo acceso deberá realizarse mediante credenciales personales, seguras e intransferibles. Está prohibido compartir contraseñas, tokens u otros mecanismos de autenticación.
- Software y hardware autorizados: únicamente podrán instalarse y usarse aplicaciones, sistemas y dispositivos aprobados por el área de TI. Está prohibida la instalación de software no licenciado o no validado por la organización.
- Protección de la información: los colaboradores deberán aplicar medidas de seguridad como cifrado, almacenamiento en repositorios corporativos, copias de respaldo y uso de canales seguros para la transmisión de información sensible.
- Dispositivos externos y portátiles: el uso de dispositivos de almacenamiento externo o equipos portátiles requerirá autorización expresa del Comité de Seguridad o del área de TI, y deberán estar protegidos con cifrado y controles definidos.
- Responsabilidad individual: cada colaborador es responsable de proteger los activos que le sean asignados, reportar inmediatamente cualquier pérdida, daño, incidente o sospecha de uso indebido, y devolverlos en caso de transferencia o egreso.

El incumplimiento de estas disposiciones será tratado como incidente de seguridad de la información y podrá derivar en sanciones administrativas, contractuales o legales, según corresponda.

7 Ciclo de vida de los activos

La gestión de los activos de información en Interfase ISA abarca todas las etapas de su ciclo de vida, desde su creación o adquisición hasta su disposición final. Cada fase deberá estar documentada y bajo control, asegurando que se mantengan las medidas de seguridad apropiadas en todo momento.

- Alta de activos: todo nuevo activo deberá ser inventariado por el área de TI y asignado a un propietario formal. Deberán documentarse su clasificación, nivel de criticidad y controles aplicables.
- Mantenimiento y uso: durante su utilización, los activos deberán contar con medidas de seguridad vigentes (actualizaciones, parches, controles de acceso, cifrado, respaldos). El propietario del activo será responsable de verificar periódicamente su correcto uso y protección.
- Transferencia de activos: cualquier transferencia de activos entre áreas, colaboradores o terceros deberá quedar documentada y aprobada por el propietario, asegurando la continuidad de las medidas de seguridad.

 	Política de Gestión de Activos de Información	C-1 Información Pública
Versión: 2.0 Fecha: 18/09/2025		Página: 8 de 9

- Baja y disposición final: los activos obsoletos, dañados o que hayan dejado de ser necesarios deberán ser retirados de forma controlada. Para los activos de información, la eliminación se realizará mediante métodos seguros que garanticen la imposibilidad de recuperación no autorizada (borrado seguro, destrucción física o equivalentes). La baja deberá ser registrada y contar con la aprobación del Comité de Seguridad.

8 Integración con otras políticas

El Comité de Seguridad, en coordinación con el área de TI y la PM SGSI, será responsable de supervisar la correcta aplicación de los lineamientos de gestión de activos. Para ello:

- Auditorías periódicas: se realizarán revisiones al menos una vez al año sobre el inventario de activos, verificando su exactitud, la vigencia de los controles asociados y la correcta aplicación de las clasificaciones.
- Indicadores de gestión: se establecerán métricas como el porcentaje de activos inventariados, el porcentaje de activos con propietario definido, el número de incidencias relacionadas con uso indebido de activos y el grado de cumplimiento de los plazos en la baja de activos obsoletos.
- Reporte al Directorio: los resultados de estas revisiones se consolidarán en un informe anual presentado en la Revisión por la Dirección, constituyendo evidencia del compromiso de mejora continua del SGSI.
- Actualización de la política: esta política será revisada al menos una vez al año, o antes si ocurren cambios relevantes en el entorno tecnológico, organizacional, legal o contractual. Cualquier modificación deberá quedar registrada bajo control de versiones y ser aprobada por el Directorio antes de su entrada en vigor.

9 Cumplimiento y seguimiento

El cumplimiento de esta política es obligatorio para todos los colaboradores, contratistas y terceros que utilicen activos de Interfase ISA.

El incumplimiento será gestionado conforme a la Política General de Seguridad de la Información y a los reglamentos internos de la organización.

El Comité de Seguridad supervisará periódicamente la aplicación de esta política, evaluará la eficacia de los controles implementados y elaborará un reporte anual de cumplimiento que será elevado al Directorio como parte de la Revisión por la Dirección.

	Política de Gestión de Activos de Información	C-1 Información Pública
Versión: 2.0 Fecha: 18/09/2025		Página: 9 de 9

Los indicadores mínimos para revisar incluirán: porcentaje de acuerdos de confidencialidad firmados, tiempo de revocación de accesos al egreso, tasa de finalización de capacitaciones y resultados de las auditorías internas. Estos resultados serán presentados semestralmente al Comité de Seguridad y anualmente en la Revisión por la Dirección.

10 Vigencia y Publicación

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

El Comité de Seguridad es responsable de garantizar que únicamente la versión aprobada esté publicada y accesible, así como de coordinar su revisión periódica. La política será revisada al menos una vez al año o antes si ocurren cambios relevantes en el contexto legal, contractual, organizacional o tecnológico.

Toda modificación deberá registrarse bajo control de versiones y ser aprobada por el Directorio antes de su entrada en vigor.

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