Política de Uso Aceptable de Activos

Fecha: 17/09/2025
Versión: 2.0

Control de versiones

Fecha	Versión	Descripción	Autor
15/11/2024	0.1	Creación del Documento	PM SGSI
29/11/2024	1.0	Revisión del Documento	Comité de Seguridad de la Información
11/12/2024	1.1	Actualización con EOL	Comité de Seguridad de la Información
17/09/2025	2.0	Actualización de Política según alcance e implementación de SGSI	Comité de Seguridad de la Información

Contenido

1 Objetivo

El propósito de esta política es establecer los lineamientos de uso aceptable de los activos de información de Interfase ISA, garantizando que su utilización sea responsable, segura y alineada con los objetivos estratégicos de la organización.

2 Alcance

Esta política aplica a todos los colaboradores, contratistas y terceros que utilicen activos de información de Interfase ISA en todas las sedes y en esquemas de teletrabajo autorizados. Se incluyen: equipos de cómputo, dispositivos móviles, correo electrónico, aplicaciones, recursos de comunicación, Internet, redes sociales corporativas y cualquier medio que procese o almacene información de la organización o de sus clientes.

3 Roles y responsabilidades

El uso aceptable de activos es una responsabilidad compartida:

- Directorio aprueba esta política, asegura recursos para su cumplimiento y lidera con el ejemplo.
- Comité de Seguridad supervisa la aplicación de esta política, gestiona las excepciones y revisa periódicamente su eficacia.
- PM del SGSI coordina la implementación, difunde la política y asegura que esté integrada a los procesos de negocio.
- Responsables de Área velan por el cumplimiento de la política en sus equipos, reportando incidentes o incumplimientos.
- Colaboradores, contratistas y terceros deben cumplir los lineamientos aquí definidos, utilizar los activos de forma ética y reportar cualquier uso indebido o incidente de seguridad.

Las responsabilidades específicas y la segregación de funciones relacionadas con el uso aceptable de activos se encuentran documentadas en la Matriz RACI del SGSI, la cual constituye evidencia formal para auditorías internas y externas.

4 Principios de uso aceptable

El uso de los activos de información de Interfase ISA debe regirse por los siguientes lineamientos:

El acceso a los activos de información se otorgará bajo el principio de mínimo privilegio, de modo que cada usuario cuente únicamente con los recursos necesarios para el desempeño de sus funciones.

Acceso y Autenticación

El acceso a los activos estará restringido a usuarios autorizados, con credenciales personales, seguras e intransferibles. Está prohibido compartir contraseñas, tokens u otros mecanismos de autenticación.

Uso de Correo Electrónico y Comunicaciones

El correo corporativo debe utilizarse únicamente para fines laborales. No está permitido el envío de información sensible a cuentas personales ni el reenvío de correos laborales a plataformas no autorizadas. El uso de mensajería instantánea y otros canales de comunicación debe seguir los mismos principios de seguridad y confidencialidad.

Uso de Internet y Redes Sociales

El acceso a Internet debe orientarse exclusivamente a fines laborales. El uso de redes sociales y canales digitales corporativos debe realizarse de manera profesional, sin divulgar información confidencial ni afectar la reputación de Interfase ISA, en concordancia con la Política de Clasificación y Manejo de la Información.

Dispositivos y Equipos

Todo hardware y software provisto por Interfase ISA debe usarse únicamente para fines laborales. Se prohíbe la instalación de software no autorizado, así como la conexión de dispositivos externos sin la aprobación expresa del Comité de Seguridad.

Protección de la Información

Los colaboradores deben aplicar las medidas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad, almacenando y transmitiendo los datos solo a través de medios corporativos autorizados.

Servicios en la nube

El uso de aplicaciones y plataformas en la nube deberá realizarse exclusivamente mediante cuentas corporativas y proveedores autorizados, respetando la clasificación de la información,

las restricciones de compartición externa, los acuerdos de confidencialidad y los controles de acceso definidos por Interfase ISA. Queda prohibido utilizar cuentas personales o servicios no aprobados para procesar información corporativa.

Retención y Eliminación

Los activos de información que ya no sean necesarios deben eliminarse de forma segura, conforme a los procedimientos definidos por el Comité de Seguridad.

5 Reporte de incidentes

El uso indebido de activos, la pérdida de dispositivos, la instalación de software no autorizado, los accesos fuera de horario, así como cualquier actividad sospechosa que pueda comprometer la seguridad de la información, deberá ser reportado de inmediato (máximo dentro de las 24 horas de detectado).

Los reportes deberán realizarse a través de los canales oficiales definidos en el Procedimiento de Gestión de Incidentes del SGSI, garantizando que cada incidente sea registrado, clasificado y tratado de manera oportuna.

Los responsables de área tienen la obligación de asegurar que los incidentes sean documentados y que se apliquen las medidas correctivas correspondientes en los plazos establecidos. El Comité de Seguridad consolidará los incidentes reportados y presentará un informe periódico al Directorio como parte del proceso de seguimiento del SGSI.

6 Relación con otras políticas

La presente política de Uso Aceptable de Activos se complementa con otras políticas y lineamientos del SGSI que abordan aspectos específicos:

- Política de Gestión de Activos de Información, que define el inventario, los propietarios de activos y el ciclo de vida de estos.
- Política de Clasificación y Manejo de la Información, que establece los niveles de clasificación y tratamiento de la información.
- Política de Control de Acceso, que regula la autorización, revisión y revocación de accesos a los activos.
- Política de Seguridad en Recursos Humanos, que incorpora el uso aceptable de activos en los procesos de inducción, capacitación y desvinculación de colaboradores.

- Política de Gestión de Incidentes de Seguridad, que regula la notificación, tratamiento y cierre de incidentes relacionados con el uso de activos.

El cumplimiento de esta política depende directamente de la correcta aplicación de estas políticas complementarias, cuya vigencia y actualización son responsabilidad del Comité de Seguridad.

7 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.

8 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.

tuid
FIRMA DIGITAL
Leonardo Adrian Noach Meierovich

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