Política de Teletrabajo y Dispositivos móviles

Fecha: 06/10/2025

Versión: 1.0

Control de versiones

Fecha	Versión	Descripción	Autor
06/10/2025	0.1	Creación del Documento	Comité de Seguridad de la Información
10/10/2025	1.0	Revisión del Documento	Comité de Seguridad de la Información

Contenido

1 Objetivo

Establecer los lineamientos generales para proteger la seguridad de la información en las modalidades de teletrabajo y en el uso de dispositivos móviles dentro de Interfase ISA, garantizando la confidencialidad, integridad y disponibilidad de los activos sin importar el lugar desde donde se acceda.

Esta política establece los requisitos mínimos para garantizar que las modalidades de teletrabajo y el uso de dispositivos móviles mantengan niveles equivalentes de seguridad, confidencialidad, trazabilidad y cumplimiento que las operaciones presenciales.

Forma parte del Sistema de Gestión de Seguridad de la Información (SGSI) de Interfase ISA y se alinea con los controles A.5.10, A.5.18 y A.6.2 de la norma ISO/IEC 27001:2022, asegurando la continuidad operativa, la protección de los activos de información y la gestión de riesgos asociados al trabajo remoto y la movilidad.

2 Alcance

Aplica a todas las sedes de Interfase ISA, y a colaboradores, contratistas, proveedores o terceros que accedan a los sistemas, redes, aplicaciones o información de la organización mediante teletrabajo o dispositivos móviles, ya sean provistos por Interfase ISA o personales autorizados (BYOD – Bring Your Own Device).

Su cumplimiento es obligatorio en todas las modalidades de trabajo remoto o móvil, así como en los servicios prestados a clientes bajo el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

3 Roles y responsabilidades

El teletrabajo y el uso de dispositivos móviles son responsabilidades compartidas que requieren coordinación entre las áreas técnicas, de gestión y de soporte de Interfase ISA.

- 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, revisa su eficacia, aprueba excepciones y presenta informes de cumplimiento al Directorio.

- PM del SGSI: coordina la implementación y actualización de esta política, consolida evidencias de cumplimiento y promueve la concientización del personal.
- Área de TI: aplica y mantiene los controles tecnológicos que respaldan la seguridad del teletrabajo y la gestión de dispositivos móviles.
- Responsables de Área: garantizan el cumplimiento dentro de sus equipos, autorizan el teletrabajo y notifican incidentes o incumplimientos.
- Colaboradores y terceros: acatan las disposiciones establecidas, protegen los activos asignados y reportan de inmediato cualquier pérdida, incidente o uso indebido.

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

4 Requisitos generales para teletrabajo

El teletrabajo extiende el entorno laboral de Interfase ISA fuera de sus instalaciones, por lo que debe garantizar el mismo nivel de seguridad y cumplimiento que en la modalidad presencial.

Antes de habilitar el teletrabajo, el Comité de Seguridad y el Área de TI deberán realizar una evaluación de riesgos específica, considerando los activos involucrados, los tipos de información que serán tratados y las medidas de control requeridas.

Solo se autorizará el teletrabajo cuando los riesgos identificados se encuentren mitigados a un nivel aceptable y exista evidencia de cumplimiento de los requisitos técnicos y organizativos definidos por el SGSI

- El teletrabajo deberá realizarse únicamente bajo autorización formal y en cumplimiento de los requisitos definidos por el SGSI.
- Todo acceso remoto deberá emplear mecanismos de conexión segura, autenticación multifactor y cifrado de las comunicaciones.
- Los colaboradores deberán mantener la confidencialidad, integridad y trazabilidad de la información procesada, evitando su exposición a terceros no autorizados.
- Los entornos remotos de trabajo deberán contar con condiciones adecuadas de seguridad física y lógica, control de acceso y resguardo de los activos corporativos.

- Cualquier incidente o sospecha de compromiso de seguridad deberá reportarse de manera inmediata a los canales oficiales del SGSI.
- Los lineamientos operativos complementarios se encuentran documentados en el Procedimiento de Teletrabajo y Dispositivos Móviles, parte integrante del SGSI.
- El Comité de Seguridad y el Área de TI deberán verificar periódicamente la correcta aplicación de estas condiciones y conservar evidencia de cumplimiento dentro del SGSI.

Los equipos utilizados en teletrabajo deberán mantenerse actualizados, con antivirus activo, parches de seguridad instalados y mecanismos de respaldo configurados conforme al Procedimiento de Mantenimiento y Respaldo de Activos.

En caso de desvinculación o finalización del contrato, los dispositivos deberán someterse a un proceso de eliminación segura de datos, supervisado por el Área de TI y documentado como evidencia de cumplimiento en el Registro de Activos y el Registro de Eliminación Segura del SGSI.

5 Uso de dispositivos móviles

El uso de dispositivos móviles corporativos o personales autorizados (BYOD – “Trae tu propio dispositivo”) implica responsabilidades específicas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información, así como a asegurar la trazabilidad de los datos.

- Solo se autorizará el uso de dispositivos gestionados o aprobados por Interfase ISA y registrados en el inventario del SGSI.
- Todos los equipos deberán operar bajo políticas corporativas de gestión y protección (cifrado, bloqueo, autenticación y monitoreo).
- El almacenamiento o transmisión de información clasificada deberá realizarse únicamente mediante medios y repositorios corporativos.
- El uso de cuentas personales, aplicaciones o servicios no autorizados para tratar información corporativa está estrictamente prohibido.
- La pérdida, robo o daño de un dispositivo deberá ser reportado de inmediato para la ejecución de las acciones definidas en los procedimientos técnicos correspondientes.
- Los dispositivos móviles deberán operar bajo políticas corporativas de gestión y protección que incluyan cifrado de disco, bloqueo automático de sesión, autenticación multifactor y supervisión técnica.

En caso de pérdida o robo de un equipo, el área técnica procederá a bloquear los accesos corporativos asociados (correo, VPN, sistemas) y verificará que el dispositivo cuente con cifrado completo de disco (BitLocker u otro equivalente), garantizando la inaccesibilidad de la información.

En la actualidad, Interfase ISA no dispone de un sistema de gestión centralizada de dispositivos móviles (MDM); sin embargo, los controles implementados —cifrado, bloqueo y gestión de incidentes— constituyen medidas compensatorias suficientes para mitigar el riesgo de divulgación no autorizada.

- Las aplicaciones móviles deberán descargarse exclusivamente de tiendas oficiales y mantenerse actualizadas.
- Se prohíbe expresamente el almacenamiento local de información clasificada sin cifrado aprobado o fuera de los repositorios corporativos autorizados.

El Comité de Seguridad y el Área de TI revisarán anualmente la eficacia de las medidas aplicadas a los dispositivos móviles y actualizarán los controles conforme a las amenazas emergentes o cambios tecnológicos detectados.

Estos lineamientos se desarrollan y aplican conforme al Procedimiento P8-II – Teletrabajo y Uso Seguro de Dispositivos Móviles, parte integrante del SGSI.

6 Indicadores y revisión de eficacia

El Comité de Seguridad y el PM del SGSI medirán la eficacia de esta política a través de indicadores tales como:

- Porcentaje de dispositivos móviles registrados y actualizados.
- Número de incidentes o pérdidas reportadas en modalidad de teletrabajo.
- Resultados de auditorías de cumplimiento de los controles BYOD.

Los resultados se analizarán durante la Revisión por la Dirección, y servirán de base para ajustar los controles y fortalecer la concienciación del personal

7 Cumplimiento y mejora continua

El cumplimiento de esta política es obligatorio y será supervisado por el Comité de Seguridad, en coordinación con el Área de TI y el PM del SGSI. Los resultados de su implementación serán revisados anualmente en la Revisión por la Dirección, asegurando la mejora continua de los controles asociados.

El incumplimiento podrá dar lugar a medidas disciplinarias, contractuales o legales, según la gravedad del caso y la normativa vigente.

Esta política deberá revisarse al menos una vez al año o ante cualquier cambio significativo en la tecnología, normativa, o modalidades de trabajo remoto. Las revisiones deberán documentarse en el control de versiones y conservar evidencia de aprobación por el Directorio.

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 institucionales 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 anual o cada vez que se produzcan cambios relevantes en el contexto legal, contractual, organizacional o tecnológico.

Toda modificación deberá registrarse bajo control de versiones, conservar evidencia de aprobación y deberá contar con la aprobación formal del Directorio antes de su aplicación.

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

tuid
FIRMA DIGITAL
Leonardo Adrian Noach Meierovich