# Política de Seguridad en Recursos Humanos

**Fecha:** 18/09/2025
**Versión**: 2.0

## Control de versiones

| Fecha | Versión | Descripción | Autor |
|---|---|---|---|
| 10/11/2023 | 0.9 | Creación del Documento | Comité de Seguridad de la Información |
| 20/02/2023 | 1.0 | Actualización del Documento | Comité de Seguridad de la Información |
| 23/02/2024 | 1.1 | Revisión del documento | Comité de Seguridad de la Información |
| 28/02/2025 | 1.2 | 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

## 1 Objetivo

El propósito de esta política es establecer los lineamientos de seguridad de la información aplicables a colaboradores, contratistas y terceros en todas las sedes de Interfase ISA. Su objetivo es garantizar que las obligaciones de seguridad se apliquen durante todo el ciclo de vida laboral —desde la selección e incorporación, durante la permanencia, hasta el egreso—, fortaleciendo la protección de la confidencialidad, integridad y disponibilidad de la información de la organización y de sus clientes.

## 2 Alcance

Esta política aplica a todos los procesos relacionados con la gestión de personas en Interfase ISA, en todas sus sedes y modalidades de trabajo (presencial, remoto o híbrido). Incluye a colaboradores internos, contratistas y terceros que, en virtud de sus funciones, accedan a los sistemas, procesos, instalaciones o activos de información de la organización.

## 3 Roles y responsabilidades

La seguridad en recursos humanos 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 lidera con el ejemplo el compromiso con la seguridad de la información.
- Comité de Seguridad: define las obligaciones de seguridad del personal, valida excepciones, supervisa el cumplimiento y eleva informes de cumplimiento al Directorio.
- Gerencia de Recursos Humanos: asegura la ejecución de los controles de seguridad en las fases de incorporación, permanencia y egreso; gestiona la firma de compromisos de confidencialidad; coordina programas de concientización en conjunto con el PM del SGSI. Es responsable de mantener la documentación de soporte (contratos, acuerdos de confidencialidad, registros de capacitación y formularios de egreso) como evidencia de cumplimiento del SGSI. Cuando se tercericen funciones de RRHH, la Gerencia de RRHH deberá evaluar y revisar periódicamente el cumplimiento de obligaciones de seguridad por parte de dichos proveedores (acuerdos de confidencialidad, protección de datos personales, revocación de accesos en egresos, resguardo de documentación), manteniendo evidencia de estas revisiones para auditoría.
- Responsables de Área: garantizan que los colaboradores bajo su cargo conozcan y apliquen esta política, notifican cambios de rol o función y apoyan en la gestión de accesos.

- Colaboradores y terceros: cumplen con las obligaciones establecidas en esta política, protegen los activos de información asignados y reportan cualquier incidente de seguridad.

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.

Adicionalmente, la Gerencia de Recursos Humanos deberá coordinar de manera permanente con el área de TI y con los responsables de área cada vez que se produzcan cambios en la situación contractual, funciones o roles de un colaborador, asegurando la actualización inmediata de accesos y la revocación oportuna de privilegios. El incumplimiento de esta coordinación será considerado un riesgo de seguridad sujeto a reporte formal al Comité de Seguridad.

## 4 Incorporación de colaboradores

Todo proceso de selección deberá incluir verificaciones proporcionales a la criticidad del cargo, tales como referencias laborales, académicas y, cuando corresponda, validaciones adicionales.

Antes de iniciar actividades, cada colaborador o tercero deberá suscribir acuerdos de confidencialidad y aceptar por escrito las políticas de seguridad vigentes de Interfase ISA. Recursos Humanos será responsable de conservar estos registros como evidencia de cumplimiento.

El proceso de incorporación e inducción deberá registrarse en las herramientas corporativas de la empresa (por ejemplo, sistema de RRHH o plataforma de gestión documental), asegurando la trazabilidad y disponibilidad de la evidencia ante auditorías o revisiones internas.

El Comité de Seguridad revisará anualmente los procesos de incorporación para asegurar que las verificaciones, registros y acuerdos de confidencialidad cumplen con los estándares normativos y contractuales aplicables.~~Todo proceso de selección deberá incluir verificaciones proporcionales a la criticidad del cargo, tales como referencias laborales, académicas y, cuando corresponda, validaciones adicionales.~~

~~Antes de iniciar actividades, cada colaborador o tercero deberá suscribir acuerdos de confidencialidad y aceptar por escrito las políticas de seguridad vigentes de Interfase ISA. Recursos Humanos será responsable de conservar estos registros como evidencia de cumplimiento.~~

~~El Comité de Seguridad revisará anualmente los procesos de incorporación para asegurar que las verificaciones y los acuerdos de confidencialidad cumplen con los estándares normativos y contractuales aplicables.~~

Commented [RA1]: Aca pondría algo como que el proceso de incorporación e inducción debe quedar registrado en las herramientas de la empresa

Commented [MG2R1]: De acuerdo

## 5 Permanencia

Durante la relación laboral, todos los colaboradores deberán recibir capacitación periódica en materia de seguridad de la información, al menos una vez al año. Esta formación incluirá: uso aceptable de activos, reporte de incidentes, protección de datos personales, y cumplimiento normativo aplicable.

Cuando se produzcan cambios de funciones o roles, Recursos Humanos deberá coordinar con los responsables de área y con TI para ajustar los accesos y asegurar que el nivel de privilegios sea consistente con la nueva posición.

El Comité de Seguridad y Recursos Humanos medirán la efectividad de estas capacitaciones mediante indicadores como: porcentaje de asistencia, evaluaciones de conocimiento y número de incidentes reportados por colaboradores capacitados.

Adicionalmente, los accesos lógicos y físicos deberán revisarse al menos una vez al año para asegurar que se mantienen alineados al principio de mínimo privilegio. En los procesos de egreso, todos los accesos deberán ser revocados antes de la desvinculación efectiva del colaborador, dejando constancia documental de dicha revocación como evidencia de cumplimiento.

## 6 Egreso de Personal

Al finalizar el vínculo laboral o contractual, Recursos Humanos deberá coordinar de manera inmediata la revocación de accesos a sistemas, instalaciones y activos de información.

El procedimiento de egreso incluirá:

- Desactivación de credenciales de usuario y retiro de autorizaciones de acceso físico.
- Devolución de equipos y activos tecnológicos.
- Firma de recordatorio de obligaciones de confidencialidad vigentes incluso después del cese del vínculo.
- Todo el proceso de egreso deberá quedar documentado en un checklist formal, bajo custodia de RRHH y con validación del área de TI para garantizar la revocación completa de accesos.

El proceso de egreso, junto con sus validaciones, deberá registrarse en las herramientas corporativas de la empresa (por ejemplo, sistema de RRHH o repositorio documental del SGSI), asegurando la trazabilidad y disponibilidad de la información ante auditorías. Los checklists de egreso, junto con las validaciones de TI, serán conservados por Recursos Humanos por un plazo

mínimo de cinco años como evidencia de cumplimiento~~Los checklists de egreso, junto con las validaciones de TI, serán conservados por Recursos Humanos por un plazo mínimo de cinco años como evidencia de cumplimiento y estarán disponibles para auditorías internas o externas~~.

Commented [RA3]: Igual que el anterior

## 7 Teletrabajo y dispositivos móviles

El personal que realice teletrabajo deberá cumplir con la Política de Teletrabajo y Dispositivos Móviles, garantizando el uso seguro de recursos fuera de las instalaciones de Interfase ISA. La organización proveerá los medios técnicos necesarios para reducir los riesgos asociados a esta modalidad de trabajo.

En el caso de teletrabajo, los colaboradores deberán utilizar únicamente dispositivos corporativos o autorizados, conectarse mediante canales seguros (VPN u otros definidos por TI) y cumplir con los lineamientos de cifrado y autenticación multifactor establecidos en la Política de Control de Acceso.

Los dispositivos móviles autorizados deberán cumplir con las configuraciones de seguridad definidas por TI (cifrado, bloqueo automático, antivirus y control de actualizaciones). Todo incumplimiento en estas medidas será tratado como un incidente de seguridad.

## 8 Concientización y formación

Todos los colaboradores, contratistas y terceros que accedan a los sistemas o a la información de Interfase ISA deberán participar en programas de concientización y formación en seguridad de la información. La Gerencia de RRHH será responsable de coordinar dichas actividades junto al Comité de Seguridad, asegurando que se dicten al menos una vez por año y que sus registros se mantengan como evidencia de cumplimiento.

El programa de concientización incluirá simulaciones de phishing, campañas de sensibilización y recordatorios periódicos en los canales corporativos. Los resultados de estas actividades serán revisados por el Comité de Seguridad como parte del ciclo de mejora continua del SGSI

## 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 a Directorio como parte de la Revisión por la Dirección.

Los indicadores mínimos a 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 |

tuid
FIRMA DIGITAL
**Leonardo Adrian Noach Meierovich**