Política de Control de Acceso

Fecha: 16/09/2025
Versión: 2.0

Control de versiones

Fecha	Versión	Descripción	Autor
18/11/2024	0.1	Creación del Documento	PM SGSI
29/11/2024	1.0	Revisión del Documento	Comité de Seguridad de la Información
16/09/2025	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 que regulan el acceso a los sistemas, aplicaciones, datos y redes de Interfase ISA, asegurando que los accesos se concedan, utilicen y controlen de manera adecuada, en cumplimiento con los principios de confidencialidad, integridad y disponibilidad establecidos por la norma ISO/IEC 27001:2022.

2 Alcance

La política aplica a todas las sedes y operaciones de Interfase ISA, incluyendo también los esquemas de teletrabajo autorizados. Es de cumplimiento obligatorio para todos los colaboradores, contratistas, proveedores y terceros que accedan a sistemas, redes o información de la organización.

3 Roles y responsabilidades

La gestión del control de acceso en Interfase ISA es una responsabilidad compartida que involucra a todas las áreas de la organización:

- Directorio aprueba esta política, asegura los recursos necesarios para su cumplimiento y refuerza con su ejemplo el compromiso de la organización con la seguridad de la información.
- Comité de Seguridad supervisa la correcta aplicación de esta política, revisa periódicamente la eficacia de los controles de acceso, aprueba las excepciones justificadas y recibe reportes de auditoría y revisiones de accesos.
- PM del SGSI coordina la implementación de los lineamientos aquí definidos, centraliza la documentación y asegura la comunicación entre las distintas áreas.
- Infraestructura y Soporte TI administran las cuentas de usuario, contraseñas, permisos, accesos privilegiados y redes, incluyendo la revocación inmediata de accesos cuando corresponda.
- RRHH notifica oportunamente las altas, bajas y cambios de rol de los colaboradores para garantizar una gestión precisa y oportuna de accesos.
- Propietarios de activos de información autorizan y revisan periódicamente los accesos otorgados a los sistemas y datos bajo su responsabilidad, asegurando que respondan al principio de mínimo privilegio.

Commented [MG1]: Directorio

- Colaboradores y terceros deben utilizar los accesos otorgados únicamente para fines autorizados, proteger sus credenciales, no compartirlas bajo ninguna circunstancia y reportar de inmediato cualquier incidente o uso indebido.

Las responsabilidades específicas y la segregación de funciones vinculadas a la gestión de accesos están documentadas en la Matriz RACI del SGSI, la cual complementa esta política y constituye evidencia verificable de la asignación de roles y responsabilidades para fines de auditoría.

4 Principios de control de acceso

El control de acceso en Interfase ISA se fundamenta en principios que aseguran que la información y los sistemas de la organización se utilicen únicamente por personas autorizadas y en el marco de sus funciones.

- El acceso se concede bajo los principios de mínimo privilegio y necesidad de conocer, evitando otorgar permisos innecesarios.
- El uso de cuentas genéricas o compartidas está prohibido, salvo casos excepcionales debidamente justificados, con plazo limitado y aprobación formal del Comité de Seguridad.
- Todos los accesos deben ser solicitados formalmente, autorizados y documentados, incluyendo altas, bajas y modificaciones.
- Las excepciones deberán estar sustentadas en una justificación clara, documentadas en el SGSI y aprobadas explícitamente por el Comité de Seguridad.

Estos principios son de aplicación transversal en todos los sistemas, redes y procesos de Interfase ISA, constituyendo la base de la presente política.

5 Gestión de identidades y autenticación

La gestión de identidades y autenticación garantiza que cada usuario esté claramente identificado y validado antes de acceder a los recursos tecnológicos de Interfase ISA.

- Cada colaborador, contratista o tercero tendrá una cuenta única, personal e intransferible vinculada a su identidad.
- Las contraseñas deben cumplir con requisitos de complejidad, longitud y caducidad definidos en los estándares técnicos de TI, y no podrán ser compartidas. Los requisitos de complejidad de contraseñas, caducidad y parámetros técnicos específicos (como

longitud mínima, bloqueo de cuentas tras intentos fallidos o configuración de MFA) estarán definidos en un Procedimiento Técnico de Gestión de Credenciales de TI, el cual deberá ser elaborado, aprobado y mantenido bajo control documental del SGSI

- En sistemas críticos y accesos remotos se implementará obligatoriamente autenticación multifactor (MFA).
- Las cuentas inactivas por más de noventa días serán deshabilitadas automáticamente.
- Las estaciones de trabajo deberán configurarse para bloquearse tras un período de inactividad y requerir nuevamente autenticación para reactivarse.

El Comité de Seguridad revisará periódicamente la aplicación de estas medidas y su alineación con las mejores prácticas internacionales.

6 Gestión de privilegios y cuentas especiales

Los accesos con privilegios elevados representan un riesgo mayor y, por lo tanto, deben ser controlados bajo lineamientos estrictos.

- Los accesos de administradores de sistemas, redes, bases de datos o aplicaciones críticas deberán estar justificados y documentados.
- Estas cuentas se limitarán a lo estrictamente necesario y no podrán utilizarse para tareas cotidianas.
- Toda asignación de privilegios será aprobada por el propietario del activo y registrada en sistemas de auditoría.
- Las acciones realizadas con privilegios elevados deberán quedar documentadas en logs de seguridad que serán revisados regularmente por TI y el Comité de Seguridad.
- Los accesos privilegiados deberán ser objeto de una revisión formal y documentada al menos una vez al año, realizada por el Comité de Seguridad y el área de Infraestructura. Los resultados de esta revisión deberán registrarse en actas o reportes oficiales del SGSI, a fin de garantizar la trazabilidad y disponibilidad de evidencia para auditorías internas o externas.

7 Accesos a sistemas, aplicaciones y datos

El acceso a sistemas y datos corporativos se gestiona de manera controlada, asegurando que solo usuarios autorizados tengan acceso a la información necesaria para su labor.

- La solicitud de accesos debe realizarse formalmente por el supervisor directo y contar con la autorización del propietario del activo.
- Los permisos se asignarán siguiendo perfiles predefinidos y roles de usuario, que limitan las funciones disponibles según la necesidad.
- Los sistemas críticos o sensibles deberán contar con controles adicionales de protección y, siempre que sea posible, estar aislados de sistemas de menor criticidad.
- Los propietarios de activos realizarán una revisión anual de todos los accesos otorgados, ajustando las altas y bajas necesarias.
- El acceso de terceros estará condicionado a acuerdos de confidencialidad y a la autorización formal de la organización.

8 Acceso remoto y teletrabajo

La protección del acceso a redes y modalidades de teletrabajo es esencial para prevenir accesos no autorizados y mantener la continuidad del negocio.

- Todo acceso a la red interna y a servicios corporativos deberá estar formalmente autorizado y registrado.
- El perímetro de red será protegido con firewalls y reglas de filtrado previamente aprobadas y monitoreadas en tiempo real.
- Cualquier interconexión con redes externas, como las de clientes o proveedores, deberá contar con aprobación expresa del Comité de Seguridad, además de autenticación robusta, cifrado y registro de eventos.
- El teletrabajo y acceso remoto solo se permitirá a través de la VPN corporativa con MFA, y mediante dispositivos autorizados y gestionados por Interfase ISA.
- El acceso remoto y el teletrabajo se realizarán exclusivamente mediante la VPN corporativa y autenticación multifactor (MFA), utilizando únicamente dispositivos autorizados y gestionados por Interfase ISA. Los terceros con acceso remoto deberán firmar un acuerdo de confidencialidad y uso aceptable, y además incluir cláusulas de seguridad en sus contratos que aseguren el cumplimiento de los lineamientos de esta política. Todas las interconexiones con redes externas deberán estar autorizadas previamente por el Comité de Seguridad y contar con medidas de cifrado, autenticación robusta, monitoreo y registro de eventos.

9 Monitoreo, revisión y revocación de accesos

La efectividad de los controles de acceso depende de su monitoreo constante y de la oportuna revocación de accesos no vigentes. Además de la revisión anual, los accesos a sistemas críticos deberán revisarse obligatoriamente tras incidentes relevantes (por ejemplo, fuga de información, compromiso de cuentas privilegiadas o hallazgos de auditoría), dejando evidencia de las altas/bajas y ajustes de privilegios realizados.

- Todos los accesos se registrarán en logs de seguridad que permitirán detectar accesos indebidos o intentos fallidos reiterados.
- Los accesos de colaboradores desvinculados o con cambios de rol serán revocados inmediatamente, en coordinación entre RRHH y TI.
- El Comité de Seguridad garantizará una revisión de los accesos a sistemas críticos, mínimo una vez al año o tras incidentes relevantes, consolidando reportes que serán elevados a Directorio.
- Las auditorías internas y externas del SGSI incluirán la verificación de la aplicación de estos controles.

10 Cumplimiento y revisión

El cumplimiento de esta política es obligatorio para todos los colaboradores, contratistas y terceros que procesen información en nombre de Interfase ISA.

El incumplimiento será gestionado conforme a lo definido en la Política General de Seguridad de la Información y en 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 del proceso de revisión del SGSI, asegurando visibilidad y compromiso del Directorio en la mejora continua del sistema.

11 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 se encuentre publicada y accesible, así como de coordinar su revisión periódica. La presente política

deberá revisarse al menos una vez al año, o antes si ocurren cambios relevantes en el contexto legal, contractual, organizacional o tecnológico.

Toda modificación deberá quedar registrada bajo control de versiones y ser sometida a aprobación del 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