

|                                                                                                                                    |                                                          |                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | Política de Seguridad de la Información y Ciberseguridad | <br>Edición: 2.0 |
|                                                                                                                                    | CO n. 034                                                | Fecha: 28/09/2026                                                                                   |

CO n.034 – 28/09/2026

## Política de Seguridad de la Información y Ciberseguridad

|                                   | Nombre Apellido(s)           | Cargo                                 | Firma                 |
|-----------------------------------|------------------------------|---------------------------------------|-----------------------|
| <b><u>Elaborado</u></b>           | <b>Paolo Trevisan</b>        | Jefe de Security                      | <b><u>FIRMADO</u></b> |
|                                   | <b>Alexis Martin Montero</b> | Resp. Arquitectura cloud IT           | <b><u>FIRMADO</u></b> |
| <b><u>Revisado</u></b>            | <b>Marino Santopinto</b>     | Director Técnico                      | <b><u>FIRMADO</u></b> |
|                                   | <b>Rafael Gonzalez</b>       | Director Sistema de Información IT    | <b><u>FIRMADO</u></b> |
| <b><u>Conforme con el SGI</u></b> | <b>Mª del Pilar Pedroche</b> | Jefe HSQE                             | <b><u>FIRMADO</u></b> |
| <b><u>Aprobado</u></b>            | <b>Fabrizio Favara</b>       | Consejero Delegado y Director General | <b><u>FIRMADO</u></b> |

|                                                                                                                                    |                                                                   |                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <h1>Política de Seguridad de la Información y Ciberseguridad</h1> |  |
|                                                                                                                                    |                                                                   | Edición: 2.0                                                                        |
| CO n. 034                                                                                                                          |                                                                   | Fecha: 28/09/2026                                                                   |

## **CONTROL DE MODIFICACIONES**

| Versión | Fecha      | Modificaciones                                                                                                                                                            |
|---------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | 30/08/2024 | Primera edición de la Política de Seguridad de la Información y Ciberseguridad IRYO/ILSA.                                                                                 |
| 2       | 28/09/2026 | Versión integrada: ampliación con referencias normativas, objetivos estratégicos, gestión de proveedores, seguridad en nube, continuidad, auditoría y revisión periódica. |

|                                                                                                                                    |                                                                     |                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p>Política de Seguridad de la<br/>Información y Ciberseguridad</p> | <br>Edición: 2.0<br><br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                           |                                                                                                                              |

## INDICE DE CONTENIDOS

### Contenido

|                                                                     |    |
|---------------------------------------------------------------------|----|
| 1. Objeto .....                                                     | 4  |
| 2. Alcance .....                                                    | 4  |
| 3. Documentación de referencia .....                                | 5  |
| 4. Definiciones .....                                               | 6  |
| 5. Principios y objetivos estratégicos .....                        | 7  |
| 5.1 Principios básicos de actuación .....                           | 7  |
| 5.2 Objetivos estratégicos .....                                    | 7  |
| 5.3 Objetivos principales de seguridad .....                        | 8  |
| 6. Desarrollo: políticas de seguridad cibernética .....             | 8  |
| 6.1 Cumplimiento normativo y protección de datos .....              | 8  |
| 6.3 Control de accesos, contraseñas y autenticación .....           | 9  |
| 6.4 Clasificación, manejo y cifrado de la información .....         | 10 |
| 6.5 Actualizaciones, parches y gestión de vulnerabilidades .....    | 10 |
| 6.6 Almacenamiento, copias de seguridad y recuperación .....        | 11 |
| 6.7 Seguridad en puesto de trabajo y dispositivos .....             | 11 |
| 6.8 Uso de correo electrónico y herramientas colaborativas .....    | 12 |
| 6.9 Seguridad en red, Wi-Fi, acceso remoto y segmentación .....     | 12 |
| 6.10 Seguridad en la nube .....                                     | 13 |
| 6.11 Gestión de proveedores y terceros .....                        | 13 |
| 6.12 Monitorización, cibervigilancia y respuesta a incidentes ..... | 13 |
| 6.13 Continuidad de negocio y recuperación ante desastres .....     | 14 |
| 6.14 Concienciación y capacitación .....                            | 14 |
| 7. Responsabilidades .....                                          | 14 |
| 8. Cumplimiento, auditoría y mejora continua .....                  | 16 |
| 9. Incumplimiento y consecuencias .....                             | 16 |
| 10. Registros y anexos .....                                        | 16 |

|                                                                                                                                    |                                                                                                        |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p style="text-align: center;"><b>Política de Seguridad de la<br/>Información y Ciberseguridad</b></p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                                                              |                                                                                                                          |

## 1. Objeto

El objeto de esta Política es establecer los principios, responsabilidades y marco de gobierno de Seguridad de la Información y Ciberseguridad de IRYO/ILSA para proteger la información, los servicios, los sistemas IT y OT y los activos asociados frente a amenazas que puedan afectar a su confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad. La Política constituye el marco general del SGSI y se desarrolla mediante políticas, procedimientos, estándares y planes específicos. Los riesgos físicos que puedan afectar a la información, los sistemas o la operación se gestionarán bajo el principio de Security Convergence, correspondiendo los controles físicos específicos a la Política de Seguridad Física.

## 2. Alcance

Esta política aplica a todos los centros de trabajo actuales y futuros de IRYO/ILSA, así como a cualquier ubicación desde la que se utilicen recursos informáticos de la compañía, incluyendo teletrabajo, desplazamientos, talleres, oficinas, puntos de venta, estaciones y entornos de operación o soporte.

El alcance subjetivo comprende a empleados, directivos, colaboradores, personal subcontratado, proveedores, terceros y cualquier entidad que tenga acceso, directo o indirecto, a información, sistemas, redes, aplicaciones, dispositivos, servicios en la nube o recursos tecnológicos de IRYO/ILSA.

El alcance material incluye toda la información corporativa, operativa, comercial, técnica, financiera, contractual, de clientes, empleados o proveedores, tanto si se encuentra almacenada como si se transmite por correo electrónico, aplicaciones corporativas, redes, soportes físicos, plataformas cloud, sistemas OT/IT o cualquier otro medio.

Quedan incluidos los servidores corporativos, intranet, sitios web, correo electrónico corporativo, herramientas colaborativas, bases de datos, sistemas de almacenamiento, dispositivos móviles, equipos portátiles, redes Wi-Fi, VPN, entornos productivos y no productivos, plataformas de seguridad, sistemas de monitorización, servicios de terceros y cualquier solución tecnológica utilizada para la actividad de la compañía.

Las instalaciones y activos físicos quedan incluidos únicamente en cuanto puedan originar o verse afectados por riesgos de Seguridad de la Información, Ciberseguridad u OT, remitiéndose su control específico a la Política de Seguridad Física.

|                                                                                                                                    |                                                                        |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p><b>Política de Seguridad de la Información y Ciberseguridad</b></p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                              |                                                                                                                          |

### 3. Documentación de referencia

- GR\_PY Cyber & Information Security n.86 v.01 y COI 46/AU de 17/02/2026, una vez confirmada su adopción formal aplicable a IRYO.
- GR\_LG OT Cyber & Information Security n.153 v.01 y COI 75/AD de 11/05/2026, una vez confirmada su adopción formal aplicable a IRYO.

La política se apoya en el cuerpo normativo interno de IRYO/ILSA y en marcos de referencia reconocidos para la gestión de la seguridad de la información, la ciberseguridad y la continuidad de negocio. Las referencias se utilizarán como guía para interpretar, desplegar, auditar y mejorar los controles definidos.

| Referencia                                            | Aplicación en esta política                                                                                                                              |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO/IEC 27001 e ISO/IEC 27002                         | Buenas prácticas para establecer, mantener y mejorar un sistema de gestión de seguridad de la información y su catálogo de controles.                    |
| NIST Cybersecurity Framework                          | Marco de identificación, protección, detección, respuesta y recuperación ante riesgos e incidentes de ciberseguridad.                                    |
| NIST SP 800-53                                        | Catálogo de controles técnicos, organizativos y operativos para sistemas de información.                                                                 |
| Guías CCN-STIC y CCN-CERT                             | Buenas prácticas de protección, configuración, monitorización y respuesta ante incidentes aplicables a entornos corporativos.                            |
| INCIBE                                                | Guías, recursos y kits de concienciación para empresas y empleados.                                                                                      |
| RGPD, LOPDGDD y normativa de privacidad               | Obligaciones relativas al tratamiento, confidencialidad, integridad y disponibilidad de datos personales.                                                |
| Directiva NIS2 y normativa nacional de transposición  | Requisitos de gestión de riesgos, gobernanza, continuidad, notificación de incidentes y seguridad de la cadena de suministro cuando resulten aplicables. |
| PCI-DSS                                               | Controles aplicables a entornos o procesos vinculados a datos de tarjetas de pago, cuando proceda.                                                       |
| CO n. 004 - Uso de recursos tecnológicos corporativos | Procedimiento interno de referencia para el uso adecuado de recursos tecnológicos y correo electrónico corporativo.                                      |

|                                                                                                                                    |                                                                 |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p>Política de Seguridad de la Información y Ciberseguridad</p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                       |                                                                                                                          |

#### 4. Definiciones

**Activo:** Cualquier elemento de valor para la compañía que deba protegerse frente a riesgos, incluyendo información, sistemas, aplicaciones, infraestructuras, dispositivos, servicios, reputación, personas, procesos y software.

**Activo de información:** Información y sistemas que la procesan, almacenan, transmiten o gestionan, tales como bases de datos, documentación técnica, contratos, información de clientes, planes de continuidad, auditorías, procedimientos y archivos corporativos.

**Ciberseguridad:** Conjunto de medidas técnicas, organizativas y humanas orientadas a proteger los sistemas, redes, aplicaciones y datos frente a ciberamenazas.

**Confidencialidad:** Propiedad por la que la información solo está disponible para personas, procesos o entidades autorizadas.

**Integridad:** Propiedad por la que la información y los sistemas se mantienen completos, exactos y protegidos frente a modificaciones no autorizadas.

**Disponibilidad:** Propiedad por la que los sistemas y datos pueden ser utilizados por usuarios autorizados cuando son necesarios.

**Evento de seguridad:** Suceso que indica que un control puede haber fallado o que una política de seguridad puede no haberse cumplido.

**Incidente de seguridad:** Evento que puede suponer acceso, uso, modificación, interrupción, destrucción o revelación no autorizada de información, sistemas o servicios.

**Fuga de información:** Incidente confirmado en el que se ha producido acceso, uso, modificación, pérdida o revelación no autorizada de información protegida.

**Política de seguridad:** Documento de alto nivel que establece directrices generales y compromisos de seguridad de la información.

**Norma de seguridad:** Regla obligatoria que regula una materia concreta de seguridad, como contraseñas, acceso, cifrado, uso de dispositivos o gestión de incidentes.

**Procedimiento de seguridad:** Secuencia de pasos definidos para ejecutar de forma controlada una actividad de seguridad.

**Estándar de seguridad:** Requisito técnico o configuración mínima que debe cumplirse de forma uniforme en sistemas, aplicaciones o servicios.

**Guía de seguridad:** Documento de orientación o buenas prácticas que ayuda a aplicar políticas y normas, sin sustituir controles obligatorios.

|                                                                                                                                    |                                                                        |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p><b>Política de Seguridad de la Información y Ciberseguridad</b></p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                              |                                                                                                                          |

## 5. Principios y objetivos estratégicos

### 5.1 Principios básicos de actuación

**Safety First:** cuando una decisión de ciberseguridad afecte a sistemas OT o a servicios cuya indisponibilidad o alteración pueda afectar a la seguridad de la operación ferroviaria, deberá evaluarse prioritariamente su impacto sobre Safety y continuidad operacional.

En entornos OT, la priorización de los objetivos de protección considerará, de acuerdo con el riesgo operacional, Disponibilidad, Integridad y Confidencialidad, sin excluir las obligaciones de protección aplicables a ninguna de estas dimensiones.

Aplicar un enfoque preventivo, integral y proporcionado, orientado a reducir riesgos físicos, lógicos, operativos y de terceros.

Proteger adecuadamente la información, los sistemas de control, las comunicaciones y las infraestructuras críticas para la prestación del servicio ferroviario.

Asegurar la continuidad de los servicios esenciales mediante medidas de resiliencia, copias de seguridad, redundancia y recuperación ante desastres.

Combatir el fraude, proteger la marca IRYO y preservar la confianza de clientes, empleados, proveedores y socios.

Garantizar el derecho a la protección de datos personales de clientes, empleados, candidatos, proveedores y demás personas físicas vinculadas a la compañía.

Aplicar medidas de seguridad eficientes y alineadas con el nivel de riesgo, evitando controles desproporcionados que dificulten injustificadamente la actividad.

Fomentar una cultura de seguridad mediante acciones periódicas de divulgación, formación, simulación y concienciación.

Transmitir los principios de esta política a proveedores y terceros, incluyendo requisitos de seguridad en los procesos de contratación y evaluación.

Actuar conforme a la legislación vigente, el código ético, el sistema de gobierno interno y las obligaciones contractuales asumidas por la compañía.

### 5.2 Objetivos estratégicos

Garantizar la confidencialidad, integridad y disponibilidad de la información y de los sistemas IT/OT relevantes para la operación.

Fortalecer la ciberresiliencia frente a incidentes, ciberataques, errores humanos, fallos técnicos y eventos de terceros.

|                                                                                                                                    |                                                                 |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p>Política de Seguridad de la Información y Ciberseguridad</p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                       |                                                                                                                          |

Cumplir las normativas y estándares de ciberseguridad, privacidad, continuidad y seguridad sectorial aplicables.

El compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información.

El compromiso de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Gestionar los riesgos de ciberseguridad en toda la cadena de suministro y durante el ciclo de vida de los sistemas.

Mejorar continuamente el sistema de gestión de ciberseguridad mediante indicadores, auditorías, revisión de incidentes y planes de mejora.

Asegurar una respuesta coordinada y documentada ante incidentes de seguridad, con notificación interna y externa cuando proceda.

### 5.3 Objetivos principales de seguridad

**Confidencialidad:** el acceso a información y sistemas debe limitarse a usuarios autorizados y a las necesidades de sus funciones. Se aplicarán mecanismos de control de acceso, MFA, segmentación, cifrado y registro de actividad especialmente sobre datos sensibles y roles privilegiados.

**Integridad:** los datos, sistemas y configuraciones deben protegerse frente a modificaciones no autorizadas. Se mantendrán registros de actividad, controles de cambios, copias de seguridad y mecanismos de validación que permitan detectar y corregir alteraciones indebidas.

**Disponibilidad:** los sistemas y datos deben estar disponibles para usuarios autorizados cuando sean necesarios. Se implementarán medidas de respaldo, redundancia, continuidad, recuperación ante desastres y monitorización para minimizar indisponibilidades.

## 6. Desarrollo: políticas de seguridad cibernética

### 6.1 Cumplimiento normativo y protección de datos

IRYO/ILSA debe operar dentro de los límites legales, regulatorios, contractuales y éticos aplicables, protegiendo la información sensible de clientes, empleados, proveedores y demás partes interesadas.

Los datos personales se tratarán conforme al RGPD, la LOPDGDD y las políticas internas de privacidad.

|                                                                                                                                    |                                                                                                        |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p style="text-align: center;"><b>Política de Seguridad de la<br/>Información y Ciberseguridad</b></p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                                                              |                                                                                                                          |

La información confidencial deberá cifrarse en tránsito y, cuando proceda por clasificación o riesgo, también en reposo.

La información deberá clasificarse, etiquetarse, manejarse y compartirse conforme a la Política de Clasificación de la Información. Las medidas criptográficas se aplicarán de forma proporcional a la clasificación, criticidad, riesgo y requisitos legales o contractuales. Los algoritmos, protocolos, mecanismos de gestión de claves, certificados, secretos y excepciones se establecerán en la Política de Criptografía y en el estándar técnico criptográfico vigente.

El acceso a datos de clientes, empleados y proveedores se limitará mediante privilegios, aprobaciones y segregación de funciones gestionadas por Tecnología.

Los procesos sujetos a PCI-DSS deberán mantenerse bajo controles específicos y escaneos periódicos de cumplimiento.

Se mantendrán evidencias de cumplimiento, revisiones, aprobaciones, auditorías, excepciones y acciones correctoras.

## 6.2 Gestión de riesgos

La gestión de riesgos de ciberseguridad debe identificar amenazas, vulnerabilidades, impactos y controles necesarios sobre activos críticos, sistemas productivos, datos personales, servicios en la nube, entornos de operación y terceros relevantes.

Se realizarán evaluaciones periódicas de riesgo sobre sistemas críticos y cambios significativos.

Los riesgos se clasificarán según probabilidad, impacto y criticidad para la continuidad del negocio.

Las medidas de tratamiento deberán priorizar la reducción del riesgo a niveles aceptables y documentar los riesgos residuales.

Los resultados relevantes se comunicarán a la Dirección de Tecnología y, cuando corresponda, a la Dirección Ejecutiva.

## 6.3 Control de accesos, contraseñas y autenticación

El acceso a información y sistemas se concederá conforme a los principios de necesidad de saber, mínimo privilegio y segregación de funciones, y se gestionará durante todo su ciclo de vida de acuerdo con la Política de Control de Accesos y el procedimiento de gestión de identidades. En bajas definitivas o finalización de la relación contractual, los accesos

|                                                                                                                                    |                                                                                                        |                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p style="text-align: center;"><b>Política de Seguridad de la<br/>Información y Ciberseguridad</b></p> | <div style="text-align: center;">  </div> <div> Edición: 2.0<br/> CO n. 034<br/> Fecha: 28/09/2026 </div> |
|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

serán revocados conforme al procedimiento establecido. En cambios de función se ajustarán a las nuevas necesidades. En ausencias temporales, la suspensión o restricción de accesos se determinará considerando la duración de la ausencia, criticidad del puesto, tipo de acceso, necesidad operativa y riesgo asociado.

Los usuarios son responsables de proteger sus credenciales y utilizar los accesos asignados exclusivamente para las funciones autorizadas. El acceso a sistemas críticos e información confidencial estará limitado por necesidad de uso, mínimo privilegio y segregación de funciones.

Los requisitos de autenticación, MFA, cuentas privilegiadas y credenciales técnicas se desarrollan en la Política de Control de Accesos y en los estándares técnicos aplicables.

Se aplicará autenticación multifactor mediante Microsoft Authenticator u otro mecanismo aprobado para accesos corporativos, roles privilegiados, acceso remoto y servicios expuestos.

Las contraseñas deberán cumplir requisitos mínimos de longitud, complejidad y no reutilización. La compañía podrá elevar estos requisitos según el nivel de riesgo del sistema.

Las cuentas privilegiadas, claves SSH, OTP y secretos técnicos deberán custodiarse en una herramienta aprobada de gestión de contraseñas o secretos.

Los accesos se revocarán cuando dejen de ser necesarios por cambio de rol, baja temporal, baja definitiva o finalización de relación contractual.

Tecnología revisará periódicamente los accesos a aplicaciones y sistemas, manteniendo registro de actividad para detectar intrusiones o usos indebidos.

#### **6.4 Clasificación, manejo y cifrado de la información**

La información deberá clasificarse, etiquetarse, manejarse y compartirse conforme a la Política de Clasificación de la Información. Las medidas criptográficas se aplicarán de forma proporcional a la clasificación, criticidad, riesgo y requisitos legales o contractuales. Los algoritmos, protocolos, mecanismos de gestión de claves, certificados, secretos y excepciones se establecerán en la Política de Criptografía y en el estándar técnico criptográfico vigente

#### **6.5 Actualizaciones, parches y gestión de vulnerabilidades**

IRYO mantendrá un proceso de identificación, evaluación, priorización y tratamiento de vulnerabilidades técnicas conforme a la criticidad y exposición de los activos. Los criterios

|                                                                                                                                    |                                                                 |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p>Política de Seguridad de la Información y Ciberseguridad</p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                       |                                                                                                                          |

técnicos, frecuencias, SLAs y excepciones se desarrollarán en la Política y Procedimiento de Gestión de Vulnerabilidades.

## 6.6 Almacenamiento, copias de seguridad y recuperación

Las copias de seguridad deben garantizar la recuperación de información crítica ante incidentes, errores humanos, corrupción de datos, fallos de hardware, ataques de ransomware o desastres.

IRYO mantendrá mecanismos de copia de seguridad y restauración proporcionales a la criticidad de la información y de los servicios, alineados con los RPO y RTO aprobados. Las frecuencias, retenciones, tecnologías, medidas de protección, monitorización y pruebas de restauración se establecerán en la Política de Backup y en las matrices y procedimientos técnicos asociados. La capacidad de recuperación deberá coordinarse con el Plan de Continuidad de Negocio y el IT Recovery Plan.

Información de Adif, Control Room, ILSA IT y Train Sec: mantenimiento de versiones y periodo de gracia de borrado de 365 días, con redundancia geográfica cuando aplique.

Webs: periodo de gracia de borrado de 7 días en todos los entornos.

Documentación en Teams y SharePoint, correo electrónico y OneDrive de mandos directivos y managers: copia diaria según los procedimientos de Tecnología.

Los discos de equipos corporativos deberán protegerse mediante BitLocker u otro cifrado aprobado.

Se realizarán pruebas periódicas de restauración, al menos quincenales para bases de datos productivas y servidores relevantes, verificando legibilidad y consistencia de los datos recuperados.

## 6.7 Seguridad en puesto de trabajo y dispositivos

Los puestos de trabajo y dispositivos corporativos deberán configurarse conforme a estándares de seguridad definidos por Tecnología, evitando modificaciones no autorizadas y reduciendo el riesgo de compromiso.

La instalación de software y cambios de configuración que requieran privilegios administrativos deberán ser gestionados por Tecnología.

Los equipos deberán contar con protección antimalware/EDR, cifrado de disco, bloqueo automático y configuración segura.

Los dispositivos móviles corporativos deberán gestionarse mediante MDM/Intune y configurarse con PIN no correlativo u otro mecanismo equivalente aprobado.

|                                                                                                                                    |                                                                        |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p><b>Política de Seguridad de la Información y Ciberseguridad</b></p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                              |                                                                                                                          |

Los dispositivos perdidos, robados o comprometidos deberán notificarse inmediatamente para su bloqueo, borrado remoto o revocación de accesos.

No se permitirá el uso de dispositivos no autorizados para acceder a información Confidencial salvo aprobación expresa y controles compensatorios.

### **6.8 Uso de correo electrónico y herramientas colaborativas**

Las cuentas de correo electrónico y herramientas colaborativas de IRYO/ILSA son propiedad de la compañía y se reservan para uso profesional conforme al procedimiento CO n. 004 y las normas internas aplicables.

El correo corporativo deberá estar protegido mediante filtrado avanzado, políticas antispam, antiphishing y antimalware.

El acceso desde ubicaciones no confiables o fuera de la Unión Europea podrá bloquearse automáticamente, salvo autorización excepcional del Departamento de IT.

Los usuarios deberán extremar la precaución ante adjuntos, enlaces, solicitudes de credenciales, cambios de cuenta bancaria, instrucciones urgentes o comunicaciones sospechosas.

La información confidencial enviada por correo o herramientas colaborativas deberá compartirse con destinatarios autorizados y, cuando proceda, mediante cifrado, enlaces controlados o permisos limitados.

### **6.9 Seguridad en red, Wi-Fi, acceso remoto y segmentación**

La infraestructura de red deberá protegerse mediante firewalls, segmentación, controles de acceso, monitorización y sistemas de detección o prevención de intrusiones.

Las sedes de IRYO/ILSA mantendrán redes Wi-Fi separadas para empleados, invitados, dispositivos móviles y clientes cuando aplique.

Las redes de invitados y públicas deberán configurarse para impedir visibilidad o acceso a otros dispositivos internos.

El acceso de bajo nivel a bases de datos, mensajería, cachés, Kubernetes u otros sistemas técnicos deberá realizarse mediante VPN u otros mecanismos aprobados.

Los servicios web internos deberán protegerse mediante controles de Zero Trust, autenticación y autorización reforzada.

Se mantendrá segmentación entre entornos productivos, preproductivos, desarrollo y redes de usuario, evitando que datos personales de clientes estén disponibles en entornos no productivos salvo anonimización o aprobación específica.

|                                                                                                                                    |                                                                        |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p><b>Política de Seguridad de la Información y Ciberseguridad</b></p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                              |                                                                                                                          |

## 6.10 Seguridad en la nube

La contratación y uso de servicios cloud deberá someterse a evaluación de riesgo, requisitos de seguridad, protección de datos, gestión de proveedores, continuidad y estrategia de salida conforme a la Política de Seguridad Cloud.

## 6.11 Gestión de proveedores y terceros

Los proveedores y terceros que accedan a sistemas, redes, datos o servicios de IRYO/ILSA deberán cumplir los requisitos de seguridad establecidos por la organización, de forma proporcional al riesgo y al tipo de acceso concedido.

Los contratos y acuerdos con proveedores deberán incorporar, cuando resulte aplicable, cláusulas relativas a confidencialidad, protección de datos, seguridad de la información, notificación de incidentes, subcontratación, continuidad del servicio y derecho de auditoría.

Con carácter previo a la concesión de accesos, se realizará la evaluación correspondiente dentro del proceso de homologación del proveedor y se asignarán únicamente los permisos necesarios para el desempeño de las funciones autorizadas, aplicando el principio de mínimo privilegio.

Los accesos concedidos a proveedores y terceros deberán ser trazables, revisables y gestionados durante todo el periodo de vigencia de su homologación. Su mantenimiento, modificación o revocación estará vinculado al estado de homologación del proveedor y a las necesidades del servicio, siendo retirados cuando el proveedor deje de estar homologado o cuando ya no exista una necesidad de acceso.

Todos los proveedores homologados serán sometidos a un proceso de reevaluación al finalizar el periodo de homologación establecido por la organización, con el fin de verificar que continúan cumpliendo los requisitos aplicables en materia de seguridad, calidad y cumplimiento.

Cualquier incidente de seguridad que afecte a un proveedor o tercero y pueda tener impacto sobre los sistemas, servicios o información de IRYO/ILSA deberá notificarse y gestionarse conforme al procedimiento de gestión de incidentes de seguridad de la organización.

## 6.12 Monitorización, cibervigilancia y respuesta a incidentes

Los eventos e incidentes de Seguridad de la Información y Ciberseguridad deberán detectarse, registrarse, evaluarse, escalar y gestionarse conforme a la Política y Procedimiento de Gestión de Incidentes. Los incidentes con potencial impacto OT o Safety requerirán coordinación con las funciones operativas y de seguridad correspondientes.

|                                                                                                                                    |                                                                 |                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <p>Política de Seguridad de la Información y Ciberseguridad</p> | <br>Edición: 2.0<br>Fecha: 28/09/2026 |
|                                                                                                                                    | CO n. 034                                                       |                                                                                                                          |

Función de Seguridad de la Información/Ciberseguridad designada por IRYO: definir criterios de Seguridad de la Información y Ciberseguridad, supervisar y monitorizar la adecuación de los controles, participar en la gestión de riesgos y excepciones y realizar funciones de control independientes de las operaciones IT.

### 6.13 Continuidad de negocio y recuperación ante desastres

IRYO/ILSA deberá mantener medidas de continuidad y recuperación que permitan restaurar servicios esenciales, sistemas críticos y datos relevantes en caso de incidente grave, desastre, indisponibilidad prolongada o ciberataque.

Los sistemas críticos deberán contar con estrategias de respaldo, recuperación y redundancia proporcionales a su criticidad.

El Plan de Recuperación ante Desastres (DRP) deberá probarse periódicamente y actualizarse ante cambios relevantes de infraestructura, procesos o riesgos.

Las pruebas deberán validar tiempos de recuperación, integridad de datos, dependencias técnicas, roles de actuación y comunicaciones.

Los resultados de pruebas, simulacros e incidentes reales deberán alimentar planes de mejora.

### 6.14 Concienciación y capacitación

La ciberseguridad es una responsabilidad compartida. IRYO/ILSA promoverá la formación continua y la concienciación de empleados, personal externo y perfiles con acceso a información o sistemas corporativos.

Se impartirán acciones periódicas sobre phishing, malware, ingeniería social, uso seguro del correo, protección de credenciales, clasificación de información y notificación de incidentes.

Los perfiles con funciones técnicas, administrativas o acceso privilegiado recibirán formación específica acorde a sus responsabilidades.

La compañía podrá realizar simulaciones, campañas y comunicaciones internas para reforzar hábitos seguros.

La participación en formación y concienciación podrá registrarse como evidencia de cumplimiento.

## 7. Responsabilidades

| Responsable | Funciones |
|-------------|-----------|
|-------------|-----------|

|                                                                                                                                    |                                                                   |                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <h2>Política de Seguridad de la Información y Ciberseguridad</h2> | <br>Edición: 2.0<br>CO n. 034<br>Fecha: 28/09/2026 |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|

|                                         |                                                                                                                                                                                                                                                   |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dirección Ejecutiva                     | <p>Proporcionar liderazgo y apoyo para implementar y mantener la ciberseguridad. Asignar recursos adecuados. Revisar periódicamente el estado de la seguridad y tomar decisiones correctivas cuando sea necesario.</p>                            |
| Dirección de Tecnología                 | <p>Desarrollar, implementar y mantener políticas, normas, estándares y procedimientos de ciberseguridad. Supervisar infraestructura de seguridad, gestión de accesos, vulnerabilidades, monitorización, continuidad y respuesta a incidentes.</p> |
| Operaciones y Gobierno IT               | <p>Coordinar la aplicación de la política, asegurar la trazabilidad de controles, impulsar mejora continua y alinear la gestión de seguridad con los procesos operativos de la compañía.</p>                                                      |
| Chief Safety and Security Officer       | <p>Alinear la ciberseguridad con los requisitos de seguridad y continuidad de la operación ferroviaria, participando en la evaluación de riesgos que puedan impactar servicios esenciales.</p>                                                    |
| Asesoría Jurídica / Protección de Datos | <p>Apoyar la implementación de obligaciones legales, privacidad, protección de datos, procedimientos laborales o penales y auditorías tecnológicas cuando proceda.</p>                                                                            |
| Calidad / SGI                           | <p>Asegurar la coherencia de esta Política con el Sistema de Gestión Integrado, coordinar el control documental y facilitar las evidencias requeridas por los procesos de auditoría y mejora</p>                                                  |

|                                                                                                                                    |                                                                   |                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <h1>Política de Seguridad de la Información y Ciberseguridad</h1> |  |
|                                                                                                                                    |                                                                   | Edición: 2.0                                                                        |
| CO n. 034                                                                                                                          |                                                                   | Fecha: 28/09/2026                                                                   |

|                              |                                                                                                                                                                                            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Empleados y personal externo | Cumplir políticas y procedimientos, proteger credenciales, utilizar recursos corporativos de forma adecuada, informar de actividad sospechosa y participar en formación de ciberseguridad. |
| Proveedores y terceros       | Cumplir los requisitos contractuales y técnicos de seguridad, proteger la información de IRYO/ILSA, notificar incidentes y colaborar en auditorías o revisiones cuando aplique.            |

## 8. Cumplimiento, auditoría y mejora continua

IRYO/ILSA podrá realizar auditorías periódicas, revisiones técnicas, análisis de cumplimiento y controles internos para verificar la aplicación de esta política, detectar desviaciones, evaluar vulnerabilidades y definir acciones correctoras.

Las auditorías podrán cubrir accesos, configuración de sistemas, cumplimiento normativo, copias de seguridad, proveedores, nube, respuesta a incidentes y concienciación.

Las desviaciones deberán documentarse, priorizarse y tratarse mediante planes de acción con responsable y plazo.

La política se revisará al menos anualmente o cuando se produzcan cambios relevantes en sistemas, riesgos, normativa, organización, proveedores o incidentes significativos.

Los indicadores de seguridad, resultados de auditoría, informes de incidentes, vulnerabilidades y pruebas de continuidad servirán como base para la mejora continua.

## 9. Incumplimiento y consecuencias

El incumplimiento de esta política o de las normas y procedimientos derivados podrá conllevar la revocación de accesos, medidas disciplinarias, finalización de la relación contractual o laboral, exigencia de responsabilidades y, en su caso, comunicación a autoridades competentes.

Las consecuencias se determinarán según la gravedad, intencionalidad, impacto, reiteración, normativa aplicable y obligaciones contractuales o laborales existentes.

## 10. Registros y anexos

Se consideran registros generados por la aplicación de esta política, entre otros, los siguientes documentos y evidencias:

|                                                                                                                                    |                                                                   |                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <br><small>INTERMODALIDAD DE LEVANTE S.A.</small> | <h2>Política de Seguridad de la Información y Ciberseguridad</h2> | <br>Edición: 2.0 |
|                                                                                                                                    |                                                                   | Fecha: 28/09/2026                                                                                   |

Inventario y clasificación de activos de información.

Matriz de riesgos y planes de tratamiento.

Revisiones de accesos y evidencias de alta, modificación o baja de usuarios.

Informes de vulnerabilidades, parches y medidas de mitigación.

Registros de copias de seguridad y pruebas de restauración.

Informes de monitorización, alertas e incidentes de seguridad.

Evidencias de formación y campañas de concienciación.

Evaluaciones de proveedores y cláusulas contractuales de seguridad.

Informes de auditoría, desviaciones y acciones correctoras.

Versiones aprobadas, revisiones y actas de aprobación de la política.