CÓDIGO: NG.FER.SI-001
VERSIÓN: 3.0
FECHA DE PRIMERA PUBLICACIÓN: 27/01/2022
FECHA DE PUBLICACIÓN DE LA VERSIÓN VIGENTE: 22/07/2026
APROBADA POR: CEO

TÍTULO: Política Global de Ciberseguridad
ALCANCE: General
CANCELA A: v.2.0
IDIOMA DE LA VERSIÓN ORIGINAL: Inglés

ÁREA EMISORA: Departamento de Ciberseguridad

HISTORIAL DE REVISIONES

Versión	Fecha de difusión	Motivo y resumen de cambios	Anula/Sustituye:
1.0	27/01/2022	N/A – Versión inicial del documento.	N/A
2.0	22/05/2026	Actualización de la denominación social a Ferrovial N.V., como sociedad matriz del grupo Ferrovial.	Versión Anterior (NG.FER.SI-001, 27/01/2022)
3.0	22/07/2026	Alineación con leyes, regulaciones aplicables (SEC, NIS2) y estándares de ciberseguridad (NIST CSF 2.0 y ENS). Actualización de riesgos, objetivos y capacidades de ciberseguridad.	Versión Anterior (NG.FER.SI-001, 22/05/2026)

ÍNDICE

INTRODUCCIÓN Y FINALIDAD

La finalidad de esta Política Global de Ciberseguridad (la "Política") es establecer los principios y objetivos fundamentales de Seguridad, así como asignar las responsabilidades clave para trabajar en su consecución, orientadas a asegurar la protección de la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la IT, OT e IoT de Ferrovial (según se definen más adelante), así como de la información generada y utilizada en sus procesos de negocio y operaciones, de conformidad con los niveles de sensibilidad y criticidad de Ferrovial, promoviendo al mismo tiempo el cumplimiento de las leyes, regulaciones y acuerdos contractuales que resulten de aplicación.

ALCANCE

La Política aplica a Ferrovial N.V. y a su grupo consolidado y, en general, a cualquier entidad bajo su control directo o indirecto ("Ferrovial"), lo que a estos efectos significará la capacidad de ejercer más del 50 % de los derechos de voto o de nombrar o destituir a la mayoría del órgano de administración o dirección, salvo en aquellas sociedades cuyas estructuras de control impuestas estatutariamente determinen lo contrario y que no se considerarán parte del grupo Ferrovial a efectos de esta Política.

Todos los empleados, colaboradores y terceros incluidos en el ámbito de aplicación de esta Política y de sus documentos relacionados son responsables de conocer, respetar y hacer cumplir sus requisitos.

El Global CISO, responsable de alinear la estrategia de Seguridad con la visión y misión de Ferrovial, será el principal responsable de la comunicación, promoción y cumplimiento de esta Política.

En la medida en que resulte comercialmente viable, se promoverá en los órganos de decisión de aquellas entidades en las que Ferrovial no ostente el control, la aprobación de la alineación de la práctica local de Seguridad con esta Política.

Cualquier incumplimiento de la Política o de las políticas y procedimientos que forman parte de ella podrá ser objeto de sanción por Ferrovial o en su nombre y, cuando corresponda, podrá dar lugar a acciones disciplinarias y/o judiciales.

Definiciones

Las definiciones de los términos de ciberseguridad relevantes utilizados a lo largo del presente documento se recogen en el Anexo I.

Estándares y Requisitos de Referencia

La Política está diseñada para alinearse con los estándares de referencia y los requisitos aplicables incluidos en su Anexo II, que podrán ser modificados cuando sea necesario por el Área Emisora, informando al órgano de aprobación, con el fin de actualizar los estándares regulatorios de ciberseguridad aplicables a Ferrovial.

Los estándares y requisitos anteriores definen el marco tecnológico, organizativo y procedimental que se utilizará para desarrollar, implantar, monitorizar, revisar, mantener y mejorar la Seguridad de Ferrovial.

Principios y Objetivos de Seguridad

Con el fin de apoyar la CID, así como la trazabilidad y autenticidad de su IT, OT, IoT y de la información que sustenta las operaciones de negocio de Ferrovial, la ciberseguridad y la seguridad de la información ("**Seguridad**") en Ferrovial pretenden alinearse con los siguientes Principios y Objetivos de Seguridad, que a su vez dan soporte a la estrategia de Seguridad de Ferrovial:

1. **Existencia de un Entorno Digital y Tecnológico con el Nivel de Seguridad Requerido**, mediante la identificación de amenazas y la gestión de los riesgos asociados, procurando asegurar la protección de la información, del IT, del OT y del IoT, a lo largo de su ciclo de vida.
2. **Cumplimiento de los Requisitos Legales, Regulatorios y Contractuales Aplicables,** mediante la identificación de obligaciones relevantes, la definición de modelos de control adecuados y el soporte de auditorías, revisiones y otras actividades relacionadas con el cumplimiento.
3. **Gestión Adecuada de los Incidentes de Seguridad y Fortalecimiento de la Resiliencia, con el fin** de minimizar su impacto en la organización, dotando a Ferrovial de capacidades de detección y respuesta, así como de los recursos y estrategias necesarios para procurar la resiliencia, la recuperación y la continuidad de los procesos críticos de negocio.
4. **Promoción de una Cultura de Seguridad Adecuada**, mediante la concienciación y formación en ciberseguridad para las personas que diseñan, implantan, operan o utilizan Información, IT, OT e IoT, e integrando una perspectiva de Seguridad en los órganos de gobierno de Ferrovial, proporcionándoles la formación y concienciación necesarias.
5. **Seguridad en la Cadena de Suministro**, mediante la gestión de los riesgos de Seguridad derivados de terceros, de forma proporcional a su criticidad, y promoviendo prácticas de gestión de riesgos en la Cadena de Suministro que favorezcan la consecución de niveles de Seguridad coherentes con los de Ferrovial cuando resulte comercialmente posible.
6. **Armonización de la Seguridad en Ferrovial,** mediante el establecimiento de un modelo de Seguridad alineado con el negocio y la definición clara de roles, responsabilidades y autoridades en materia de Seguridad dentro de Ferrovial.
7. **Facilitación de la Digitalización, la Innovación y la Adopción de Nuevas Tecnologías como Habilitadores del Negocio,** mediante la integración de la Seguridad en las iniciativas de innovación y la evolución de las capacidades y soluciones de Seguridad para dar soporte al negocio.
8. **Facilitación de Oportunidades de Negocio y Procesos de Licitación**, mediante el aprovechamiento del modelo de gobierno, controles y capacidades de Seguridad de Ferrovial como factor diferenciador para apoyar oportunidades de negocio y procesos de licitación.
9. **Establecimiento de Colaboraciones Estratégicas en Materia de Seguridad,** mediante el fomento del intercambio de información, incluidos indicadores y buenas prácticas, y promoviendo la participación activa de Ferrovial en foros e iniciativas sectoriales y globales de Seguridad.

Estos objetivos promueven la alineación con la estrategia de Negocio y de IT, refuerzan la gestión de los riesgos de ciberseguridad, apoyan el cumplimiento de las obligaciones legales, regulatorias y contractuales, mejoran la supervisión de los riesgos de ciberseguridad para la operación del negocio y contribuyen a los esfuerzos para asegurar la resiliencia de la organización en la respuesta y recuperación ante eventos disruptivos relacionados con ciberseguridad e IT.

Capacidades de Seguridad

Los principios y objetivos fundamentales descritos anteriormente se desarrollan mediante un conjunto de capacidades:

- **Gobierno**. Capacidades relacionadas con (i) la comprensión del contexto, procesos, servicios críticos y partes interesadas relevantes para Ferrovial; (ii) el establecimiento y mantenimiento de la estrategia, objetivos y políticas de gestión de riesgos de Seguridad de la organización; (iii) la definición de roles, responsabilidades y rendición de cuentas en materia de Seguridad en toda la organización; (iv) la integración de la Seguridad en la gestión de riesgos empresariales y en los procesos de toma de decisiones; (v) la supervisión por la dirección y la mejora mediante evaluación del desempeño y reporte; (vi) la promoción de una cultura de cumplimiento y comportamiento ético alineada con las obligaciones legales, regulatorias y contractuales aplicables; y (vii) la gestión de los riesgos de Seguridad relacionados con terceros en la Cadena de Suministro.

- **Identificación.** Capacidades relacionadas con (i) la identificación, clasificación y análisis de los activos relevantes para Ferrovial a efectos de Seguridad; (ii) la identificación, análisis y tratamiento de los riesgos de Seguridad que puedan comprometer dichos activos; (iii) la identificación de obligaciones legales y estándares sustantivos en evolución; y (iv) la mejora mediante auditorías, revisiones y procesos de mitigación de riesgos.

- **Protección.** Capacidades relacionadas con la protección de los activos identificados según su nivel de importancia para Ferrovial mediante (i) mecanismos de control de acceso basados en la identidad y en los principios de necesidad de conocer y mínimo privilegio; (ii) la promoción de una cultura de Seguridad adecuada y la impartición de formación o información a empleados y terceros; (iii) la implantación de mecanismos de protección que contribuyan a garantizar la Seguridad de la información; (iv) la adquisición, diseño, construcción y configuración de productos y servicios digitales seguros; (v) la protección y monitorización de redes y canales de comunicación, aplicando líneas de defensa en profundidad conforme a los principios de arquitectura de Seguridad; y (vi) el establecimiento y aplicación de procedimientos para contribuir a asegurar el uso seguro y adecuado de los recursos tecnológicos.

- **Detección.** Capacidades relacionadas con la monitorización continua de (i) productos y servicios digitales; (ii) identidades digitales y su comportamiento; (iii) redes y canales de comunicación; (iv) infraestructura IT, OT e IoT y las instalaciones en las que se alojan; (v) amenazas cibernéticas internas y externas y eventos adversos que puedan afectar a los activos de Ferrovial; y (vi) las herramientas y técnicas utilizadas por los agentes de amenaza.

- **Respuesta**. Capacidades relacionadas con (i) la definición, despliegue, gestión y prueba de planes de respuesta a incidentes cibernéticos que se activen cuando las amenazas cibernéticas puedan afectar o hayan afectado a los activos de Ferrovial; (ii) la realización de actividades de detección, triaje, análisis, contención, escalado y resolución; y (iii) la comunicación con los grupos de interés, incluidos aquellos requeridos por la legislación, regulación o contratos, así como con las unidades de negocio y filiales.

- **Recuperación.** Capacidades relacionadas con (i) asegurar la resiliencia de los activos de Ferrovial para recuperarse del impacto de un evento adverso y volver a la operación normal; (ii) definir, desplegar, gestionar y probar planes de recuperación; y (iii) identificar lecciones aprendidas y aplicarlas para prevenir la recurrencia o escalado de dichos eventos.

Estas capacidades se desarrollarán, implantarán y mantendrán mediante medidas de Seguridad adecuadas basadas en la estructura organizativa, los procesos, las tecnologías, las personas y los recursos aplicables.

Riesgos de Seguridad

Las categorías de riesgo de Seguridad que se indican a continuación proporcionan una taxonomía estratégica de los principales vectores de amenaza aplicables a Ferrovial, que podrá ser actualizada periódicamente. La cuantificación del impacto económico se realizará utilizando criterios alineados con el marco de Gestión de Riesgos Empresariales de Ferrovial, considerando las dimensiones financiera, operacional, legal y reputacional.

NOMBRE DEL RIESGO	DESCRIPCIÓN
Ransomware y Secuestro de Activos	Cifrado o bloqueo del acceso a los activos digitales de Ferrovial, o toma de control de sistemas, infraestructuras o servicios mediante la explotación de vulnerabilidades o configuraciones incorrectas.
Exfiltración y Exposición de Información	Extracción, divulgación o publicación no autorizada de información de Ferrovial, ya sea de forma intencionada o accidental.
Robo y Suplantación de Identidad Digital	Obtención fraudulenta o uso indebido de identidades digitales para obtener acceso no autorizado, cometer fraude o suplantar a personal de Ferrovial.
Disrupción de Activos	Ataques diseñados para degradar, interrumpir o detener la operación normal de los activos de Ferrovial.
Compromiso de la Cadena de Suministro	Riesgos derivados de vulnerabilidades o ataques que afecten a terceros, proveedores y socios.
Deepfakes y Amenazas Potenciadas por la IA	Ataques que utilizan contenido generado o manipulado mediante la IA para engañar a personas o sistemas, para automatizar acciones maliciosas o para evadir mecanismos de detección.
Criptominería	Uso no autorizado de los recursos de computación de Ferrovial para minar criptomonedas.
Robo y pérdida de activos	Robo, pérdida o extravío de activos de Ferrovial, con posible exposición de información sensible o interrupción de las operaciones.
Compromiso de la inteligencia artificial y de la integridad de los datos	Compromiso de la integridad, confidencialidad o fiabilidad de los datos o modelos de IA de Ferrovial mediante ataques adversarios como envenenamiento de datos, inyección de instrucciones o evasión de modelos, o por el mal uso de las herramientas, habilidades y capacidades por parte de empleados o colaboradores.
Tecnologías emergentes y amenazas cuánticas	Riesgos asociados a tecnologías emergentes y disruptivas, incluido el potencial de la computación cuántica para romper los estándares criptográficos asimétricos actuales.

Roles, Organización, Liderazgo y Despliegue

El Consejo de Administración de Ferrovial N.V. ejerce la supervisión de los riesgos y la estrategia de Seguridad, incluida la supervisión de los riesgos materiales y de la eficacia del programa de Seguridad de Ferrovial.

Cuando resulte necesario, los Consejeros Ejecutivos de Ferrovial, junto con la Dirección de Ferrovial, son responsables de aprobar las medidas de gestión de riesgos de Seguridad, supervisar su implantación y revisarlas y actualizarlas periódicamente.

Cuando resulte necesario, los miembros del Consejo de Administración y de la Dirección de Ferrovial deberán recibir formación periódica en Seguridad para adquirir conocimientos y competencias suficientes que les permitan identificar riesgos y evaluar las prácticas de gestión de riesgos de Seguridad y su impacto. Ferrovial promoverá de forma periódica una formación equivalente en toda la organización.

Los empleados y contratistas deberán informar al Departamento de Ciberseguridad de cualquier amenaza potencial identificada en el desarrollo de sus actividades diarias, a través de los canales definidos por Ferrovial. Asimismo, deberán recibir la formación o información adecuada que les permita identificar y responder a dichas amenazas.

El Departamento de Ciberseguridad de Ferrovial es responsable de liderar el despliegue de esta Política en Ferrovial. Se ha definido un modelo formalizado de roles, responsabilidades y estructura organizativa en materia de Seguridad. Este modelo especifica:

- Los roles establecidos para gobernar y desplegar la Seguridad en Ferrovial.
- Las actividades y responsabilidades asignadas a cada rol de Seguridad dentro de su ámbito de competencia definido.
- Cómo serán supervisados por los órganos de Ferrovial los niveles de Seguridad, riesgo y control.
- Cómo ejercerá el Departamento de Ciberseguridad la supervisión de la Seguridad en todo Ferrovial.
- El modelo de colaboración e interacción dentro de Ferrovial.
- Los criterios utilizados para clasificar unidades de negocio y sociedades filiales y asignarlas a niveles de Seguridad.
- Las capacidades y controles de Seguridad requeridos para cada nivel.
- Cómo se medirán a nivel global los niveles de riesgo y control de Seguridad y cómo se reportarán a los órganos de Ferrovial.

La descripción completa de los roles, responsabilidades y órganos de gobierno de Seguridad se recoge en PG.FER.SI.026 (Roles, Responsabilidades y Organización Global de Ciberseguridad). El procedimiento que desarrolla los requisitos de divulgación de incidentes de ciberseguridad de la SEC se define en PG.FER.SI.030 (Cyber Incidents Disclosure Procedure).

Excepciones a esta Política

Podrán permitirse desviaciones respecto de esta Política de forma excepcional, teniendo en cuenta, por ejemplo, justificaciones de negocio, operativas, técnicas o legales, con la debida consideración de los riesgos asociados y la implantación de medidas de mitigación siempre que resulte posible. Cuando proceda, las desviaciones deberán estar limitadas en el tiempo y cesar una vez se hayan abordado las circunstancias que las justificaron.

Las desviaciones deberán documentarse y, siempre que resulte viable, deberá solicitarse la aprobación del Global CISO antes de su implantación.

Cuando resulte aplicable, también deberá tenerse en cuenta el Plan de Respuesta ante Ciber Incidentes de Ferrovial (CIRP, por sus siglas en inglés) y los procedimientos relacionados, en el contexto de una desviación.

Distribución

El Departamento de Ciberseguridad distribuirá esta Política a través de los medios que considere adecuados a todas las partes interesadas en materia de Seguridad, tanto internas como externas. Esta Política no confiere derechos ni recursos a ningún tercero.

Revisión

Esta Política deberá ser revisada al menos anualmente por el Departamento de Ciberseguridad, y siempre que se produzcan cambios significativos o las circunstancias así lo requieran.

Validez

Esta política será de aplicación desde el día que se publique en la Intranet de Ferrovial.

Anexo I – Definiciones

- **IT (Tecnologías de la Información):** Productos y Servicios Digitales que dan soporte a las operaciones corporativas y de negocio de Ferrovial, incluidas aplicaciones, sistemas de información y servicios en la nube.
- **OT (Tecnología Operacional):** Sistemas Industriales utilizados en los activos de infraestructura y concesiones de Ferrovial, incluidos sistemas de control, SCADA y plataformas de automatización industrial.
- **IoT (Internet de las Cosas):** Activos conectados que incorporan capacidades digitales en infraestructuras físicas, incluidos sensores, dispositivos conectados y sistemas inteligentes desplegados en las operaciones de Ferrovial.
- **Confidencialidad, Integridad y Disponibilidad (CID):** Las tres propiedades fundamentales de la Seguridad: Confidencialidad, mediante la prevención de la divulgación no autorizada; Integridad, asegurando la exactitud y completitud; y Disponibilidad, garantizando el acceso oportuno y fiable a los usuarios autorizados.
- **Clasificación de la Información:** proceso mediante el cual los activos de información se categorizan en función de su sensibilidad, criticidad e impacto en el negocio, con el fin de determinar las medidas de protección adecuadas, de conformidad con la Política de Clasificación de la Información de Ferrovial.
- **NIST CSF 2.0:** Marco de Ciberseguridad del National Institute of Standards and Technology, versión 2.0, estándar principal de referencia que estructura las capacidades de ciberseguridad de Ferrovial en torno a las funciones Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar.
- **Global CISO:** Chief Information Security Officer, responsable de definir y liderar la estrategia de Seguridad de Ferrovial a nivel global, según se describe con mayor detalle en PG.FER.SI.026 (Roles, Responsabilidades y Organización Global de Ciberseguridad).
- **Incidente de Seguridad:** Cualquier evento que comprometa o amenace la CID de la IT, OT, IoT o Información de Ferrovial, y que requiera un proceso estructurado de detección, respuesta y recuperación.
- **Cadena de Suministro:** Red de terceros, proveedores, socios y prestadores de servicios cuyo acceso o integración con los sistemas de Ferrovial genera una exposición de ciberseguridad que requiere una gestión de riesgos proporcionada.

ANEXO II – ESTÁNDARES Y REQUISITOS

- NIST CSF (National Institute of Standards in Technology Cybersecurity Framework).
- ISO/IEC 27001 & ISO/IEC 27002.
- Real Decreto 311/2022, del 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS).
- CIS Critical Security Controls (Center for Internet Security).
- Cloud Security Alliance (CSA).
- SEC – Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rules.
- Directiva (EU) 2022/2555 (NIS2 – Network and Information Systems Directive).