CÓDIGO: NG.FER.SI.001
VERSIÓN: 1.0
FECHA DE PRIMERA PUBLICACIÓN: 27/01/2022
FECHA PUBLICACIÓN DE LA VERSIÓN VIGENTE: 27/01/2022
APROBADO POR: Consejero Delegado

TÍTULO: Política Corporativa de Ciberseguridad
ALCANCE: General
CANCELA A: N/A
IDIOMA VERSIÓN ORIGINAL: Español

ÁREA EMISORA: Dirección de Ciberseguridad

Histórico de revisiones

Versión	Fecha de	Motivo y resumen de cambios	Cancela/Sustituye a:
1.0	27/01/2022	N/A - Versión inicial del documento.	N/A

ÍNDICE

Introducción

Ferrovial reconoce la importancia estratégica de sus Productos y Servicios Digitales (en adelante, "IT"), de sus Sistemas Industriales (en adelante, "OT"), de sus Activos Conectados a Internet (en adelante, "IoT") y de la Información que se genera y utiliza en todos los procesos y operaciones que soportan las actividades de su negocio. Representan un elemento esencial para la generación y entrega de valor a sus *stakeholders*.
Asimismo, Ferrovial considera que las normas y procedimientos que regulan la creación, tratamiento, operación y control de los citados activos constituyen un factor clave tanto del desempeño de su actividad como de su reputación.
A tal fin, se establece la presente Política Corporativa de Ciberseguridad (en adelante, "Política de Seguridad"), fundamentada a través de un conjunto de principios y objetivos que regirán la estrategia y ámbito de actuación de la Ciberseguridad dentro de Ferrovial.

Objeto

El objeto de la presente Política es establecer los principios fundamentales de Seguridad que aseguren en Ferrovial la salvaguarda de la integridad, la confidencialidad y la disponibilidad de su IT, de su OT, de su IoT y de la Información generada y utilizada en todos los procesos y operaciones de su negocio.

Alcance

La presente Política será de aplicación a Ferrovial, S.A. y a las sociedades mercantiles que comprenden su grupo consolidado y, en general, a toda entidad bajo su control directo o indirecto ("Ferrovial"). Se entiende que existe control cuando Ferrovial cuenta con la mayoría de los derechos de voto en el órgano de administración o dirección.
En la medida de lo posible, se promoverá en los órganos de decisión de aquellas entidades donde Ferrovial no tenga el control la aprobación del alineamiento de la práctica local de Seguridad con la presente Política.
Asimismo, esta Política podrá ser complementada y desarrollada por las diferentes normas, procedimientos y estándares de Seguridad que se vayan emitiendo para su implantación, los cuales deberán ser coherentes con los principios establecidos en la misma. Las normas de desarrollo adquirirán el mismo carácter vinculante y de obligado cumplimiento.
Cualquier vulneración de la presente Política o de las normas y procedimientos que la desarrollen podrá ser motivo de sanción por parte de Ferrovial y, en su caso, dar lugar a las acciones disciplinarias y/o judiciales que se estimen necesarias.

Aplicación de la Política

La presente Política Corporativa de Ciberseguridad tiene en cuenta las siguientes normas de referencia:

- NIST CSF (National Institute of Standards in Technology Cybersecurity Framework).
- ISO/IEC 27001 e ISO/IEC 27002.
- Esquema Nacional de Seguridad (ENS).
- Cloud Security Alliance (CSA).
- CIS Critical Security Controls (Center for Internet Security).

Estas normas determinan el marco tecnológico, organizacional y procedimental con el que desarrollar, implantar, controlar, revisar, mantener y mejorar el nivel de Seguridad de Ferrovial.

Todos los empleados, colaboradores y terceras partes cubiertos por el alcance de la presente Política y su normativa de desarrollo tienen la responsabilidad de asegurar que, tanto ellos como cualquier otra persona o entidad a su cargo, conocen, respetan y hacen respetar esta Política.

El Global CISO *(Chief Information Security Officer)* de Ferrovial, como responsable de alinear la estrategia de Seguridad con la visión y misión de Ferrovial, velará por la difusión, promoción y cumplimiento de la presente Política.

Esta Política ha sido aprobada por el Consejero Delegado de Ferrovial, S.A.

Misión de la Ciberseguridad

La Ciberseguridad y la Seguridad de la Información (la "Seguridad") en Ferrovial tienen por misión garantizar la confidencialidad, la integridad y la disponibilidad de su IT, de su OT, de su IoT y de la Información que se genera y utiliza en todos los procesos y operaciones que soportan sus actividades de negocio, de acuerdo con los siguientes principios y objetivos de Seguridad que sustentan y guían la estrategia de Seguridad de Ferrovial:

1. **Existencia de un entorno digital y tecnológico con el nivel de Seguridad necesario**: proporcionar el adecuado nivel de seguridad al entorno digital y tecnológico de Ferrovial, mediante la gestión de los riesgos inherentes a él.

2. **Garantizar el cumplimiento legal, regulatorio y contractual**: asegurar el cumplimiento de las leyes y normas de aplicación en Ferrovial, así como de los requisitos contractuales propios de la actividad de negocio.

3. **Gestionar adecuadamente los incidentes de seguridad y dotarse de resiliencia ante los mismos**: llevar a cabo una gestión correcta de los incidentes de seguridad que permita minimizar su impacto, así como disponer de los elementos necesarios que permitan la recuperación ante los mismos y la continuidad del negocio.

4. **Fomentar una adecuada cultura de Seguridad:** capacitar a todas las personas que diseñen, implementen y/o utilicen IT, OT, IoT e Información de Ferrovial para poder identificar y actuar ante amenazas y eventos de Seguridad que puedan tener lugar en el desempeño de sus actividades diarias.

5. **Armonizar la Seguridad entre las diferentes unidades de negocio y compañías filiales**: fomentar que todas las unidades de negocio desplieguen las medidas de seguridad adecuadas y proporcionales desde una perspectiva de gestión del riesgo.

6. **Facilitar la digitalización, la innovación y la adopción de nuevas tecnologías como soporte al negocio**: gestionar los riesgos asociados a la digitalización, la innovación y la adopción de nuevas tecnologías facilitando la creación de nuevos modelos de negocio basados en ellas.

7. **Facilitar oportunidades de negocio y procesos de licitación**: mediante la puesta en valor de los modelos, buenas prácticas y tecnologías de Seguridad desplegadas por Ferrovial como elemento diferenciador de sus competidores.

8. **Establecer colaboraciones estratégicas en materia de Seguridad**: implantar un conjunto de colaboraciones estratégicas que permitan incrementar el nivel de Seguridad de Ferrovial, en el ecosistema de la Seguridad, y en la sociedad en general.

Capacidades de Ciberseguridad

Los principios fundamentales anteriormente señalados se desarrollan a través de un conjunto de capacidades:

- **Identificación.** Capacidades relacionadas con (i) la identificación del contexto, procesos y servicios críticos de la organización, (ii) la identificación, clasificación y análisis de todos los activos relevantes para la organización, (iii) la identificación y tratamiento de los riesgos que pueden comprometerlos, y (iv) garantizar el cumplimiento legislativo, regulatorio y contractual, relativos al desarrollo de la actividad de negocio.

- **Protección.** Capacidades relacionadas con (i) la protección de los activos identificados conforme a su nivel de importancia para Ferrovial, (ii) el diseño y la construcción de productos y servicios digitales seguros, (iii) los mecanismos de control de acceso basados en la identidad y en la necesidad de saber y de usar, (iv) la protección de las comunicaciones internas y externas, (v) el control de las operaciones de los activos, (vi) de la cadena de suministro, (vii) de las claves criptográficas, (viii) fomentando una adecuada cultura en materia de Seguridad.

- **Detección.** Capacidades relacionadas con (i) la vigilancia de los productos y servicios digitales, (ii) de las comunicaciones, (iii) de la infraestructura tecnológica y (iv) de las instalaciones donde esté albergada, (v) para la detección y clasificación de ciber amenazas y eventos adversos, tanto internos como externos, que pueden impactar en los activos de Ferrovial.

- **Respuesta.** Capacidades relacionadas con (i) el establecimiento, gestión y pruebas de los planes de respuesta ante la materialización de ciber amenazas, y (ii) la comunicación con las partes interesadas, incluyendo aquellas exigidas por legislación, regulación o contrato.

- **Recuperación.** Capacidades relacionadas con (i) la resiliencia de los activos de Ferrovial para recuperarse del impacto de un evento adverso y volver a la situación normal, y (ii) identificar lecciones aprendidas que posteriormente se desplieguen para evitar la reproducción de dichos eventos.

Todas estas capacidades se implementarán mediante las adecuadas medidas de Seguridad basadas en estructura organizativa, procesos, tecnologías y personas, y el despliegue de un marco de actuación alineado con las mejores prácticas de mercado.

Riesgos de Ciberseguridad

Las capacidades anteriormente señaladas deberán desarrollarse para asegurar la adecuada gestión de los siguientes riesgos de ciberseguridad con impacto en la actividad de negocio de Ferrovial:

Categoría **Ciberamenazas**: riesgos asociados a los agentes de amenaza existentes en el ciberespacio (como mafias, crimen organizado, agentes-estado malintencionados, hacktivistas, *insiders*...), que pueden comprometer la seguridad y la normal operación de los Activos IT, OT e IoT y la Información de Ferrovial a través de ciberataques de diversa índole.

1. **Robo y suplantación de la identidad digital**: riesgo de sufrir el robo de una identidad digital para la posterior explotación ilícita de la misma, incluyendo acceso a información confidencial, profesional y personal, chantajes, fraude a terceros, etc.

2. **Disrupción y secuestro del activo**: riesgo de que un activo de Ferrovial sufra un ciberataque con el propósito de provocar una disrupción significativa en su operación o la imposibilite porque el activo haya sido secuestrado. Se incluyen los ataques de Denegación de Servicio Distribuida (DDoS), dirigidos a saturar la capacidad de un activo, provocando una degradación crítica en su funcionamiento u operación.

3. **Brecha, fuga, revelación y secuestro de información**: riesgo de que información de Ferrovial sea revelada, sustraída o secuestrada de forma no autorizada o sin conocimiento de la organización, bien de forma intencionada o bien de manera accidental. La fuga, revelación o secuestro de información podría llevar asociado, adicionalmente, el incumplimiento de los marcos regulatorios de aplicación y estar sujeto a sanciones.

4. ***Insiders:*** riesgo de sufrir ataques de diferente naturaleza (robo o fuga de información, suplantación de identidad, denegación/disrupción del servicio, despliegue de *malware*...) realizados por un empleado o colaborador, actual o antiguo, que dispone o dispuso de acceso legítimo a los activos de la organización y que puede, de forma intencionada o no intencionada, abusar de dichos accesos.

5. **Ciber espionaje**: riesgo de sufrir el robo de secretos, de propiedad intelectual/industrial o de información sensible para Ferrovial por parte de agentes-estado malintencionados, competidores u otros agentes de amenaza.

6. **Control y compromiso en la cadena de suministro**: riesgo de sufrir el compromiso de activos de Ferrovial (robo o fuga de información, indisponibilidad/disrupción de activos, fraude, extorsión...) motivado por la inadecuada acreditación y supervisión de los servicios prestados por socios y/o terceros, cuya seguridad podría haberse comprometido previamente.

7. **Fraude**: riesgo de sufrir una pérdida económica o de oportunidad de negocio asociada a técnicas de engaño utilizando medios digitales. Se incluye la suplantación de la identidad de empleados y colaboradores de Ferrovial o de los interlocutores de una transacción financiera en procesos de negocio.

8. **Extorsión**: riesgo de que Ferrovial sufra presiones a partir de la materialización de ciberamenazas (disrupción de negocio por secuestro de activos, divulgación de información confidencial...) con objeto de obtener un beneficio económico o de cualquier otra naturaleza.

9. **Robo y extravío de activos**: riesgo de que activos de Ferrovial sean sustraídos por parte de agentes malintencionados o ser extraviados por sus empleados y/o colaboradores. Dentro de esta categoría

se incluyen elementos tales como ordenadores, smartphones, tablets, y dispositivos de almacenamiento masivo, así como otros elementos propios de entornos industriales.

10. **Inadecuada cultura de seguridad**: riesgo asociado a (i) la materialización de amenazas de seguridad basadas en técnicas de ingeniería social (*phishing, vishing, smishing*...) y/o en la explotación de vulnerabilidades, y (ii) la incapacidad de reconocer y notificar cualquier amenaza de seguridad que pueda tener lugar en la organización (*malware*, suplantación, fraude...) por falta de cultura, concienciación y/o capacitación en materia de Seguridad.

Categoría **Continuidad de Negocio**: riesgos asociados a una inadecuada definición, implementación y mantenimiento de planes de continuidad del negocio y de recuperación para todos los procesos críticos de Ferrovial, así como a la prueba y la mejora continua de éstos.

11. **Inadecuada preparación de la continuidad**: riesgo de (i) no disponer de modelos que permitan identificar los procesos críticos para la organización y los tiempos, personas, recursos y otros requisitos de recuperación y operación necesarios ante una situación de contingencia grave. Incluye también el riesgo de (ii) no disponer de los planes que permitan la gestión de la crisis, (iii) la recuperación de los procesos críticos, (iv) su operación durante la contingencia y (v) la vuelta a la normalidad, una vez que la contingencia ha concluido.

12. **Inadecuada gestión de las contingencias**: riesgo de que (i) los planes definidos ante contingencias no sean efectivos, bien por su inadecuado diseño, bien por la no preparación de las personas que los tienen que llevar a cabo. Este riesgo incluye también la (ii) no realización de pruebas y (iii) la no incorporación de cambios, modificaciones y mejoras dentro de los procesos como consecuencia de las revisiones y pruebas realizadas.

Categoría **Legislación y Cumplimiento**: riesgos asociados al incumplimiento de leyes, regulaciones y acuerdos contractuales en materia de Seguridad y privacidad a los que Ferrovial, en el desarrollo de su actividad de negocio, deba dar el debido cumplimiento.

13. **Inadecuada identificación de requisitos y obligaciones en materia de Seguridad y/o privacidad**: riesgo de no identificar las leyes, regulaciones y compromisos, y requisitos asociados, de aplicación para Ferrovial en el desarrollo de su actividad de negocio.

14. **Inadecuado cumplimiento de regulaciones en materia de Seguridad y/o privacidad**: riesgo de recibir sanciones y de perder oportunidades de negocio por incumplir o no cumplir de forma adecuada con los requisitos, en materia de Seguridad y/o privacidad, derivados de leyes y regulaciones de aplicación. Incluye también el incumplimiento de leyes y regulaciones focalizadas específicamente en Seguridad.

15. **Inadecuado cumplimiento de compromisos contractuales en materia de Seguridad**: riesgo de sufrir consecuencias negativas (penalización, sanción, extinción contractual...) por incumplimiento contractual en materia de Seguridad en el contexto del ciclo de vida (construcción, mantenimiento y operación) de un activo / contrato gestionado por Ferrovial.

Organización y Liderazgo de Ciberseguridad

La Dirección de Ciberseguridad de Ferrovial será la encargada de liderar el despliegue de la presente Política en las diferentes unidades de negocio y compañías filiales. En este sentido, se ha establecido un modelo formalizado de roles, responsabilidades y organización en materia de Seguridad que especifica:

- Cuáles son los roles en materia de Seguridad en Ferrovial y en sus unidades de negocio y compañías filiales.
- Cuáles son los Órganos de gobierno de la Seguridad en Ferrovial.
- Qué actividades tienen encomendadas cada uno de los roles de seguridad dentro de su ámbito de competencia.
- Cómo se relacionan las diferentes unidades de negocio y compañías filiales en materia de Seguridad.
- Qué nivel de exigencia en materia de Seguridad deberán alcanzar las diferentes unidades de negocio y compañías filiales.
- Cómo se establece el nivel de exigencia en materia de Seguridad.
- Qué información se debe reportar en materia de Seguridad, a qué Órganos de gobierno de Ferrovial y a qué Órganos de gobierno de Seguridad.

Difusión

La Dirección de Ciberseguridad difundirá la presente Política, a través de los medios que considere apropiados, a todas las partes interesadas en materia de Seguridad, tanto internas como externas.

Aprobación Y Vigencia

La Política Corporativa de Ciberseguridad ha sido aprobada por el Consejero Delegado de Ferrovial y será de aplicación a partir del día de su publicación en la intranet de Ferrovial.