Específico de la entidad

CIBERSEGURIDAD Y TRATAMIENTO DE DATOS

SBM-3 - IMPACTOS, RIESGOS Y OPORTUNIDADES MATERIALES Y SU INTERACCIÓN CON LA ESTRATEGIA Y EL MODELO DE NEGOCIO

Específico de la entidad	Fase de la cadena de valor*	Descripción	Probabilidad de ocurrencia	Horizontes temporales
Ciberseguridad				
(+) Impacto	OP, S	Prevención y/o mitigación de incidentes que puedan afectar a la integridad de las infraestructuras gestionadas por la Compañía, así como a la integridad y privacidad de las personas, y/o al medioambiente.	Actual	C
(+) Impacto	CV	Mejora de la cultura de ciberseguridad entre las partes interesadas de la empresa.	Actual	C
(-) Impacto	CV	Materialización de incidentes que puedan impactar en la integridad de las infraestructuras gestionadas por la Compañía, a la integridad y privacidad de las personas y/o al medio ambiente.	Actual	C
Riesgo	CV	Ciberataques sofisticados que afectan a las operaciones, productividad, información, propiedad intelectual o imagen/reputación de la Compañía, así como a la integridad de las personas.		C
Riesgo	CV	Multas y sanciones severas por incumplimiento de la normativa y de los marcos de control de la aplicación.		C
Oportunidad	CV	La seguridad como motor del negocio, reforzando la ventaja competitiva de la empresa mediante prácticas de seguridad avanzadas y altos niveles de cumplimiento.		C
Oportunidad	CV	Mejora del gobierno corporativo y de la confianza en la Compañía.		C

** OP: Operaciones propias; CV: Cadena de valor; Com: Compras; Cl: Clientes; S: Socios; C: Corto plazo; M: Medio plazo; L: Largo plazo*

MDR-P: POLÍTICAS

Ferrovial cuenta con una Política Corporativa de Ciberseguridad aprobada por el Consejero Delegado en 2022, que se aplica a todas las divisiones y filiales y que puede consultarse en la página web de la compañía. Sus principios y objetivos se encuentran en consonancia con la estrategia empresarial. Se implementa mediante Políticas de Seguridad que engloban organización, personas, procesos y tecnologías, formalizadas en un conjunto de Principios de Seguridad basados en las mejores prácticas del sector, destacando el NIST CSF y la norma ISO 27001, bajo la que Ferrovial está certificada desde 2012.

Política	Política de Ciberseguridad
Descripción	La presente Política define los principios y directrices para salvaguardar la información, los sistemas y las operaciones de Ferrovial frente a las ciberamenazas, garantizando la confidencialidad, integridad y disponibilidad de los activos digitales. Respalda el compromiso de la organización con la continuidad del negocio y la gestión segura de los datos.
Objetivo	La política pretende: • Garantizar un entorno digital y tecnológico con el nivel de Seguridad necesario. • Garantizar el cumplimiento legal, regulatorio y contractual. • Garantizar la resistencia operativa frente a los ciberataques. • Fomentar una cultura de concienciación y responsabilidad en ciberseguridad entre empleados, proveedores y socios.
Impactos, riesgos y oportunidades materiales asociados	• Impactos materiales: Pérdidas financieras potenciales, daños a la reputación, incumplimiento legal, regulatorio y contractual, e interrupciones debidas a incidentes cibernéticos. • Riesgos: Ataques cibernéticos sofisticados que afectan las operaciones, la productividad, la información, la propiedad intelectual o la imagen/reputación de la Compañía, así como la integridad de las personas. Multas y sanciones severas por incumplimiento de la normativa y de los marcos de control de la aplicación. • Oportunidades: Fomentar la confianza de las partes interesadas mediante prácticas sólidas de ciberseguridad, aprovechar la innovación para obtener ventajas competitivas y cumplir con los estándares regulatorios globales para reforzar el posicionamiento en el mercado.

Proceso de seguimiento y corrección	Ferrovial garantiza la aplicación y el cumplimiento de la Política de Ciberseguridad mediante revisiones periódicas de los riesgos y controles que abarcan todas las unidades de negocio y los activos participados. Esta información se comunica periódicamente a los Órganos de Gobierno de la Compañía que supervisan el estado de la Ciberseguridad.

Ámbito de la política	
Partes interesadas	Todos los empleados, proveedores y clientes de Ferrovial con acceso a sistemas o datos de la Compañía.
Áreas geográficas	Global
Aplicación en la cadena de valor	La política se extiende a toda la cadena de valor, incluidos los proveedores y clientes, garantizando prácticas seguras en todas las interacciones comerciales. La ciberseguridad es una práctica que respalda los activos digitales que, en última instancia, apoyan las actividades empresariales.
Exclusiones a la aplicación	Actualmente no hay exclusiones; la política se aplica a todas las áreas de actividad, geografías y partes interesadas a nivel mundial.
Flujo de aprobación de la política	
Parte responsable	Consejero Delegado (CEO): responsable de aprobar y aplicar la política
Otras cuestiones que comunicar (si procede)	
Coherencia con instrumentos o normas de terceros	La política cumple: • Normas internacionales, incluida la ISO 27001 • Normativas europeas como el RGPD • El Esquema Nacional de Seguridad (ENS) • Políticas de Responsabilidad Corporativa y Sostenibilidad de Ferrovial
Compromiso de las partes interesadas	La política incorpora los comentarios de las principales partes interesadas para abordar de manera eficaz los problemas de ciberseguridad y garantizar una colaboración segura en toda la organización.
Cómo se proporciona	Esta política está disponible en la página web de Ferrovial (ferrovial.com) y en la intranet.
Cambios importantes en la política	N/A – no se han realizado cambios.

"Impactos, riesgos y oportunidades materiales asociados" es un concepto relacionado con el NEIS y la doble materialidad. NO está relacionado con la materialidad de los incidentes cibernéticos considerados por la SEC.

MDR-A: ACTUACIONES

EL MODELO DE DETECCIÓN, CORRELACIÓN Y CIBERINTELIGENCIA DE AMENAZAS

La Compañía cuenta con capacidades de SOC *(Centro de Operaciones de Seguridad)* para proteger sus centros de datos, perímetros, puntos finales y entornos en la nube. Este servicio responde a las alertas generadas por las herramientas SIEM *(Security Information and Event Management)* y detecta eventos de acuerdo con los casos de uso definidos por la Dirección de Ciberseguridad de Ferrovial.

Actualmente existe una plataforma SOAR *(Security Orchestration Automation and Response)* que permite la integración y el funcionamiento coordinados de diversas herramientas de prevención y protección, facilitando la detección y respuesta automatizadas, así como la orquestación de actividades para la contención, resolución y neutralización de amenazas.

La organización integra capacidades avanzadas de ciberseguridad para la protección frente a amenazas y la detección de compromisos relacionados con la información, como accesos no autorizados, transmisión anómala de grandes volúmenes de datos y exfiltración, ya sea a través del almacenamiento físico o de servicios en la nube.

Las capacidades de ciberinteligencia amplían los procesos de detección de amenazas y mejoran las capacidades de respuesta mediante la identificación de Indicadores de Compromiso (IoC) y Tácticas, Técnicas y Procedimientos (TTP) utilizados por los ciberdelincuentes para llevar a cabo sus ataques. También se llevan a cabo ejercicios de caza de amenazas para identificar compromisos potenciales que no se hayan detectado previamente.

Por último, la Compañía intercambia información sobre amenazas y gestiona incidentes en coordinación con organismos nacionales e internacionales de ciberseguridad cuando procede.

RESPUESTA A LOS CIBERATAQUES

La Compañía cuenta con un CSIRT *(Computer Security Incident Response Team)* que responde a los eventos detectados por el SOC (Security Operations Center) que pueden convertirse en incidentes de seguridad. Este equipo cuenta con capacidades DFIR *(Digital Forensics and Incident Response)* para analizar, contener, mitigar y prevenir este tipo de sucesos. La identificación periódica de IoC*(Indicadores de Compromiso)* y TTP*(Tácticas, Técnicas y Procedimientos)* es clave para mejorar los mecanismos de protección y detección y la respuesta del SOC, tanto manual como automatizada.

Asimismo, Ferrovial cuenta con herramientas de postura de ciberseguridad que permiten evaluar en tiempo real el cumplimiento de parámetros y controles de seguridad específicos, de la infraestructura TI gestionada (en centros de datos y entornos *cloud*) y de los *endpoints*. Esto proporciona una visión global de los riesgos y controles relacionados con las recomendaciones de seguridad emitidas por los fabricantes, las normas del mercado y los marcos de seguridad, además de permitir el desarrollo de planes de acción para mejorar la postura.

Las capacidades y procesos descritos anteriormente están impulsados por la inteligencia artificial generativa, tanto con fines de optimización como para contrarrestar las nuevas técnicas aplicadas por los ciberdelincuentes, que también se basan en estas tecnologías.

Ferrovial dispone de un protocolo de respuesta ante incidentes basado en las mejores prácticas del mercado (Guía INCIBE-CERT, ISO/IEC 27035 y NIST). Además, se ha implantado un procedimiento global para la identificación y comunicación de ciberincidentes materiales a los organismos reguladores (SEC, agencias nacionales e internacionales de ciberseguridad, AEPD, entre otros). La comunicación con reguladores, autoridades, clientes y otros grupos de interés, a través de mecanismos en plazos concretos, es uno de los elementos clave para que Ferrovial garantice la transparencia y la debida diligencia.

Las capacidades de detección y respuesta se evalúan sistemáticamente mediante *simulaciones de Breach & Attack y Pentesting*, utilizando tecnologías disponibles en el mercado (Cymulate y Pentera, respectivamente).

Es importante destacar que, durante 2025, no se produjeron brechas materiales de ciberseguridad en los sistemas de información de Ferrovial. El CSIRT y el equipo de Ciberseguridad de Ferrovial gestionaron aproximadamente 3.165 incidentes.

RESILIENCIA Y CIBERRESILIENCIA

La Compañía ha establecido Planes de Contingencia y Planes de Recuperación para responder y recuperarse de acontecimientos perturbadores. Ferrovial está invirtiendo actualmente en la evolución del modelo de Continuidad, con el objetivo de adoptar un enfoque más global para estandarizar las prácticas en todas las divisiones de negocio de la Compañía.

Estos Planes de Contingencia cubren los escenarios de crisis desencadenados por las ciberamenazas. Existe un Comité de Crisis Cibernética encargado de gestionar este tipo de incidentes. Asimismo, Ferrovial dispone de un procedimiento para comunicar incidentes a los reguladores y otras partes interesadas en este ámbito.

Ferrovial, consciente de la importancia de la resiliencia en su cadena de suministro, incorpora la verificación de los planes de contingencia y recuperación en el proceso de *Gestión de Riesgos de Proveedores (VRM*), en el contexto del servicio prestado a la Compañía.

El modelo de continuidad de la actividad establece la necesidad de realizar pruebas periódicas de los planes, por lo que a lo largo del año se han llevado a cabo pruebas del Table-Top y del Plan de Recuperación de Desastres. Los resultados han sido globalmente positivos y se han identificado oportunidades de mejora, que se están aplicando actualmente.

La Compañía mantiene una póliza de seguro cibernético, habiendo ampliado los límites y tipos de cobertura para eventos disruptivos e incidentes cibernéticos que puedan ocurrir en el contexto de las actividades llevadas a cabo por Ferrovial, sus unidades de negocio y filiales; estos incluyen cobertura financiera, respuesta a incidentes y asesoramiento legal. Cabe señalar que en 2025 no fue necesario activar esta política, ya que no se produjeron incidentes cibernéticos importantes.

GESTIÓN DE RIESGOS DE TERCEROS

El programa Vendor Risk Management (VRM) de Ferrovial define los requisitos de seguridad que deben cumplir terceros, en función del tipo de servicio que prestan a la Compañía y del nivel de acceso que tienen a su información y activos digitales.

En 2025, se ha automatizado y sistematizado el proceso de alta *de* proveedores, y actualmente se están llevando a cabo procesos de automatización y sistematización del *seguimiento* de los proveedores que prestan servicios recurrentes a Ferrovial.

El proceso VRM evalúa las acreditaciones, certificaciones, cualificaciones y pruebas que atestiguan el nivel de cumplimiento en materia de seguridad del producto o servicio pertinente proporcionado por el vendedor, así como el nivel de madurez en materia de seguridad que el vendedor puede demostrar. Si se detectan riesgos importantes durante los procesos de revisión, se toman las medidas oportunas, incluida la rescisión del contrato.

La gestión de riesgos de terceros garantiza que los incidentes cibernéticos que puedan afectar a Ferrovial se notifiquen a tiempo y que existan planes de respuesta y recuperación en caso necesario.

VERIFICACIÓN EXTERNA Y ANÁLISIS DE VULNERABILIDAD

Como parte del proceso de mejora continua de Ferrovial, es fundamental la realización de auditorías tanto internas como externas para identificar vulnerabilidades y áreas de mejora, cuya implantación reforzará la ciberseguridad y contribuirá a mitigar los riesgos.

A continuación se detallan las revisiones y auditorías que se llevan a cabo de forma recurrente en la organización:

- Auditorías internas y de terceros basadas en la certificación ISO 27001.
- Auditorías SOX integradas:
  - Controles ITGC.
  - Controles del modelo de ciberseguridad.
- Auditoría externa realizada por SWIFT (*Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales*).
- Auditorías realizadas por Auditoría Interna (tercera línea de defensa) de acuerdo con su plan anual (dos o tres auditorías anuales).
- Cuestionarios, aprobaciones de seguridad requeridas por los clientes de Ferrovial.
- Índice Dow Jones Best-in-Class.
- Informe de Sostenibilidad ESG (doble materialidad).
- Revisiones de seguridad ad hoc de acuerdo con la planificación anual
- *Breach & attack*, y *pentesting* recurrente basado en las herramientas Cymulate y Pentera, según planificación anual.

- Revisión de la caza de amenazas y evaluación de compromisos para identificar posibles compromisos/infracciones no detectados por los sistemas de supervisión
- Revisión de vulnerabilidades en centros de datos, *endpoints*, perímetros y entornos en nube, así como en entornos industriales
- Revisión de vulnerabilidades en el código fuente.
- Revisión del rating de ciberseguridad de Ferrovial a través de *BitSight*.
- Revisiones de los riesgos de seguridad de los proveedores *(gestión de riesgos de proveedores)*.
- Simulacros de crisis *(ejercicios de mesa)*.
- Gestión de la postura mediante herramientas de ciberseguridad (*Microsoft Compliance y Wiz*).

El Departamento de Ciberseguridad consolida, asigna, planifica y supervisa la aplicación de los distintos planes de acción derivados de las evaluaciones, revisiones y auditorías realizadas.

El proceso de revisión por la dirección se lleva a cabo formalmente con carácter anual, siendo uno de sus objetivos la revisión del nivel de consecución correspondiente a las acciones de ciberseguridad previstas. Este proceso está supervisado por el CISO Global, teniendo en cuenta una serie de datos, como los KGI y los KPI, los resultados de los procesos de auditoría y revisión, y el seguimiento de los planes de tratamiento de riesgos.

MDR-T: METAS

Los objetivos definidos en la Política Corporativa de Ciberseguridad se miden mediante Indicadores de Objetivos Clave (KGI) definidos en el Sistema de Gestión de la Seguridad de la Información (SGSI), que se basa en la norma ISO 27001, auditada anualmente por BSI. Esto permite supervisar la eficacia de la aplicación de la Política. Los indicadores se basan en mediciones de las capacidades organizativas, tecnológicas y de procesos relacionadas con la ciberseguridad, asociadas a cada uno de los Objetivos Estratégicos establecidos en la Política.

Algunos de los principales objetivos son

- Garantizar un entorno digital y tecnológico con el nivel de Seguridad necesario.
- Garantizar el cumplimiento legal, regulatorio y contractual.
- Gestionar adecuadamente los incidentes de seguridad y reforzar la capacidad de reacción ante ellos.
- Fomentar una cultura de seguridad adecuada.
- Armonizar la seguridad en las distintas unidades de negocio y filiales.
- Facilitar la digitalización, la innovación y la adopción de nuevas tecnologías para apoyar el negocio.
- Facilitar oportunidades de negocio y procesos de licitación.
- Establecimiento de asociaciones estratégicas en el ámbito de la seguridad.
- Fomentar una cultura de concienciación y responsabilidad en ciberseguridad entre empleados, proveedores y socios.

MDR-M: MÉTRICAS

100% de incidentes de seguridad gestionados con éxito	193.592 correos electrónicos de simulación de *phishing* recibidos anualmente por los empleados	11.431 usuarios únicos incluidos anualmente en simulaciones de *phishing*
61.538 correos electrónicos de *phishing* bloqueados al mes por los sistemas de la compañía	14.991 intentos de acceso a recursos corporativos bloqueados (fuente maliciosa/no fiable) al mes	9,3 ataques de *ransomware* detectados y bloqueados automáticamente al mes

Incidentes de seguridad

En 2025, el 100% de los incidentes de seguridad se gestionaron con éxito. El objetivo de este indicador es verificar que los incidentes de seguridad que se producen en Ferrovial se gestionan de la mejor manera posible para mitigar su potencial impacto. Solo se incluyen en esta revisión los incidentes gestionados por el Departamento de Ciberseguridad, que abarcan todas las divisiones de negocio que utilizan Productos y Servicios Digitales Corporativos. El criterio de medición es la proporción de incidentes gestionados correctamente frente al número total de incidentes registrados en el periodo de referencia, basándose en el tiempo de respuesta, las medidas adoptadas, el seguimiento y la recopilación de pruebas, la resolución, el análisis de la causa raíz proporcional al tipo de incidente y las lecciones aprendidas. Los datos proporcionados corresponden a la media anual, calculada a partir de todas las mediciones mensuales recogidas durante el año comprendido entre enero de 2025 y diciembre de 2025. Este control forma parte del marco de ciberseguridad SOX y es revisado por el auditor externo PwC.

Correos electrónicos de simulación de phishing recibidos por los empleados

En 2025, los empleados recibieron un total de 193.592 correos electrónicos de simulación de *phishing*, en el marco de una formación periódica y sistemática destinada a reforzar la capacidad de los usuarios para identificar posibles amenazas. Esta métrica se basa en el número de correos electrónicos emitidos a través de la plataforma de concienciación durante campañas de *phishing* simuladas, limitadas a usuarios gestionados por el Departamento de Ciberseguridad Corporativa, que abarcan de enero a diciembre de 2025. El KPI está integrado en el Sistema de Gestión de la Seguridad de la Información (SGSI) y es auditado externamente por BSI en el marco de la certificación ISO 27001, lo que garantiza la solidez y trazabilidad del proceso.

Usuarios incluidos en simulaciones de *phishing*

A lo largo de 2025, 11.431 usuarios únicos participaron en simulaciones de *phishing*. El indicador refleja el número de usuarios únicos registrados en la plataforma de concienciación e implicados en simulaciones de *phishing*. Se aplica exclusivamente a los usuarios gestionados por el Departamento de

Ciberseguridad Corporativa y utiliza el número de usuarios únicos registrados en la plataforma KnowBe4. Este KPI forma parte del SGSI, y se somete a la auditoría externa (BSI) requerida para la certificación ISO 27001.

Correos electrónicos de *phishing* bloqueados

Los sistemas de la empresa bloquearon una media de 61.538 correos electrónicos de *phishing* al mes, a lo largo de 2025, lo que demuestra la eficacia y calidad de las capacidades de filtrado de la plataforma MS Defender. La métrica se calcula a partir del número total de mensajes de *phishing*, *malware*, correos electrónicos bloqueados por suplantación de identidad y mensajes bloqueados por políticas, excluyendo el spam. Se aplica únicamente a los usuarios dependientes del Departamento de Ciberseguridad Corporativa, y refleja una media anual de las mediciones mensuales recopiladas entre enero y diciembre de 2025. El KPI se incorpora al Sistema de Gestión de la Seguridad de la Información (ISMS) y está sujeto a una auditoría externa por parte de BSI en virtud de la certificación ISO 27001, lo que garantiza una supervisión y verificación rigurosas.

Intentos bloqueados de acceder a recursos corporativos

En 2025, la empresa bloqueó una media de 14.991 intentos al mes de acceder a recursos corporativos desde fuentes maliciosas o no fiables, lo que demuestra la eficacia y calidad del filtrado de comunicaciones realizado por la plataforma MS Defender. Este indicador se basa en el número de dominios maliciosos, IPs y URLs bloqueadas, y cubre a los usuarios gestionados por el Departamento de Ciberseguridad Corporativa, siguiendo la media anual calculada a partir de todas las mediciones mensuales recogidas entre enero y diciembre de 2025. El KPI forma parte del Sistema de Gestión de Seguridad de la Información (ISMS) y es auditado externamente por BSI bajo la certificación ISO 27001, garantizando una supervisión y verificación rigurosas.

Ataques de *ransomware* detectados y bloqueados automáticamente

En 2025, se detectó y bloqueó automáticamente una media anual de 9,3 ataques de *ransomware* al mes. Este indicador mide la eficacia de las capacidades de detección y protección frente al *ransomware*, tras la exclusión (manual) de posibles falsos positivos y abarca únicamente a los usuarios gestionados por el Departamento de Ciberseguridad Corporativa, utilizando el criterio de medición de Microsoft Defender (XDR), tras filtrar manualmente los posibles falsos positivos. Este KPI está incluido en el SGSI, y sujeto a la auditoría externa (BSI) requerida para la certificación ISO 27001.

INNOVACIÓN, DIGITALIZACIÓN Y TECNOLOGÍA APLICADAS A LA ACTIVIDAD

SBM-3 - IMPACTOS, RIESGOS Y OPORTUNIDADES MATERIALES Y SU INTERACCIÓN CON LA ESTRATEGIA Y EL MODELO DE NEGOCIO

La rápida evolución de las tecnologías digitales genera impactos materiales que transforman el modelo de negocio de Ferrovial, creando tanto riesgos como oportunidades estratégicas. La digitalización transversal y la adopción acelerada de tecnologías emergentes mejoran la eficiencia, la competitividad y la resiliencia operativa, pero también aumentan la exposición a las ciberamenazas, los riesgos para la privacidad, la obsolescencia tecnológica y la presión normativa. Estos factores requieren una inversión continua en capacidades digitales y una sólida gobernanza para garantizar la sostenibilidad de los cambios.

La estrategia ReadIT 2027 se implementa como respuesta a este entorno integrando innovación, resiliencia y creación de valor en un marco directamente aplicado a los objetivos empresariales. Entre los impactos más relevantes destacan la transformación de procesos y plataformas, la migración a la nube y la adopción de inteligencia artificial, reduciendo los tiempos, optimizando costes y posibilitando nuevos modelos de negocio basados en datos. Sin embargo, estos avances conllevan riesgos críticos: vulnerabilidades de ciberseguridad que pueden comprometer los activos y la reputación, posible incumplimiento de la normativa en entornos cada vez más exigentes y reticencias culturales que limitan la adopción y reducen el rendimiento de la inversión (ROI).

Frente a estos riesgos, surgen oportunidades materiales que refuerzan la posición competitiva de Ferrovial: la automatización de tareas y flujos de trabajo, la creación de productos digitales escalables, la colaboración con startups en los campos de la robótica, los gemelos digitales y la realidad virtual, así como la explotación de analítica avanzada para la toma de decisiones basadas en datos. La interacción entre estos elementos se estructura a través de iniciativas que garantizan la resiliencia operativa -como la mejora de la postura de ciberseguridad, la supervisión de la obsolescencia y la automatización de los controles SOX- al tiempo que promueven la innovación abierta y la experimentación tecnológica en casos de uso reales.

Además, la inversión en iniciativas de inteligencia artificial y el marco de gobernanza asociado reflejan el compromiso de Ferrovial con una integración sostenible y estructurada de la IA en los procesos y plataformas, reduciendo los riesgos asociados a la adopción acelerada y garantizando impactos positivos a largo plazo. Esta estrategia no solo mitiga las amenazas, sino que convierte la transformación digital en un motor de eficiencia, competitividad y diversificación, alineando cada iniciativa con los objetivos y metas corporativas definidas para 2027.

Ferrovial asume que la innovación tecnológica debe venir acompañada de responsabilidad, transparencia y alineación con los valores corporativos. Por ello, ha definido un marco de gobernanza y principios éticos que guía el desarrollo y la aplicación de soluciones de IA en todas las áreas de negocio. Este marco se articula en torno a cinco pilares básicos:

1. **Transparencia y explicabilidad**

   Cada modelo debe ser comprensible y auditable, garantizando que las decisiones automatizadas puedan explicarse a los equipos internos y a las partes interesadas. Este aspecto refuerza la confianza y la responsabilidad.

2. **Supervisión humana en decisiones críticas**

   El principio de "human in the loop" se aplica para garantizar que la IA actúa como herramienta de apoyo, no como sustituto del juicio profesional, especialmente en procesos delicados.

3. **Protección de datos y privacidad**

   Todas las soluciones cumplen el GDPR y la normativa aplicable, incorporando técnicas de anonimización y cifrado para salvaguardar la información de clientes, empleados y socios.

4. **Equidad y mitigación de prejuicios**

   Se establecen procesos de validación continua para detectar y corregir sesgos en datos y algoritmos, evitando impactos discriminatorios y garantizando resultados justos.

5. **Alineación de sostenibilidad y ESG**

   La IA se evalúa no solo por su impacto económico, sino también por su contribución a los objetivos de sostenibilidad y responsabilidad social, en línea con los compromisos ESG de Ferrovial.

Para facilitar una adopción segura, la empresa ha desarrollado manuales internos y programas de formación que incluyen recomendaciones prácticas para el uso de herramientas como Microsoft Copilot y otras soluciones generativas. Estos recursos están disponibles en el portal de IA en MyForum, que centraliza documentos, casos de uso y comunidades de práctica para impulsar una cultura de responsabilidad digital.

Ferrovial también ha creado comités de revisión y métricas de impacto ético que supervisan la coherencia entre la innovación tecnológica y los valores corporativos. Este planteamiento se complementa con la observación de marcos normativos internacionales, como el Reglamento europeo sobre IA, para anticiparse a los requisitos y garantizar el cumplimiento de la normativa.

En resumen, la IA no solo se concibe como motor de eficiencia y competitividad, sino también como catalizador de la confianza, la sostenibilidad y el valor social, garantizando que cada avance tecnológico refuerce la reputación y el propósito corporativos.

Específico de la entidad	Fase de la cadena de valor*	Descripción	Probabilidad de ocurrencia	Horizontes temporales
Innovación, digitalización y tecnología aplicadas a la actividad				
(+) Impacto	OP, S	Promoción de una cultura innovadora y digital que fomente la mejora continua del Grupo y genere un entorno de trabajo más agradable.	Actual	C
(+) Impacto	OP, S	Fomento de la innovación y la digitalización para mejorar la seguridad en los proyectos, reduciendo los accidentes y los riesgos para los trabajadores.	Actual	C
(+) Impacto	OP, S	Generación de innovación en la sociedad a través de la creación de centros de investigación mediante el desarrollo de colaboraciones y alianzas.	Actual	C
(+) Impacto	OP, S	Mejora del impacto ambiental de los proyectos de la compañía (eficiencia energética, reducción de emisiones, etc.) como resultado de la implantación de nuevas tecnologías en el proceso del producto y de herramientas de gestión digital que ayudan a cuantificar su impacto.	Actual	C
(-) Impacto	OP, S	Cuestiones relacionadas con el mantenimiento y la sustitución de maquinaria adaptada a las nuevas tecnologías.	Actual	C
(-) Impacto	OP	Impacto en las funciones de los empleados y en la progresión profesional en el contexto de la evolución de las competencias y los requisitos de la transformación digital.	Actual	C
(-) Impacto	OP	Desplazamiento de la mano de obra y transformación de funciones como consecuencia de la automatización y la adopción de nuevas tecnologías.	Actual	C
Riesgo	OP, S	Vulnerabilidad en las operaciones debido a interrupciones del servicio derivadas de la exposición a catástrofes naturales.		C
Riesgo	OP, S	Posibles multas y pérdida de reputación por incumplimiento de la normativa en materia de IA.		M
Oportunidad	OP, S	Implantación de nuevas tecnologías que generen una cartera de activos más resistente.		M
Oportunidad	OP, S	Identificación de nuevos negocios a partir de la evaluación de nuevas tecnologías de bajas emisiones (plantas fotovoltaicas, SMR nucleares, energía eólica marina, etc.).		M

** OP: Operaciones propias; CV: Cadena de valor; Com: Compras; Cl: Clientes; S: Socios; C: Corto plazo; M: Medio plazo; L: Largo plazo*

MDR-P: POLÍTICAS

Ferrovial gestiona los programas e iniciativas de innovación a través de una política estructurada, transversal y alineada con la visión de futuro de la compañía. Esta política, liderada por la alta dirección, se extiende a todas las áreas y empleados de Ferrovial, y es implementada por un equipo especializado que gestiona áreas clave como la innovación abierta, el crecimiento, la gestión de activos, la sostenibilidad y el desarrollo de nuevos modelos de negocio. Cada una de estas áreas está organizada en programas transversales y supervisada por gestores de proyectos.

La Política de Innovación de Ferrovial sitúa a la innovación como motor fundamental para anticipar y liderar la transformación del sector, generando valor sostenible y diferenciador tanto para la compañía como para la sociedad en su conjunto. La política se basa en principios como una mentalidad transformadora, la integración de capacidades digitales y tecnologías avanzadas, la colaboración abierta con agentes internos y externos, la excelencia operativa y una fuerte orientación hacia la sostenibilidad y el compromiso social. También garantiza que las prácticas de innovación evolucionen en consonancia con los marcos normativos emergentes, como la Ley de Inteligencia Artificial de la UE, incorporando principios de diseño responsable y orientaciones internas para apoyar el desarrollo ético, seguro y conforme de tecnologías avanzadas.

La Política de Innovación actualmente es transversal y se aplica en todas las líneas de negocio de Ferrovial. Ferrovial ha formalizado una Política de Innovación global que refleja todos los esfuerzos ya en marcha en el campo de la innovación, y que se revisa periódicamente para asegurar su alineación con los retos medioambientales y las tendencias del sector.

La **Política de Innovación** tiene por objeto:

- Promover la identificación y desarrollo de oportunidades de innovación en todas las áreas de Ferrovial, anticipándose a las tendencias y retos del sector.
- Implantar nuevos productos, operaciones y tecnologías que aumenten la productividad, refuercen la resistencia y generen ventajas competitivas sostenibles.
- Promover modelos de innovación que integren criterios de sostenibilidad, responsabilidad social y viabilidad económica, garantizando un impacto positivo en el medio ambiente.
- Promover una cultura de innovación basada en los principios de colaboración, aprendizaje continuo y reconocimiento, potenciación del talento y adaptación al cambio.
- Evaluar rigurosamente el impacto de las iniciativas, garantizando su contribución tangible a los objetivos estratégicos y el valor generado para las unidades de negocio.

El ecosistema de innovación de Ferrovial es abierto y colaborativo, basado en la cocreación y la búsqueda de sinergias en todo el ecosistema global. Se da prioridad a la mejora continua de los procesos y a la integración de plataformas, garantizando la alineación con las normas corporativas y la optimización de los recursos.

Ferrovial fomenta el desarrollo de competencias digitales y el uso de herramientas avanzadas, promoviendo una cultura de aprendizaje continuo y adaptabilidad al cambio. La innovación se centra en generar un impacto positivo en la sociedad y el medio ambiente, integrando criterios de sostenibilidad, seguridad, ética y cumplimiento en todas las iniciativas.

La Política de Innovación se evalúa de forma rigurosa y periódica, reflejando el compromiso de Ferrovial por anticipar tendencias, diversificar y adaptar el modelo de negocio de forma sostenible.

MDR-A: ACTUACIONES

Ferrovial está llevando a cabo una importante transformación digital con el objetivo de mejorar su competitividad y evolucionar sus negocios y operaciones. La Compañía busca posicionarse como referente en el uso de datos, tecnología e innovación, y para ello ha definido su misión y objetivos a través del programa ReadIT 2027, que sirve de marco estratégico para la digitalización y modernización tecnológica.

La estrategia ReadIT 2027 se estructura en torno a cuatro pilares básicos que guían todas las iniciativas de transformación:

- **Palancas de la innovación:** Este pilar fomenta la generación y adopción de nuevas tecnologías, impulsa la colaboración abierta con agentes externos y promueve el desarrollo de modelos de negocio innovadores. El objetivo es experimentar con soluciones avanzadas, activar oportunidades de crecimiento y consolidar la gestión de activos de forma eficiente y sostenible.
- **Áreas de interés:** Este pilar aglutina iniciativas relacionadas con la gestión inteligente de datos, la automatización y digitalización de procesos, la integración de plataformas tecnológicas, el desarrollo de competencias digitales en las personas y la creación de productos y soluciones digitales basadas en inteligencia artificial. El objetivo es optimizar la toma de decisiones, agilizar los flujos de trabajo y mejorar la capacidad de adaptación de la organización.
- **Fundamentos:** Este pilar garantiza la sostenibilidad y el compromiso social, refuerza la resistencia operativa y asegura el cumplimiento de la normativa. Incluye la gestión responsable de los aspectos medioambientales, sociales y de gobernanza (ESG), la protección contra los riesgos tecnológicos y la vigilancia continua de la obsolescencia, garantizando un modelo de negocio sólido y preparado para el futuro.
- **Palancas de valor:** Este pilar se centra en maximizar la eficiencia, reforzar la gestión del riesgo, mejorar la competitividad y facilitar la transformación y diversificación de la Empresa. El valor generado se traduce en resultados tangibles para las distintas unidades de negocio, alineando la estrategia digital con los objetivos corporativos.

Cada uno de estos pilares incorpora variables específicas e indicadores clave de rendimiento (KPI) con objetivos concretos para 2027, lo que permite supervisar los avances y el impacto tangible de la transformación digital en ámbitos como la adopción de plataformas de datos, la automatización de procesos, la formación digital, la gestión eficiente de activos, la sostenibilidad y la resiliencia operativa.

El programa ReadIT 2027 está diseñado para fortalecer el negocio principal de Ferrovial centrándose en la automatización, la eficiencia, la competitividad, la agilidad y la monetización de datos, al tiempo que fomenta una cultura empresarial digital.

Para garantizar la eficacia de estas iniciativas, Ferrovial puso en marcha mecanismos de seguimiento y control que permiten evaluar el progreso y el impacto de la estrategia. Estos mecanismos incluyen:

- **El uso de indicadores clave de rendimiento (KPI**) para seguir el grado de avance en cada uno de los pilares estratégicos y garantizar el cumplimiento de los objetivos definidos para 2027.
- **Gestión y protección de datos y ciberseguridad,** con el apoyo de marcos normativos y herramientas especializadas que garanticen la resistencia operativa y el cumplimiento de las normas regulatorias.
- **Gobernanza tecnológica,** sustentada en modelos estandarizados que facilitan la integración y supervisión de plataformas y sistemas digitales en toda la organización.
- **Formación y desarrollo de competencias digitales,** a través de programas específicos e itinerarios de aprendizaje que promuevan la adopción de nuevas tecnologías y el uso de herramientas avanzadas como la IA y la automatización.
- **Supervisión del impacto de la sostenibilidad (ESG),** garantizando que las iniciativas digitales contribuyen de forma tangible a los objetivos medioambientales, sociales y de gobernanza, y que estos se supervisan de forma automatizada y transparente.

La estrategia establece objetivos cuantificables y sujetos a plazos vinculados a la sostenibilidad y la excelencia operativa, incluido el aumento de la digitalización y la automatización, el despliegue de soluciones de IA escalables, la mejora de la resiliencia de la ciberseguridad y el refuerzo de la estrategia ESG. Estos objetivos se supervisan mediante KPI alineados con los cuatro pilares estratégicos y se evalúan continuamente mediante informes periódicos, optimizaciones de procesos basadas en IA, seguimiento de riesgos y evolución de las iniciativas de sostenibilidad.

El compromiso de las partes interesadas desempeña un papel fundamental, pues abarca la colaboración entre unidades de negocio, las asociaciones con proveedores de tecnología, el compromiso con organismos reguladores y los bucles de información con empleados y expertos del sector. La evolución futura incluye la supervisión continua del rendimiento, el perfeccionamiento de las iniciativas centradas en la sostenibilidad y una mayor participación de las partes interesadas para garantizar la alineación con la evolución de las expectativas en materia de ESG y transformación digital.

Este enfoque estructurado garantiza que ReadIT 2027 se alinee con los objetivos más amplios de sostenibilidad corporativa y resiliencia empresarial de Ferrovial, a la vez que se mantiene adaptable a los nuevos retos y oportunidades. El programa se articula en torno a palancas de valor, de las que se extraen las capacidades necesarias para digitalizar el negocio y la Empresa en su conjunto.

Durante 2025, Ferrovial avanzó en la estrategia ReadIT 2027 a través de un conjunto focalizado de iniciativas de investigación y desarrollo dirigidas a reforzar los cimientos digitales de la Compañía y acelerar la transformación de sus negocios de infraestructuras y movilidad. Estos esfuerzos siguieron evolucionando a través de tres pilares estratégicos-palancas de innovación, áreas de interés y fundamentos-, cada uno de los cuales contribuye a un modelo operativo más eficiente, basado en datos y resistente.

En el marco del pilar Palancas de Innovación , Ferrovial amplió su capacidad para validar tecnologías emergentes en entornos operativos realistas. La Compañía reforzó las capacidades de Ferrovial Lab, donde se probaron arquitecturas de borde multisensor, motores de fusión de datos en tiempo real y modelos de conectividad de nube a borde para dar soporte a casos de uso de sistemas inteligentes de transporte (ITS) y automatización de próxima generación. Este entorno también permitió la integración de representaciones gemelo-digitales, proporcionando una visualización en tiempo real de

las detecciones y los eventos operativos. Paralelamente, Ferrovial avanzó en tecnologías de construcción autónoma, en las que los sistemas de control de máquinas guiados por GPS mejoraron la precisión de la ejecución, mejoraron las condiciones de seguridad y generaron conjuntos de datos automatizados de aseguramiento y control de la calidad (QA/QC). La Compañía también ha avanzado en su larga colaboración de investigación con el Instituto Tecnológico de Massachusetts (MIT), especialmente en modelización geotécnica predictiva y tecnologías avanzadas de monitorización de suelos, reforzando las capacidades de Ferrovial en el diseño de infraestructuras resistentes al cambio climático.

Dentro del pilar Focus Areas , Ferrovial siguió construyendo un ecosistema digital integrado que respalda la automatización, el rigor analítico y la coherencia operativa. La Compañía avanzó en la expansión de plataformas globales para procesos transaccionales y en la industrialización de sistemas de visión por ordenador basados en la nube, que mejoraron la detección automatizada de incidentes, la supervisión operativa y los análisis de seguridad en varias unidades de negocio. La ingeniería basada en datos también avanzó gracias a la evolución del entorno *Smart Tunnels*, que consolidó los modelos geotécnicos, la telemetría de las máquinas y los registros históricos de producción en una capa analítica unificada que permite un control más eficaz de la ejecución y unos procesos de licitación más precisos. Ferrovial ha reforzado aún más sus marcos de gestión de datos, incluido el mapeo de los flujos de datos financieros y operativos de extremo a extremo en su negocio de concesiones, mejorando la fiabilidad, coherencia y auditabilidad de los informes de Tráfico e Ingresos (T&R).

El pilar Fundamentos se centró en la ciberseguridad, el cumplimiento de la normativa y la innovación alineada con la sostenibilidad. En 2025, la Compañía mejoró su modelo de gobernanza de la ciberseguridad para adaptarlo a la evolución de la normativa internacional, incluida la Directiva NIS2 de la Unión Europea (Directiva sobre seguridad de las redes y de la información), las normas de la Comisión del Mercado de Valores de Estados Unidos (SEC) sobre cibergobernanza y divulgación, y las normas de Protección de Infraestructuras Críticas de la Corporación Norteamericana de Fiabilidad Eléctrica (NERC CIP). Estas actualizaciones reforzaron las capacidades de continuidad de la actividad empresarial, reforzaron la gestión de riesgos de terceros y mejoraron la integración con la plataforma corporativa de Gobierno, Riesgo y Cumplimiento (GRC). Ferrovial también avanzó en los esfuerzos de protección de datos a través de revisiones exhaustivas de los flujos de datos transfronterizos, inventarios de datos sensibles y alineación con los requisitos de privacidad aplicables en Estados Unidos y los marcos internacionales de transferencia de datos. La innovación orientada a la sostenibilidad avanzó mediante el desarrollo de la investigación sobre captura de carbono, en particular en soluciones basadas en membranas aplicables a entornos industriales, y mediante la sensorización de plantas de asfalto para apoyar mejoras de eficiencia y objetivos de reducción de emisiones.

En todos los pilares, Ferrovial siguió aplicando modelos estandarizados de gobernanza tecnológica, marcos de ciberseguridad y gestión de datos, e Indicadores Clave de Transformación (KTI) que monitorizan la adopción de tecnología y el impacto de las iniciativas digitales. En conjunto, las actividades de I+D 2025 de la Compañía reforzaron sus bases tecnológicas, mejoraron la resistencia operativa y apoyaron el desarrollo de capacidades digitales innovadoras alineadas con los compromisos de competitividad y sostenibilidad a largo plazo de Ferrovial.

Inversión en innovación en 2025	
Inversión total (€)	77.625.328,99
% de inversión directa en proyectos ESG	33,70

Nota: véase nota 3.2 de los Estados Financieros Consolidados para más información.

MDR-T: METAS

Ferrovial ha definido un enfoque integral para la gestión de objetivos y la medición del rendimiento en el marco del programa ReadIT27, alineando la estrategia con la ejecución operativa y la supervisión del impacto.

1. **ITC estratégicas y objetivos para 2027**

La estrategia de Ferrovial se estructura en torno a cuatro ejes o pilares, cada uno de ellos soportado por variables e indicadores técnicos definidos con objetivos concretos para 2027. Estos bloques representan los ejes estratégicos que sustentan la transformación digital y permiten supervisar los avances y el rendimiento en áreas clave:

- **Palancas de innovación**: Impulsan la transformación y el crecimiento fomentando la exploración de nuevas tecnologías y modelos de negocio, al tiempo que garantizan que la innovación sea transversal y relevante en todas las áreas de la empresa.
- **Áreas de interés:** Refuerzan la digitalización y la excelencia operativa, promoviendo el uso eficiente de los datos, la automatización de procesos, la integración de plataformas y el desarrollo de capacidades digitales en la organización.
- **Fundamentos:** Garantizan la sostenibilidad, la resiliencia y el cumplimiento normativo, integrando criterios ESG, ciberseguridad y vigilancia tecnológica para proteger y reforzar el modelo de negocio.
- **Palancas de valor:** Traducen la creación de valor en eficiencia, gestión del riesgo, competitividad y capacidad de transformación y diversificación, alineando los resultados con los objetivos estratégicos de Ferrovial.

2. **Modelo de impacto de los programas de iniciativas**

Además de los KTI estratégicos, cada programa e iniciativa tiene su propio modelo de impacto, que define objetivos individuales y específicos, permitiendo la medición y evaluación continuas del progreso y la creación de valor. Este modelo incluye:

- Definición de KPI operativos y de impacto a nivel de programa, flujo de trabajo e iniciativa, adaptados a la naturaleza y alcance de cada proyecto.
- Seguimiento periódico de los resultados, lo que permite tomar decisiones basadas en datos e identificar áreas de mejora.
- Evaluación continua del impacto en la eficiencia, la resistencia, la sostenibilidad, la innovación y la competitividad, garantizando la trazabilidad y la alineación con los objetivos corporativos.
- Comunicación transparente de los avances y resultados a las principales partes interesadas, reforzando la cultura de medición y mejora continua.

A través de este enfoque, Ferrovial garantiza que tanto el objetivo estratégico como los objetivos específicos correspondientes a cada programa están claramente definidos, medidos y alineados con la visión de transformación y los objetivos 2027, asegurando la creación de valor y el impacto tangible en todas las áreas de la Compañía.

Limitaciones de confidencialidad y divulgación

Cierta información cuantitativa detallada relativa a niveles objetivo específicos, valores de referencia, hitos intermedios y metodologías no se ha divulgado debido a consideraciones de confidencialidad y sensibilidad competitiva, ya que dicha información forma parte de los procesos internos de planificación estratégica y ejecución de Ferrovial.

No obstante, Ferrovial confirma que todos los objetivos definidos en el marco de ReadIT27 son medibles, están orientados a resultados y sujetos a plazos, son objeto de seguimiento periódico a través de KPI definidos y mecanismos de gobernanza, y están alineados con los objetivos estratégicos de la compañía y la hoja de ruta de transformación 2027.