CIBERSEGURIDAD

Activos protegidos

La importancia estratégica de los productos y servicios digitales (IT), de los sistemas industriales (OT), de los activos conectados a internet (IoT) y de la información que se genera y utiliza en todos los procesos y operaciones que soportan las actividades del negocio son determinantes para la creación de valor para los *stakeholders*.

100%
INCIDENTES DE SEGURIDAD GESTIONADOS SATISFACTORIAMENTE

126.800
CORREOS DE SIMULACROS DE *PHISHING* RECIBIDOS POR EMPLEADOS

26.250
USUARIOS ÚNICOS INCLUIDOS EN SIMULACROS DE *PHISHING*

32.900
CORREOS SOSPECHOSOS DE *PHISHING* REPORTADOS POR USUARIOS

Ferrovial dispone de una estructura organizativa adecuada, un modelo de seguridad robusto y se ha dotado de los recursos necesarios para garantizar la confidencialidad, integridad y disponibilidad de sus activos digitales.

ORGANIZACIÓN Y LIDERAZGO

El *Global Chief Information Security Officer* (CISO) de Ferrovial y los *Local* CISO de divisiones y filiales conforman la estructura organizativa y los recursos adecuados para implementar el programa de Ciberseguridad.

La Comunidad Global de Ciberseguridad, integrada por todos los profesionales de seguridad de las divisiones y compañías filiales, así como sus diferentes responsables de IT, da seguimiento y continuidad al desarrollo del programa de seguridad.

La Dirección de Ciberseguridad reporta a los diferentes órganos de gobierno de Ferrovial. El *Global* CISO, reporta periódicamente al Comité de Dirección de Ferrovial, a los Comités de Dirección de las divisiones, informando generalmente sobre la estrategia y el programa de seguridad, además de los principales riesgos y amenazas de seguridad.

El *Global* CISO participa en la Comisión de Auditoría y Control, bajo demanda de esta, proporcionando información sobre la estrategia y el programa de seguridad, sobre el nivel de control interno, sobre los principales riesgos y amenazas de seguridad y cómo están siendo gestionados. Además, reporta periódicamente al Consejo de Administración, proporcionando información acerca de la estrategia, del programa de seguridad y de los principales riesgos y amenazas de seguridad, así como sobre su gestión.

Durante 2022 se ha completado el plan estratégico de seguridad, iniciado en 2019. El programa de seguridad para 2023 se centra en desarrollar capacidades avanzadas de protección ante amenazas, mejorar la seguridad en el ciclo de vida de productos y servicios digitales y la gestión de riesgos de terceros, fomentar una adecuada cultura en ciberseguridad, así como aumentar las capacidades de detección y respuesta en entornos industriales.

MODELO

La Política Corporativa de Ciberseguridad, aprobada por el CEO, aplica a todas las divisiones y filiales. Se estructura en torno a un conjunto de principios y objetivos que refuerzan la estrategia de negocio. Se implementa a partir del Modelo de Seguridad basado en organización, personas, procesos y tecnologías, formalizado en un Cuerpo Normativo de Seguridad que toma como referencia las mejores prácticas del mercado, destacando el NIST CSF y el estándar ISO 27001 (Ferrovial está certificado desde 2012).

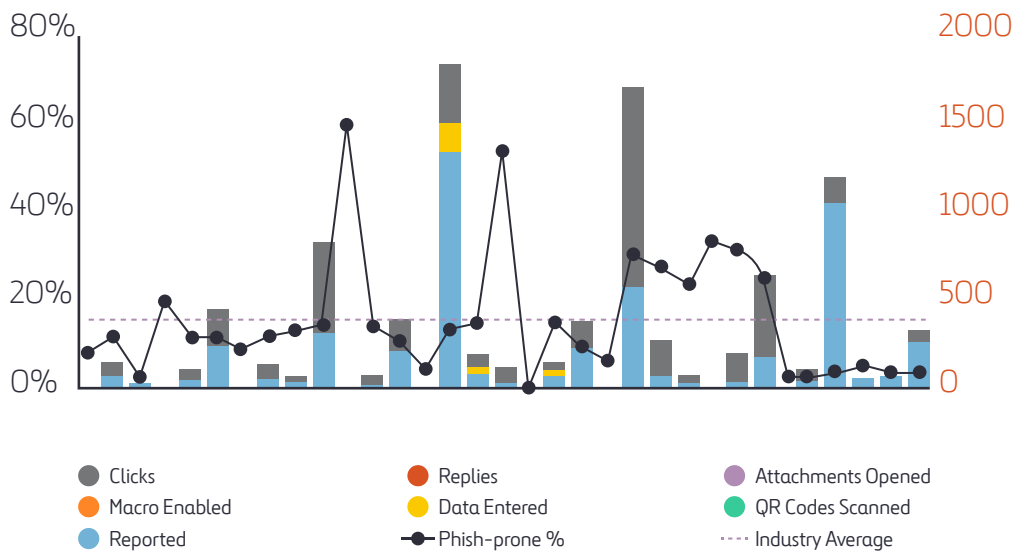
El Modelo de Ciberseguridad sigue el principio de mejora continua ISO 27001 (*Plan, Do, Check, Act*). La estrategia se implementa mediante un programa que comprende iniciativas que habilitan nuevas capacidades o mejoran las existentes. Se supervisa periódicamente por los órganos de gobierno de Ferrovial y se toman como referencia los resultados de auditorías y revisiones, el cumplimiento de los KGIs y KPIs de seguridad o nuevas amenazas de ciberseguridad.

La compañía está evolucionando su estrategia desplegando capacidades de protección, detección y respuesta para hacer frente a amenazas como las asociadas al conflicto ruso-ucraniano, la proliferación de ataques de *ransomware*, compromisos de la cadena de suministro o del correo electrónico (BEC), *phishing* o *smishing*. Entre otras medidas, se han potenciado las capacidades de detección, se han llevado a cabo simulaciones sistemáticas de compromiso y ataque y se han incrementado las campañas de entrenamiento y concienciación en materia de seguridad.

CULTURA

Con el objetivo de que los empleados y colaboradores se conviertan en la primera línea de defensa ante ciberamenazas, Ferrovial ha implantado un programa de cultura de ciberseguridad. Engloba diferentes iniciativas que se realizan de forma continua en la organización, como las simulaciones mensuales de *phishing* y las simulaciones periódicas de *smishing* y de *vishing*. Tras los simulacros, se mide el nivel de riesgo de sufrir este tipo de ataques y se adaptan los siguientes ciclos de formación, concienciación y entrenamiento a las necesidades específicas identificadas.

PHISHING SECURITY TESTS



También se utilizan medios como la intranet y Yammer para la publicación de noticias y píldoras relevantes en materia de seguridad, incluidas las relacionadas con las amenazas más comunes a las que se deben enfrentar los empleados y colaboradores, tanto en el ámbito profesional como en el privado.

Cabe destacar que los empleados de la Dirección de Ciberseguridad tienen objetivos específicos de seguridad dentro de su evaluación anual de desempeño.

CUMPLIMIENTO LEGAL, REGULATORIO Y CONTRACTUAL

El área de Cumplimiento de Seguridad, integrada en la Dirección de Ciberseguridad, es responsable de identificar la legislación aplicable y los requisitos de seguridad necesarios para garantizar el cumplimiento en esta materia.

Las normativas más relevantes cubiertas por el Modelo de Seguridad son, sin carácter enumerativo, las siguientes: el Reglamento General de Protección Datos (RGPD y LOPDGDD), el Sistema de Control Interno de la Información Financiera (SCIIF), la normativa SWIFT (*Society for Worldwide Interbank Financial Telecommunication*), la Directiva NIS, el Modelo de Prevención de Delitos tipificados en el Código Penal, el Esquema Nacional de Seguridad (ENS), la ISO 27001 y las diferentes regulaciones locales de las geografías en las que opera Ferrovial relativas a la protección de Servicios Esenciales e Infraestructuras Críticas. Cuando se identifican nuevas normas o modificaciones de los requisitos de las ya identificadas, se actualiza el Modelo de Seguridad. Asimismo, se han implantado programas específicos de cumplimiento de protección de datos, Código Penal, SCIIF e ISO 27001.

Asimismo, la Dirección de Ciberseguridad vela por el cumplimiento de los requisitos de seguridad definidos en los pliegos, licitaciones y contratos en los diferentes negocios.

DETECCIÓN, CORRELACIÓN Y CIBERINTELIGENCIA DE AMENAZAS

La compañía cuenta con dos SOC (*Security Operations Center*) que proporcionan cobertura a los eventos de seguridad que se producen en sus centros de datos, perímetros, puestos de trabajo y entornos *cloud*. Estos servicios actúan cuando reciben alertas generadas por las herramientas SIEM (*Security Information and Event Management*), al detectar los casos de uso definidos por la Dirección de Ciberseguridad.

Ferrovial dispone de capacidades de ciberinteligencia que proporcionan información de los agentes de las amenazas y sus técnicas y herramientas, lo que permite el despliegue de controles para evitar el éxito de los ataques. Además, se mantienen acuerdos formales de colaboración con agencias de ciberseguridad nacionales e internacionales con las que se comparte y recibe información relacionada con amenazas e incidentes de ciberseguridad.

RESPUESTA ANTE CIBERATAQUES

La compañía cuenta con un CSIRT (*Computer Security Incident Response Team*) que interviene cuando los eventos detectados por el SOC son susceptibles de convertirse en incidentes de seguridad. Integra capacidades de DFIR (*Digital Forensics and Incident Response*) que permiten analizar los eventos para contenerlos, mitigarlos y evitar que se repitan. Tiene especial importancia la identificación de IoCs (*Indicators*

20.000
ACCESOS BLOQUEADOS A IPS Y A DOMINIOS MALICIOSOS MENSUALMENTE

1.300
EVENTOS DE SEGURIDAD ANALIZADOS MENSUALMENTE

130.000
CORREOS *PHISHING* BLOQUEADOS MENSUALMENTE

750
INTENTOS DE ACCESO A RECURSOS CORPORATIVOS BLOQUEADOS (ORIGEN MALICIOSO/NO CONFIABLE)

of Compromise) y de TTPs (*Tactics, Techniques and Procedures*) para mejorar los mecanismos de protección y detección.

Las capacidades y procesos indicados se formalizan mediante procedimientos de gestión de incidentes basados en la Guía Nacional de Notificación y Gestión de Ciberincidentes (INCIBE-CERT) y el estándar ISO/IEC 27035, cuya operativa (respuesta, contención y erradicación) se concreta en un conjunto de procesos y *playbooks*.

Las capacidades de detección y respuesta se prueban sistemáticamente con simulaciones de *Breach & Attack* soportadas por tecnologías ya disponibles en el mercado.

RESILIENCIA Y CIBERRESILIENCIA

La compañía ha establecido Planes de Contingencia y Planes de Recuperación para responder y recuperarse de eventos disruptivos. El Protocolo de Gestión de Crisis involucra a diferentes direcciones y divisiones de Ferrovial, conforme a los protocolos establecidos para cada una de ellas. Los planes de respuesta y recuperación ante incidentes y eventos disruptivos se prueban al menos una vez al año.

Además, la compañía cuenta con una póliza de seguro ciber que ofrece, entre otros, diversos tipos de cobertura como la financiera, la de respuesta ante incidentes y la legal, ante eventos disruptivos y ciberincidentes que puedan producirse en el contexto de la actividad desarrollada por Ferrovial, unidades de negocio y filiales.

Ferrovial ha participado en los Ciberejercicios Nacionales 2022 organizados por el Instituto Nacional de Ciberseguridad (INCIBE) y por la Oficina de Coordinación de Ciberseguridad (OCC), poniendo a prueba la estructura, los procedimientos y las capacidades que articulan la detección, respuesta y recuperación ante ciberincidentes.

VERIFICACIÓN EXTERNA Y ANÁLISIS DE VULNERABILIDAD

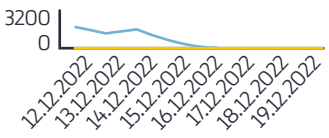
La compañía revisa de forma continua su Modelo de Seguridad para identificar áreas de mejora y vulnerabilidades. Anualmente se realizan auditorías y revisiones de seguridad, entre las que destacan:

- Auditorías asociadas a la certificación ISO 27001.
- Auditorías de seguridad en el marco de la auditoría de EEFF (ITGC e ITCC).
- Auditorías realizadas por Auditoría Interna (Tercera Línea de Defensa).
- Revisiones de seguridad *ad hoc* conforme a la planificación anual (*Red Team, Pentesting*, etc.)
- Ejercicios recurrentes de *breach & attack* combinado con *threat hunting*.
- Revisiones de vulnerabilidades en centros de datos, puestos de trabajo, perímetros y entornos *cloud.*
- Revisiones de vulnerabilidades en el código fuente.
- Revisiones de seguridad de proveedores (*Vendor Risk Management*).
- Revisión del *rating* de ciberseguridad de Ferrovial.
- Participación en ciberejercicios nacionales (INCIBE y OCC).
- Simulaciones de crisis.

Campañas de valoración del Modelo de Seguridad.

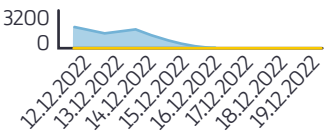
La Dirección de Ciberseguridad agrupa, asigna, planifica y monitoriza la implementación de los diferentes planes de acción que derivan de las evaluaciones, revisiones y auditorías.

Coincidencias de directivas de DLP



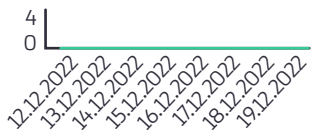
- SharePoint
- OneDrive para la Empresa
- Exchange
- Teams

DLP



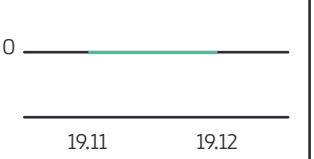
- SharePoint
- OneDrive para la Empresa
- Exchange
- Teams

Invalidaciones y falsos positivos de DLP



- Falso positivo de directiva DLP
- Reemplazo de directivas DLP

Coincidencias de directiva de DLP de terceros



- Coincidencias de directiva de DLP de terceros

Usuarios con los archivos más compartidos

Usuarios que actualmente comparten la mayoría de los archivos de las aplicaciones en la nube

Usuario	Archivos compartidos
... .com	XXX
... .com	XXX
... .com	XXX
... .com	XXX

Archivos compartidos

XXX archivos compartidos

- Compartido públicamente
- Compartido internamente

Descubrir la TI en la sombra

0 aplicaciones de alto riesgo

- Riesgo alto
- Riesgo medio
- Riesgo bajo

Informe de cifrado