CIBERSEGURIDAD

Continuidad del negocio

Los productos y servicios digitales (IT), industriales (OT), conectados (IoT) y la información, son activos estratégicos para Ferrovial de los que son responsables todos los empleados. Se debe garantizar su integridad, confidencialidad y disponibilidad para el óptimo desarrollo de la actividad en todas las líneas de negocio.

100%

Incidentes de seguridad gestionados satisfactoriamente

113.000

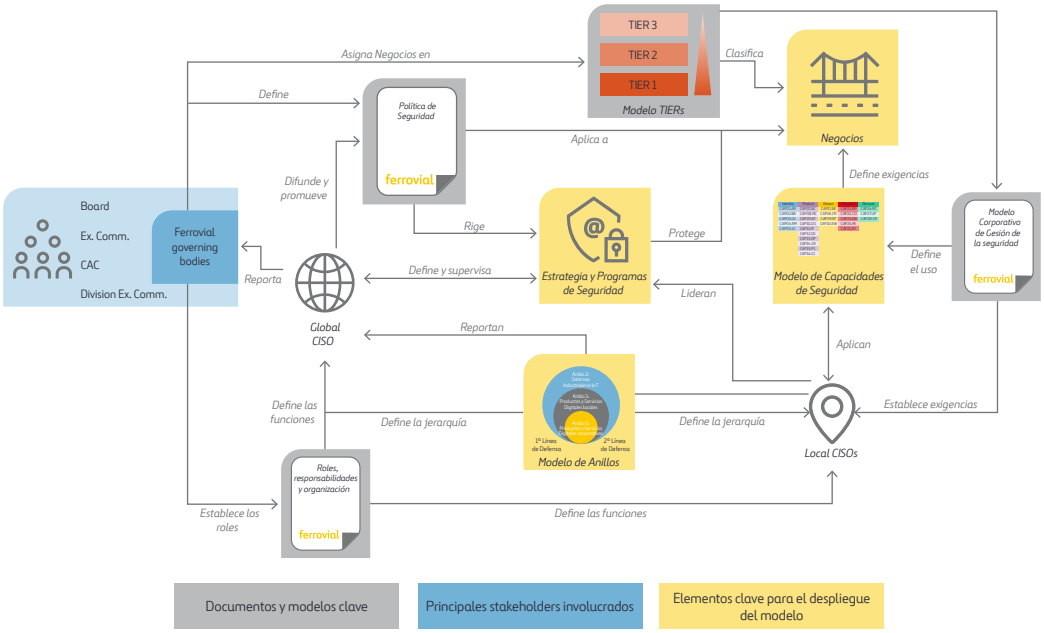
Correos de simulacros de *phishing* recibidos por empleados

18.543

Usuarios únicos incluidos en simulacros de *phishing*

14.000

SMS enviados en campañas de *smishing*



La compañía cuenta con una estructura organizativa óptima, un modelo de seguridad robusto y se ha dotado de unos recursos que garantizan la integridad de sus activos.

ORGANIZACIÓN Y LIDERAZGO DE CIBERSEGURIDAD

Ferrovial ha designado la figura de *Global Chief Information Security Officer* (CISO), dotándole de una estructura organizativa y de los recursos necesarios para implementar el programa de Ciberseguridad (seguridad) . Asimismo, cada unidad de negocio y compañía filial cuenta con la figura de *Local* CISO.

El órgano dinamizador en materia de seguridad es el Comité Global de Ciberseguridad, que permite dar seguimiento y continuidad al desarrollo del programa de seguridad. Además, hay una Comunidad Global de Ciberseguridad, integrada por todos los profesionales de seguridad en las unidades de negocio y compañías filiales, así como sus diferentes responsables de IT.

La Dirección de Ciberseguridad reporta en los diferentes órganos de gobierno de Ferrovial. El *Global* CISO, reporta periódicamente dentro del Comité de Dirección de Ferrovial y en 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.

Con carácter periódico, el *Global* CISO reporta en el Consejo de Administración proporcionando información acerca de la estrategia y del programa de seguridad, los principales riesgos y amenazas de seguridad a los que se enfrenta Ferrovial y cómo están siendo gestionados. También debe participar en la Comisión de Auditoría y Control bajo demanda de ésta 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.

Desde 2019, la Dirección de Ciberseguridad está impulsando un nuevo plan estratégico aprobado por el Comité de Dirección de Ferrovial, que se espera esté completado a lo largo de 2022.

MODELO DE SEGURIDAD

Ferrovial cuenta con una Política de General de Ciberseguridad, aprobada por el CEO, de aplicación a todas las unidades de negocio y compañías filiales. Se estructura en torno a un conjunto de principios y objetivos que soportan la estrategia de negocio de Ferrovial.

Se implementa mediante el 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).

Está basado en un conjunto de capacidades de seguridad fundamentadas en los principios del NIST CSF: Identificar, Proteger, Detectar, Responder y Recuperar todos los activos necesarios para poder realizar la actividad de negocio de Ferrovial.

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 capacidades de seguridad y proyectos que habilitan nuevas capacidades o mejoran las existentes. Se

revisa de forma periódica por parte de los órganos de gobierno de Ferrovial y se toman como referencia los resultados de las auditorías y revisiones, el cumplimiento de los KGIs y KPIs de seguridad o nuevas amenazas de ciberseguridad.

Ferrovial ha adaptado su estrategia y capacidades de seguridad para responder a las amenazas surgidas en torno a la pandemia de la COVID-19, tales como la proliferación de ataques de *phishing*, de campañas de desinformación, de ataques a empleados y colaboradores trabajando en remoto, etc. Dicha situación ha requerido potenciar las arquitecturas *Zero-Trust* ya existentes y ha fomentado la rápida adopción de modelos SASE (*Secure Access Service Edge*) y capacidades avanzadas de monitorización y correlación XDR (*Extended Detection & Response*).

CULTURA DE SEGURIDAD

Ferrovial aspira a conseguir que los empleados y colaboradores se conviertan en la primera línea de defensa ante ciberamenazas, apoyando la generación de una cultura de seguridad. Se ha desplegado el programa de concienciación en materia de seguridad "Ser consciente, te hace seguro", que comprende diversas iniciativas como la formación obligatoria en materia de seguridad y otras acciones formativas (presenciales u online), noticias y píldoras en la intranet y a través del correo; campañas preventivas y sistemáticas contra *phishing*, *ransomware*, o CEO *fraud*, así como simulacros de *phishing*, *vishing* y *smishing*. Tras los simulacros, se mide el nivel de riesgo de sufrir este tipo de ataques y se identifica qué usuarios hay que concienciar y sensibilizar en base a los resultados obtenidos.

Cabe destacar que los empleados de la Dirección de Ciberseguridad cuentan con objetivos específicos en materia de seguridad dentro de su evaluación anual de desempeño.

CUMPLIMIENTO

Dentro de la Dirección de Ciberseguridad existe un área de Cumplimiento de seguridad. Se encarga de la identificación de la legislación aplicable y los requisitos de seguridad necesarios para garantizar el cumplimiento articulado a través del Modelo de Seguridad.

Sin carácter enumerativo, las normas más relevantes cubiertas por el Modelo de Seguridad son el Reglamento General de Protección Datos (RGPD y LOPDGDD), el Sistema de Control Interno de la Información Financiera (SCIIF), la Directiva NIS, el Modelo de Prevención de Delitos tipificados en el Código Penal, el Esquema Nacional de Seguridad (ENS) y la ISO 27001. Cuando se identifican nuevas normas, o modificaciones en los requisitos de las ya identificadas, se actualiza el Modelo de Seguridad. Además, se han establecido programas específicos de cumplimiento en materia de protección de datos, el Código Penal, el SCIIF y la ISO 27001.

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

Ferrovial dispone de dos SOC (*Security Operations Center*) que proporcionan cobertura a los eventos que tienen lugar en sus *data center*, 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 eventos de seguridad definidos por la Dirección de Ciberseguridad.

Se dispone de capacidades de ciberinteligencia que proporcionan información sobre los actores de amenaza y sus técnicas y herramientas, permitiendo el despliegue de controles para evitar ataques exitosos. Además, hay acuerdos formales de colaboración con las agencias nacionales e internacionales de ciberseguridad con las que se comparte y recibe información relacionada con amenazas y ciberincidentes.

RESPUESTA ANTE CIBERATAQUES

Ferrovial dispone de un procedimiento de gestión de incidentes basado en la Guía Nacional de Notificación y Gestión de Ciberincidentes (INCIBE-CERT) y el estándar ISO/IEC 27035, cuya operativa (respuesta, contención y erradicación) está formalizada mediante un conjunto de políticas y *playbooks*.

El proceso incorpora las lecciones aprendidas de los diferentes eventos e incidentes gestionados. Es de especial importancia la identificación de IoCs (*Indicators of Compromise*) y de TTPs (*Tactics, Techniques* & *Procedures*) para mejorar los mecanismos de protección y detección.

RESILIENCIA Y CIBERRESILIENCIA

Ferrovial dispone de Planes de Contingencia y Planes de Recuperación para responder y recuperarse ante eventos disruptivos. El Protocolo de Gestión de Crisis involucra a diferentes direcciones y áreas dentro de Ferrovial, conforme a los protocolos establecidos para cada una de ellas. Los planes de respuesta y recuperación ante incidentes y eventos disruptivos son probados de forma periódica.

Además, la compañía cuenta con una póliza de seguro ciber que cubre ante eventuales eventos disruptivos y ciberincidentes que puedan acontecer en el contexto de la actividad de negocio.

VERIFICACIÓN EXTERNA Y ANÁLISIS DE VULNERABILIDAD

Ferrovial somete a revisiones continuas su Modelo de Seguridad para identificar aspectos de mejora y vulnerabilidades. Con carácter anual se realizan diferentes auditorías y revisiones de seguridad entre las que destacan:

- Auditorías asociadas a la certificación ISO 27001.
- Auditorías de seguridad en el contexto de la auditoría de EEFF (ITGC e ITCC).
- Auditorías realizadas por la función de Auditoría Interna (Tercera Línea de Defensa).
- Revisiones de seguridad ad-hoc conforme a planificación anual (*Red Team*, *Pentesting*, etc.)
- Ejercicios recurrentes de *Compromise Assessment* combinado con *threat hunting*.
- Revisiones de vulnerabilidades en *data center*, puesto de trabajo, en perímetros y en entornos *cloud*.
- Revisiones de vulnerabilidades en el código fuente.
- Revisiones de seguridad de los proveedores (*Vendor Risk Management*).
- Revisión del *rating* de ciberseguridad de Ferrovial.
- Participación en ciberejercicios nacionales.
- Simulaciones de crisis.
- Campañas de valoración del Modelo de Seguridad.

La Dirección de Ciberseguridad agrupa, asigna, planifica y realiza el seguimiento de la implementación de los diferentes planes de acción que surgen como resultado de las evaluaciones, revisiones y auditorías.