CIBERSEGURIDAD

PROTECCIÓN ANTE LAS AMENAZAS

La información es para Ferrovial un activo estratégico del que todos los empleados son responsables. Se debe garantizar su integridad, confidencialidad y disponibilidad para el óptimo desarrollo de la actividad en todas las líneas de negocio.

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 seguridad y dinamizar su despliegue en todas las unidades de negocio. Asimismo, cada unidad de negocio cuenta con la figura de Local CISO, cuyo cometido es el despliegue del programa de seguridad dentro de su entorno local. Por su parte, el órgano catalizador es el Comité Global de Ciberseguridad, que se reúne de forma periódica para dar seguimiento y continuidad al desarrollo del programa.

El Global CISO reporta directamente al Director General de Sistemas de Información e Innovación, que es miembro del Comité de Dirección. Con carácter periódico, el Global CISO reporta al Comité el estado de la estrategia y del programa de seguridad. Además, es miembro invitado de los Comités de Dirección de los Negocios de Ferrovial, donde se realiza el seguimiento sobre el grado de implantación del programa dentro de sus entornos locales.

Asimismo, con carácter anual o bajo demanda del Consejo de Administración, el Global CISO proporciona información acerca de la estrategia y del programa de seguridad, así como los principales retos y amenazas a los que se enfrenta Ferrovial en este ámbito.

MODELO DE CIBERSEGURIDAD

Ferrovial cuenta con una Política de Seguridad de la Información aprobada por el CEO, de aplicación a todas las unidades de negocio de la compañía, que expresa de forma inequívoca el compromiso de la compañía en este contexto. Se estructura en base a un conjunto de principios que soportan la estrategia de la compañía. Está disponible para todos los empleados y colaboradores en la Intranet y se comunica regularmente a través de diferentes campañas de concienciación y formaciones impartidas en materia de seguridad.

Ferrovial dispone de un modelo de seguridad de la información y ciberseguridad basado en las mejores prácticas del mercado, destacando National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) e ISO 27001 (desde 2011), cuyos objetivos son:

- Disponer de 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 proporcionar resiliencia ante los mismos.
- Homogenizar y armonizar la seguridad entre las diferentes unidades de negocio y filiales.
- Facilitar la digitalización, la innovación y la adopción de nuevas tecnologías como soporte al negocio.
- Facilitar oportunidades de negocio y procesos de licitación.
- Establecer colaboraciones estratégicas y en materia de seguridad.

El modelo se fundamenta en un conjunto de capacidades de ciberseguridad basadas en los principios del NIST: Identificar, Proteger, Detectar, Responder y Recuperar todos los activos necesarios para poder realizar la actividad de negocio de Ferrovial.

Desde 2019, la Dirección de Seguridad de la Información está impulsando un nuevo plan estratégico que tiene como objetivo dotar de capacidades de seguridad avanzadas y reforzar las ya existentes. Las iniciativas del plan están en curso y se espera que se hayan completado a principios del año 2022.

CULTURA

Ferrovial aspira a conseguir que los empleados se conviertan en la primera línea de defensa ante potenciales eventos de seguridad, apoyando la generación de cultura de ciberseguridad dentro de la compañía. Por ello, la compañía cuenta con un programa de concienciación en materia de ciberseguridad que ha desplegado por toda la organización. Bajo el lema, "Ser consciente, te hace seguro", comprende diversas iniciativas entre las que destaca la formación obligatoria en materia de ciberseguridad y otras acciones formativas, presenciales y online, en la intranet y el correo electrónico; campañas preventivas contra diversas amenazas (*phishing*, CEO *fraud*, ransomware); y simulacros contra *phishing*, *vishing* y *smishing*, entre otros.

Cabe destacar que los empleados que realizan su actividad dentro de la Dirección de Seguridad de la Información cuentan con objetivos específicos en materia de ciberseguridad dentro de su evaluación anual de desempeño. Por otro lado, todos los empleados están obligados a observar las políticas de seguridad de la información o de uso adecuado de medios tecnológicos

RESILIENCIA Y CIBERRESILIENCIA

Ferrovial dispone de un proceso general de gestión de incidentes de seguridad y ciberseguridad. El proceso está instanciado mediante capacidades de detección de amenazas y eventos potencialmente maliciosos en diferentes ámbitos, equipos de respuesta, contención y erradicación, así como de recuperación en caso de ser necesario.


CPD Telefónica, Madrid, España.

La operativa descrita está formalizada en un conjunto de políticas y procedimientos internos.

Tal y como se establece en el procedimiento de gestión de incidentes de seguridad, todos los empleados y colaboradores de Ferrovial están obligados a notificar cualquier evento sospechoso o potencialmente malicioso en los sistemas de información de Ferrovial, existiendo diferentes mecanismos para su notificación. De igual manera, los proveedores que trabajan con Ferrovial están obligados con carácter contractual a informar de cualquier incidente que pueda afectar a activos de la compañía.

Cabe destacar que las ciberamenazas son uno de los riesgos considerados en el mapa de riesgos corporativos. Puede consultarse una descripción detallada del mismo, su impacto potencial y las medidas de control implementadas en el apartado de riesgos de este informe.

Recuperación ante ciberataques

Ferrovial dispone de Planes de Contingencia y Planes de Recuperación para responder y recuperarse ante eventos potencialmente disruptivos. Existe un Protocolo de Gestión de Crisis cuya instanciación desencadena la participación de diferentes direcciones y áreas dentro de Ferrovial conforme a los protocolos establecidos por parte de cada una de ellas.

Se han identificado los procesos y activos clave para la actividad de negocio, esta relación se actualiza con carácter periódico. Los planes de recuperación se han establecido para garantizar la disponibilidad de recursos necesarios y recuperarse en los tiempos y formas determinados por las unidades de negocio, conforme a la criticidad determinada por estas.

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

VERIFICACIÓN EXTERNA Y ANÁLISIS DE VULNERABILIDAD

Ferrovial somete sus sistemas de seguridad de la información a revisiones continuas por parte de terceros independientes con el objetivo de determinar aspectos de mejora y vulnerabilidades. El objetivo es garantizar la mejora continua del programa de ciberseguridad, sus capacidades y sus recursos. Con carácter anual se realizan diferentes auditorías y revisiones de seguridad entre las que destacan:

- Auditorías asociadas a la certificación ISO 27001.
- Auditorías de sistemas en el contexto de la auditoría de estados financieros.
- Auditorías realizadas por parte de la función de Auditoría Interna.
- Revisiones de seguridad ad-hoc de diversas tipologías y con diferentes alcances, conforme a planificación anual *(Red Team, Test Intrusion, GRC, etc.)*.
- Realización de ejercicios recurrentes de Compromise Assessment combinado con ejercicios de *threat hunting*, con el objeto de detectar potenciales ataques no detectados por los sistemas de correlación de eventos.
- Revisiones de vulnerabilidades en los *data center*, en los perímetros y en los entornos *cloud*.
- Revisiones de controles anuales sobre los proveedores críticos de la Dirección General de Sistemas de Información e Innovación.
- Revisión de *rating* de ciberseguridad mediante servicio de mercado especializado.
- Participación en ciber-ejercicios.
- Simulaciones de crisis.
- Campañas de valoración de controles anuales (modelo de seguridad, SCIIF, Modelo de Prevención de Delitos).