Universidad de Buenos Aires
Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Trabajo Final de Maestría

Tema: Evaluación del Riesgo en Infraestructuras Críticas Ferroviarias

Autor: Simón Roberts

Directora de Tesis: Patricia Prandini

Cohorte: 2021

Presentación: 2023

Declaración jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Ricardo Simón ROBERTS
D.N.I. 24.589.091

Índice de Contenido

Índice de Figuras

ALCANCE

Este trabajo pretende continuar con el proyecto de especialización realizado en el primer año de la Maestría en Seguridad Informática de la Universidad de Buenos Aires. Dicho trabajo consistió en una recopilación de información relacionada con las Infraestructuras Críticas y una descripción de las principales metodologías de la gestión del riesgo en Sistemas de Gestión de Seguridad de la Información, tomando como marco de referencia las normas ISO, en particular, la norma ISO/IEC 27005:2018. Complementando y ampliando dicho trabajo, se analizará su aplicación en la Argentina, en lo relacionado a la industria del transporte, más precisamente la ferroviaria y se presentarán los principales riesgos a considerar siguiendo alguno de los modelos de gestión de riesgo detallados. También se revisarán las experiencias de otros países. Asimismo, se buscará conformar una base de conocimiento respecto a la relevancia y situación actual de la ciberseguridad en el sistema ferroviario argentino, tomando en cuenta la realidad de nuestro país y cómo se enfrenta esta situación en otros países más avanzados, en los que, como en Argentina, se lo considera una Infraestructura Crítica de Información.

INTRODUCCIÓN

La sociedad ha adquirido una gran dependencia respecto del manejo apropiado de la información. Por lo tanto, la información se ha transformado en un componente esencial de toda clase de actividades y las aplicaciones informáticas resultan cada vez más relevantes. Al mismo tiempo, los requerimientos de seguridad son cada vez mayores y esenciales en la operatoria de las organizaciones modernas. Efectivamente, los recursos informáticos se encuentran permanentemente sujetos a distintos escenarios de riesgo. Un gran número de personas, en diferentes lugares del mundo, se especializan en realizar toda clase de ataques a la seguridad, escenario frente al cual, muchas organizaciones no están adecuadamente preparadas.

Uno de los mayores retos es fortalecer la seguridad de los recursos informáticos y de las personas. La mayoría de las Infraestructuras Críticas, entendidas como aquellas que son esenciales para el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad, el bienestar económico o social de las personas, utilizan tecnologías de información y proveen servicios imprescindibles para la población. Sin embargo, debido a la falta de metodologías de identificación y clasificación de estos servicios, no se ha podido identificar cuáles son realmente críticos y, por lo tanto, cuáles requieren una protección más ajustada por parte de los operadores que las proveen.

La gestión del riesgo es un elemento fundamental en el logro de los propósitos y objetivos de las organizaciones. La explosiva evolución de la tecnología ha creado nuevos factores de riesgo que son muchas veces desconocidos por los niveles técnicos y de conducción. En este último caso, resulta fundamental que el profesional de ciberseguridad asista a los directivos a conocer en detalle los peligros que acarrea el uso de tecnologías, sus características, el efecto que una acción involuntaria o deliberada puede tener en las operaciones y lo más importante, las formas de afrontarlo, mitigarlos y/o neutralizarlos.

Por otra parte, en muchos países del mundo, el ferrocarril cumple una función de integración y comunicación entre los sectores productivos, sociales y territoriales, y permite el desenvolvimiento de muchas de sus actividades, así como la integración regional. Además, ayuda a alcanzar los objetivos de sostenibilidad ambiental y es pieza clave del sistema de transporte para asegurar la movilidad de los ciudadanos. Asimismo, es imprescindible para la consolidación económica de muchas ciudades ya que a través de ellos se movilizan y trasladan tanto personas como bienes y productos, reduciendo los costos y aumentando su productividad. Este medio se ofrece como un transporte rápido, económico y más seguro. Como otras modalidades del transporte, se han incorporado tecnologías tanto en las áreas administrativas como de operación, que se encuentran expuestas a riesgos de seguridad. Estos riesgos deben ser tratados y requieren la adopción de adecuadas medidas de protección para su mitigación

PROBLEMÁTICA GENERAL

Actualmente existen en el mercado regulaciones específicas que imponen entidades de contralor de cada sector, como bancos centrales, bolsas de valores y otros organismos de similar tenor. Estas regulaciones implican que las organizaciones deben respetar normas impuestas, ponerlas en práctica y demostrar que cumplen con ellas.

En Argentina durante los últimos años se ha avanzado en la publicación de normas relacionadas con las Infraestructuras Críticas, pero aún no se ha progresado lo suficiente en relación a su aplicación y protección, ni se han emitido pronunciamientos respecto al tratamiento de los riesgos. Cabe acotar que este tipo de transporte no ha sido expresamente mencionado ni identificado como Infraestructura Critica en Argentina, si bien podría asumirse que forma parte del sector transporte, siendo éste uno de las once áreas señaladas como críticas por el Estado Nacional.

Cabe acotar que, en este marco, la gestión de los riesgos informáticos constituye una necesidad ineludible para cualquier organización que quiera administrar y utilizar su información de manera confiable, segura y funcional para el logro de sus objetivos y dar confiabilidad a los servicios que brinda.

INFRAESTRUCTURAS CRITICAS

Los avances en la tecnología digital han revolucionado completamente la forma en que las personas, las empresas y los estados interactúan. La prestación de servicios gubernamentales, así como el flujo general de bienes y servicios, se han transformado debido a la mayor conectividad a Internet y al advenimiento del comercio electrónico y las transacciones electrónicas. Sin embargo, las tecnologías traen consigo desafíos y amenazas propias. Esto también es aplicable a las Infraestructuras Críticas de Información, ya que la adopción de nuevas tecnologías digitales permite una gestión más eficiente de las Infraestructuras Críticas en términos de escala, distancia y tiempo, pero también introduce nuevas vulnerabilidades que hacen que su debida protección sea una tarea importante y desafiante. En este sentido, la protección de los activos y sistemas de información que respaldan y forman Infraestructuras Críticas, se ha convertido en una preocupación importante para las políticas de seguridad nacional. [1]

Definición

Se define como **Infraestructura Crítica** (CI) de un país a los sistemas y dispositivos que brindan servicios esenciales para la sociedad y que, en caso de ser afectados parcial o totalmente por un ciberataque o una falla masiva, podría producirse un impacto grave que afecte a la seguridad, economía, política, energía, salud, comunicaciones o transporte, entre otros. [1]

El sector de transporte, más precisamente el ferroviario, ha sido un blanco de ataque recurrente en los últimos años. A continuación, se describen algunos ejemplos [3]:

- **Ucrania**: en el año 2015, se llevó a cabo un ataque de DoS a gran escala para desestabilizar al gobierno apuntando a centrales eléctricas, infraestructura minera y ferroviaria. El objetivo consistía en paralizar la infraestructura pública y crítica, deshabilitando los Sistemas de Control Industrial (ICS).
- **Reino Unido**: en marzo de 2020, se filtraron datos de alrededor de 10 mil personas que utilizaron una conexión gratuita de Wifi en una de las estaciones de tren. Las direcciones de correo electrónico y los detalles del viaje estuvieron expuestas en línea. El incidente ocurrió porque una base de datos de la

aplicación *'Indian Rail*' (provista por la empresa Apple) fue expuesta. Contenía 2.357.684 direcciones de correos electrónicos, fechas de nacimiento, detalles de viajes, nombres de usuario y contraseñas en texto plano.

- **Suiza**: en mayo de 2020, el fabricante suizo de vehículos ferroviarios Stadler sufrió un ataque de *ransomware*, que afectó a todas sus sucursales. Esto permitió el robo de datos confidenciales de la empresa y se filtraron en la web documentos internos; después de que la empresa se negara a ceder a las demandas de rescate.
- **España**: en julio de 2020, la entidad pública empresarial española denominada ADIF (Administrador de Infraestructuras Ferroviarias) fue atacada por un *ransomware*. A pesar de que no afectó a la CI, se expusieron gigabytes de datos comerciales.

La **Infraestructura Crítica de Información** (CII) se refiere a la infraestructura de comunicaciones e información, que incluye el sistema interno de información y comunicación utilizado en un sector en particular de CI. Si bien la definición de CII puede llegar a variar según el país, en la mayoría de ellos es parte fundamental de las políticas asociadas a una Ciberestrategia de Seguridad Nacional; dado que ocupan un rol central en su desarrollo. La manera en que se construye este concepto y se definen las áreas que serán consideradas, tiene, por lo tanto, una importancia nacional. [1]

Relevancia para la Industria y la Sociedad

Las CII en su mayoría están interconectadas con otras; es decir, que, si una infraestructura es afectada por una amenaza, es probable que sus consecuencias puedan propagarse hacia otras. Un punto innovador, en algunos países respecto a las metodologías observadas, es la clasificación de la CI en dos niveles de criticidad, uno mayor o nivel 1 y otro menor relevante, como nivel 2. Las de nivel 1, o sea aquellas que representan una alta criticidad, deben mantener un conjunto de protocolos y procedimientos para asegurar la confiabilidad de sus redes y servicios y la continuidad operacional e identificar la interdependencia con otros sectores que proveen servicios públicos y/o servicios básicos. Asimismo, es necesario incorporar a la opinión pública en la definición de estos requerimientos, para disminuir la incertidumbre y evitar la consolidación de asimetrías de poder. Si sólo deciden los expertos, no se considerarán todas las implicancias sociales, pudiendo las medidas ser insuficientes y no integrales.
Esto es así porque una CI que es afectada por un ciberataque, tiene una alta probabilidad de mostrar consecuencias que pueden repercutir de forma directa en otras

CI. Por otra parte, se ha demostrado que los sistemas críticos pueden ser altamente vulnerables debido a que al requerir un mayor nivel de monitoreo, se los conecta digitalmente haciendo más sencillo que los operadores los controlen. Es por ello que la definición de CI no puede dejar indiferente a la sociedad, ya que la elección de tecnologías (entendidas como tal, metodologías, conocimientos y/o artefactos) afectará la forma de relacionarnos y generará consecuencias políticas y sociales. [1]

Identificación

Son numerosos los desafíos que presentan las CI. Entre los primeros se encuentra definir y distinguir qué se entenderá por CI y CII, identificar las dependencias entre CI y servicios y determinar los puntos de falla. En este proceso, se deben considerar también los tipos de usuarios afectados. Considerar una industria, empresa u organización como crítica tendrá impacto en la vinculación con la sociedad. Este componente social y técnico, muestra que las CI deben ser tratadas como objetos socio técnico, es decir, objetos o procesos que requieren tanto de explicaciones técnicas como sociales, sin la imposición de una sobre la otra, para comprender su conformación, nivel de estabilidad y funcionamiento. [1]

Por otro lado, para considerarlo una infraestructura, debe contemplar tres elementos que interactúen entre sí para hacer que el sistema funcione como un todo:

- un medio de comunicación,
- una fuente de energía,
- y un mecanismo de logística.

Por lo general, se puede observar en los sectores industriales como las telecomunicaciones, medios de comunicación o repetición (antenas) e industrias de transporte (por ejemplo, ferrocarriles o infraestructura de caminos). Finalmente, debe contemplar centros de cómputos (*data centers*), instalaciones en las que se custodia la infraestructura tecnológica relacionada. Otro punto a considerar es el concepto de bien privado/público ya que, por ejemplo EE.UU. establece el sector de instalaciones comerciales como CI dado que las grandes tiendas comerciales pueden ser utilizadas como refugios o bodegas para obtener insumos de primera necesidad. Es por ello que una CI es aquella cuya inhabilitación o destrucción puede tener un efecto debilitante en la seguridad, la económica nacional, la salud pública, o cualquier combinación de estos. [1]

Características Técnicas

Las particularidades técnicas y la alta exposición de los datos que pueden ser robados, hacen que la protección de este tipo de infraestructuras sea central. Las intromisiones dirigidas a los sistemas ciberfísicos de los procesos industriales que se ejecutan en las CI hacen necesaria la adopción de nuevas estrategias capaces de detectarlos, sin interferir en su funcionamiento normal. [1]

A continuación, la figura 1 muestra las principales estrategias de protección utilizadas en los procesos industriales:

Figura 1 – Estrategias de Protección en Procesos Industriales [1]

Es relevante distinguir entre Tecnologías de Información (TI) y Tecnologías de Operación (TO), siendo que esta última se encuentra asociada a procesos productivos o industriales, y que su arquitectura difiere y no posee los mismos procesos de actualización y de seguridad, lo que dificulta los requerimientos de seguridad para CI.

En **Tecnología Informática** (TI), una vulnerabilidad se entiende como una debilidad o exposición derivada de fallas que pueden tener diversos orígenes. En general, se trata de errores o problemas documentados y disponibles al público en general, identificados mediante codificación normalizada como CVE, CWE, CVSS, etc. La explotación de una vulnerabilidad puede derivar en situaciones no deseadas: apagado de servidores, fuga de datos o eventos maliciosos varios. [1]

En **Tecnología de Operación** (TO), la ausencia de un marco normativo que contemple controles efectivos sobre ciertos dispositivos, en su mayoría obsoletos, hace que se potencie el aprovechamiento de una debilidad técnica e impacte en la CI y los servicios

esenciales que la misma brinda. Ciertamente, existen planes de contingencia y operación manual como alternativas, aunque el avance de la digitalización y el automatismo suman complejidades e interdependencias en los sistemas. [1]

Consideraciones Generales sobre Legislación

A raíz de los problemas vinculados a la protección de la CI debe pensarse en la adopción de una legislación apropiada que permita proveer adecuados niveles de integridad, confidencialidad y disponibilidad. Los aspectos jurídicos deberán acompañar los requerimientos de protección de la Información con el objetivo común de lograr el respeto de los derechos de los ciudadanos, el funcionamiento de las organizaciones y el bienestar económico del país. Es necesario que los países comprendan la necesidad de crear una conciencia y una cultura asociados al uso responsable y seguro de las tecnologías, y que identifiquen las implicancias de las amenazas crecientes, ayudando a proteger las CII, estableciendo funciones legislativas legítimas. [1] Argentina aprobó y publicó una Estrategia Nacional de Ciberseguridad en el año 2019, estableciendo una serie de principios y objetivos para un ciberespacio seguro en nuestro país. Esta estrategia menciona en su introducción que el sector analizado en este trabajo es crítico. Efectivamente, lo incluye cuando explica el concepto de servicios esenciales como aquellos que resultan" … esenciales para la vida de las personas y para la economía, como la energía, el agua, el transporte…". También hace referencia a que poseen una fuerte dependencia de las redes informáticas y que "…su protección es extremadamente compleja, entre otras razones, porque implica la coordinación de esfuerzos de múltiples actores públicos y privados…" [3]

Por otra parte, la Resolución de la ex Secretaría de Gobierno de Modernización N° 1523/2019 define el concepto de Infraestructura Crítica de Información (CII) y establece 11 sectores en las que se agrupan. Esta resolución reconoce al Transporte como uno de ellos. Si bien no está expresamente mencionado en la normativa, el transporte se divide en diversas modalidades, entre las cuales se encuentra el automotor, el ferroviario (de superficie y subterráneo), el aerocomercial y el fluvial, marítimo y de la marina mercante. A la vez, todos ellos pueden ser de pasajeros o de carga. Dentro del Ministerio de Transporte de la Nación se encuentra la Junta de Seguridad en el Transporte (JST) que se encarga de investigar sucesos (accidentes o incidentes) y emitir recomendaciones, promoviendo la cultura de seguridad en el transporte. No obstante, su enfoque es meramente a la seguridad ligada a accidentes operativos no intencionales. Es decir, no tiene en cuenta la protección contra amenazas o incidentes

intencionales ni cibernéticos. Respecto a la ciberseguridad, en Argentina existen iniciativas y acciones en las modalidades aéreo comercial, marítimo y ferroviario. [3]

Normativa vinculada a las funciones de la Dirección Nacional de Ciberseguridad de la Jefatura de Gabinete de Ministros

- Resolución JGM Nº 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información (CII) y Ciberseguridad. [1]
- Resolución ex SGM Nº 1523/2019. Definición de Infraestructuras Críticas (CI) y determinación de sectores. [1]
- Resolución ex SGM Nº 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad. [1]
- Decisión Administrativa Nº 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos. [1]
- Decisión Administrativa N° 532/2021: relacionada con la implementación de acciones relativas a la ciberseguridad y a la protección de las Infraestructuras Críticas de Información (CII), así como también a la generación de capacidades de prevención, detección, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078. [1]

Protección

Como ya hemos comentado con anterioridad, gran parte de los suministros y servicios esenciales de los países son provistos a partir de CII. Debido al carácter interdependiente y complejo y al hecho de que en economías como la nuestra, su propiedad se encuentra mayormente en manos privadas, es de suma relevancia la articulación y la cooperación para su adecuada protección. De esta manera, entre los principales actores responsables de la protección de estas infraestructuras pueden identificarse los siguientes [1]:

1. Gobiernos – Son los principales interesados en la generación e implantación de iniciativas de protección de CI para garantizar que los servicios esenciales funcionen de manera adecuada. Además, se encuentran posicionados en un espacio ideal para llevar adelante las tareas de coordinación.

2. Organismos competentes – Las tareas de difusión, elaboración y gestión de iniciativas de protección de CI es llevada a cabo por organismos públicos, privados o combinación de ambos. Esta situación puede variar según las normativas de cada país.

Estas entidades se encargan de promover que la industria adopte las medidas de seguridad establecidas por las normas aplicables. Para ello, fomentan y difunden las iniciativas de concientización y de facilitación del cumplimiento normativo. A modo de ejemplo, en España, los organismos competentes son los siguientes:

- La Secretaría de Estado de Seguridad del Ministerio del Interior.
- El Centro Nacional para la Protección de las Infraestructuras Críticas.
- Los Ministerios y Organismos Integrados en el Sistema.
- Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.
- Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.
- Las Corporaciones Locales mediante la asociación de Entidades Locales de mayor implantación a nivel nacional.
- La Comisión Nacional para la Protección de las Infraestructuras Críticas.
- El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

3. Operadores de Infraestructuras Críticas – Son los que tienen más interés en que sus infraestructuras sean seguras, funcionen de manera adecuada y no sufran daños, interrupciones ni ataques. No obstante, en ocasiones, los requerimientos de las normativas pueden entrar en conflicto con sus estrategias empresariales. Las principales funciones de los operadores críticos en materia de seguridad son:

- Analizar sus plataformas e infraestructuras tecnológicas para comprobar si hay algún tipo de problema en ellas.
- Diseñar políticas de seguridad y un marco de gobierno desde el punto de vista de la seguridad integral de sus activos de información.
- Establecer nuevas estructuras organizativas para converger la seguridad física con la cibernética bajo un mismo responsable.
- Hacer reuniones para gestionar todos temas relacionados con la seguridad que sean transversales a la organización.
- Analizar los de riesgos y las amenazas presentes y no previstas con anterioridad, ayudando a mejorar la planificación de la seguridad.
- Llevar a cabo estudios de las consecuencias y el impacto que supondría la interrupción y no disponibilidad de los servicios esenciales prestados por el operador.
- Concienciar al personal sobre la importancia del cumplimiento de los procedimientos y recomendaciones de seguridad en su operativa diaria y de la

adopción de una postura de seguridad alineada con los requerimientos de la organización.

4. Terceras partes – No se ven afectadas de manera directa por las exigencias legales, pero sí manera indirecta. Un ejemplo de ello son las empresas en que los operadores de las infraestructuras hayan delegado parcial o totalmente la gestión de las mismas. La forma en que se verán afectadas variará en función de los acuerdos establecidos con el operador de la infraestructura. Su alcance podrá cubrir la asunción de nuevas responsabilidades dentro del marco de trabajo existente en base a las exigencias legales vigentes.

Figura 2 – Principales Responsables de la Protección de las Infraestructuras Criticas [1]

Plan Completo de Seguridad Integral

Los operadores de CII necesitan incrementar sus niveles de seguridad, control, respuesta, resiliencia y comunicación en tiempo y forma frente a los posibles incidentes que los pudieran afectar, integrando la seguridad en los procesos de negocio y creando un entorno de trabajo más seguro para todos. Para lograr estos objetivos, las organizaciones deberán desarrollar una estrategia de ciberseguridad innovadora basada en principios de buena gestión de riesgos, considerando sus activos más críticos y los escenarios que plantean los eventos de riesgo que pudieran afectarlos. Se trata de un proceso deliberado de análisis de los riesgos y de decisión y ejecución de acciones para su tratamiento, con el objeto de reducir el riesgo a un nivel aceptable y a un costo razonable, teniendo en cuenta, las vulnerabilidades del sistema y actividad. Un concepto clave de la defensa en profundidad, paradigma que hoy en día es considerado una

buena práctica, es que la seguridad requiere un conjunto de medidas coordinadas. Existen cuatro pasos imprescindibles para hacer frente al riesgo y las consecuencias de un ciberataque [1]:

- Comprender el sistema, lo que es valioso y lo que necesita mayor protección.
- Comprender las amenazas conocidas a través de su modelado y de la evaluación de riesgos.
- Tratar los riesgos e implementar medidas de protección utilizando buenas prácticas internacionales.
- Aplicar un nivel adecuado de monitoreo y evaluación de conformidad (ensayos y certificación) frente a los requisitos que deben cumplirse.

GESTIÓN DE RIESGO

Como se ha venido mencionando, la información se ha convertido en uno de los activos más relevantes de toda organización y con este nuevo valor, se ha vuelto imperativa la necesidad de control, confiabilidad y disponibilidad de los datos. Para poder garantizar que este nuevo activo se encuentre seguro, independientemente del medio y el lugar en el cual se encuentre, se han generado metodologías, procesos y buenas prácticas. Es aquí donde los estándares y otras normativas sobre gestión del riesgo empiezan a tomar un papel protagónico en el proceso de asegurar la información durante todo su ciclo de vida. Nos brindan una manera sistemática de tratar los riesgos asociados y una visión global del estado actual sobre esta temática, permitiendo así planificar los controles necesarios para cumplir con los requerimientos de seguridad de la información. [2]

Enfoque Basado en Riesgo

Un enfoque de sistemas basado en el riesgo aumenta la confianza de las partes interesadas al contribuir a demostrar no solo el uso de medidas de seguridad basadas en las buenas prácticas, sino también que una organización las ha implementado de manera eficiente y efectiva. Esto significa combinar las normas correctas con el nivel correcto de evaluación de conformidad, en lugar de tratarlos como áreas distintas. El objetivo de la evaluación de la conformidad es evaluar los componentes del sistema, las competencias de las personas que lo diseñan, lo operan y lo mantienen, y los procesos y procedimientos utilizados para ejecutarlo. Esto puede significar el uso de diferentes tipos de evaluación de conformidad, que van desde la autoevaluación o la confianza del proveedor de servicios hasta la evaluación y pruebas independientes de terceros, y la selección de la que sea más adecuada de acuerdo con los diferentes niveles de riesgo.

En un mundo donde las amenazas cibernéticas son cada vez más habituales, ser capaz de aplicar un conjunto específico de normas internacionales combinado con un programa de certificación específico y de reconocimiento internacional, es un enfoque comprobado y altamente efectivo para desarrollar la resiliencia cibernética a largo plazo. Sin embargo, las normas y la evaluación de conformidad solo pueden tener un impacto máximo como parte de un enfoque basado en el riesgo que contemple una evaluación integral de las amenazas y las vulnerabilidades. Estos enfoques incorporan no solo la tecnología y los procesos, sino también las personas, lo que reconoce la función esencial de la formación. Muchas organizaciones basan sus estrategias de ciberseguridad en el cumplimiento de las normas y regulaciones obligatorias. Esto puede conducir a una mejor seguridad, pero no puede abordar las necesidades de las organizaciones individuales de manera integral. Las defensas más robustas se basan tanto en las normas horizontales como verticales. Las normas horizontales son genéricas y flexibles, mientras que las normas verticales satisfacen necesidades muy específicas. [1]

Marco de Ciberseguridad

Un enfoque de la gestión del riesgo de ciberseguridad tiene como objetivo la implementación de medidas de protección basadas en la integración de información de amenazas y vulnerabilidades identificadas y una estrategia de reducción de riesgos, promoviendo prácticas organizacionales sólidas que incluyen la planificación, los procedimientos, la priorización presupuestaria y la asignación de recursos clave (humanos, monetarios y técnicos). La gestión de riesgo se ha convertido en una instrumentación crítica en ciberseguridad. Consiste típicamente en dos sistemas de prácticas: una centrada en la evaluación de riesgos (identificación, análisis y valoración del riesgo) y otra centrada en la gestión (aceptación, transferencia, eliminación o tratamiento de riesgos). Es por ello que el objetivo de la gestión de riesgos de ciberseguridad es mantener un estado adecuado de ciberseguridad basado en las necesidades, consideraciones y mejores prácticas únicas de la industria en la que opera la organización. Con una comprensión de la tolerancia al riesgo, las organizaciones pueden priorizar las actividades de ciberseguridad, permitiendo la toma de decisiones informadas sobre el uso de recursos. [1].

La implementación de programas de gestión de riesgos permite conocer los peligros que pueden afectar a la organización a nivel informático y cómo tratarlos según su probabilidad de ocurrencia y la dimensión de su impacto. Para ello se debe contemplar lo siguiente: [1]

1. Identificación de activos.
2. Identificación de amenazas y vulnerabilidades.
3. Identificar la probabilidad de ocurrencia y su impacto.
4. Definición del riesgo asociado en base a la disponibilidad, integridad y confidencialidad deseada.
5. Tratamiento del riesgo:
    - Aceptar el riesgo hasta un cierto umbral.
    - Mitigar el riesgo en base a la implementación de medidas detectivas, preventivas y/o correctivas.
    - Transferir el riesgo a un tercero (Seguro).
    - Anular el riesgo.

Este programa le permite a la organización conocer los activos relacionados con la información, identificando amenazas y vulnerabilidades que permitan definir los riesgos reales a los que se expone dicha información y los sistemas utilizados en su gestión. No disponer de las medidas apropiadas de seguridad expone a las organizaciones a sufrir situaciones graves que pueden ocasionar pérdidas significativas (como periodos de inactividad o pérdida de datos sensibles). [1].

Metodologías

En el mercado existen varias metodologías para efectuar el análisis, evaluación y/o gestión de riesgos. A continuación, se describe un breve resumen de las herramientas y metodologías más relevantes: [2]

CRAMM

El nombre de esta metodología es el acrónimo de CCTA "*Risk Assessment and Management Methodology",* en español "método para el análisis y la gestión de riesgos de seguridad de la información". Fue desarrollado por el CCTA (*Central Communication and Telecommunication Agency* – OGC desde abril de 2001 – Reino Unido) en 1985. Es apropiado especialmente para grandes organizaciones como el gobierno o la industria. Es utilizado por el gobierno del Reino Unido. Actualmente se encuentra en la versión 5.1. [15]

Características: [15]

- Base de datos de más de 3.000 controles
- Herramientas de cumplimiento con 27001:2022
- Herramientas de evaluación de riesgos

- Herramientas para la continuidad del negocio
- Proformas para políticas de seguridad (diseño preliminar)
- Otra documentación

La metodología plantea tres etapas: [15]

- Identificación y valorización de activos
- Evaluación de amenazas y vulnerabilidades
- Recomendaciones y selección de controles.

La meta es identificar los cambios requeridos para gestionar los riesgos identificados. Se ejecuta en base a un proceso disciplinado y estructurado. Su proceso de evaluación es mixto, es decir, cuantitativo y cualitativo. Una de sus grandes cualidades es la compatibilidad de muchas de sus herramientas con la ISO/IEC 27001:2022 al tener, por ejemplo, activos de modelado de dependencia, evaluación de las consecuencias a nivel empresarial, identificación y evaluación flexible de amenazas y vulnerabilidades, cálculo del nivel de riesgo e identificación y justificación de las salvaguardas y controles necesarios. Esta metodología se complementa con un software que no se limita solo a los aspectos técnicos de la entidad, sino también abarca aspectos de seguridad provenientes de fuentes físicas y humanas, brindando una evaluación cualitativa de estos temas. Debido a su concepto y bases, CRAMM puede aplicarse en cualquier momento dentro del ciclo de vida de los sistemas de información de cualquier sistema de gestión de la seguridad de la información. Asimismo, se puede aplicar en diversos entornos tecnológicos y entidades, en los cuales se requiera asegurar una infraestructura tecnológica o inclusive, evaluar el nivel de madurez de la seguridad de la información de la entidad. De una manera resumida, a partir de la definición de activos, amenazas, vulnerabilidades y sus consecuencias, esta metodología establece una valoración para cada activo en función del impacto al que se vería expuesto. Posteriormente se correlacionan las tripletas amenazas-consecuencias-activos y se procede a la evaluación de las amenazas y vulnerabilidades generando un valor cualitativo, es decir bajo, medio o alto. Luego se computa y se genera el requerimiento de seguridad a partir del riesgo de cada una de las tripletas ya mencionadas.

Los principales problemas de la metodología son que requiere:

- Tener un conocimiento experto
- Seleccionar a los entrevistados adecuados (deben conocer los procesos relacionados)
- Conseguir un equilibrio correcto entre costo y riesgo.

Esta metodología no tiene en cuenta la política de seguridad de una organización, los productos existentes y el costo de los productos, ni la cultura organizativa de la empresa. Por otro lado, CRAMM es una metodología rigurosa, aplicable a la mayoría de los sistemas, se actualiza regularmente y cuenta con una base de datos de contramedidas de gran calidad [2].

MAGERIT

Es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de la Tecnología de Información" y fue creada por el Consejo Superior de Administración Electrónica del gobierno de España. Dada la necesidad creciente de utilizar las tecnologías de información, busca determinar y minimizar los riesgos a partir de su evaluación y de la definición de medidas de seguridad para minimizarlos. Su primera versión es de 1997 y la última, 3.0, data del 2012. Es hoy en día ampliamente usada en diversos campos de la seguridad de la información, debido a su concepto sencillo pero eficaz a la hora de generar los requisitos mínimos para la protección de la información. Esta metodología hace referencia a la seguridad como "la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o mal intencionadas que comprometen la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles". Permite analizar los riesgos que se relacionan con cualquier sistema de información, el ambiente en el cual se desarrolla y las posibles consecuencias a partir de la materialización de los riesgos seleccionados. Como resultado, se obtiene una serie de controles y salvaguardas que brinda conocimiento, prevención, seguimiento, reducción o mitigación de los riesgos investigados. Es una metodología apropiada para las entidades que estén iniciando su sistema de gestión de seguridad de la información ya que encamina los recursos y esfuerzos mediante la priorización de la resolución de los riesgos con mayor criticidad y al estar en línea con los estándares de la ISO/IEC 27001:2022, se adecua perfectamente con su ciclo de mejora continua. [2].

OCTAVE

Es un acrónimo de "Evaluación de Amenazas, Activos y Vulnerabilidades Críticos desde el Punto de Vista Operativo" (*Operationally Critical Threat, Asset, and Vulnerability Evaluation)*. Es una metodología de análisis de riesgos desarrollada en el año 2001 por el SEI (*Software Engineering Institute*) el cual depende de la Universidad Carnegie

Mellon. Tiene por objeto facilitar la evaluación de riesgos en una organización y analiza los riesgos en base a tres principios: confidencialidad, integridad y disponibilidad. Esta metodología es empleada por distintas agencias gubernamentales tales como el Departamento de Defensa de Estados Unidos.

OCTAVE equilibra los siguientes aspectos: [14]

- Riesgos operativos
- Prácticas de seguridad
- Tecnología.

Características: [14]

- Estudia la infraestructura de la información
- Es auto dirigida
- Es flexible
- Presenta una faceta diferente de los análisis tradicionales de riesgos enfocados a tecnología

Persigue los siguientes objetivos: [14]

- Permitir la comprensión del manejo de los recursos
- Identificar y evaluar los riesgos que afectan la seguridad dentro de una organización.
- Lleva adelante la evaluación de la organización y del personal que se desempeña en el área de tecnología de información

Debe existir un equipo de análisis, el cual tiene las siguientes funciones: [14]

- Identificación de recursos importantes mediante encuestas y entrevistas
- Enfoque de las actividades en el análisis de riesgos
- Relación de amenazas y vulnerabilidades
- Evaluación de riesgos
- Creación de una estrategia de protección, planes de mitigación y diseño de políticas de seguridad

La metodología OCTAVE está compuesta por tres fases destinadas a examinar los problemas organizacionales y tecnológicos, reuniendo una visión global de las necesidades de seguridad de la organización de la información. El método utiliza talleres para fomentar la discusión abierta y el intercambio de información sobre los activos, las prácticas de seguridad y estrategias. Cada fase consta de varios procesos y cada proceso tiene uno o más talleres dirigidos o realizados por el equipo de análisis. Además, existen algunas actividades de preparación necesarias que establecen una buena base para una evaluación exitosa. Estas son: [14]

- Obtener respaldo de la alta dirección: Este es el factor de éxito más crítico. Si los altos directivos apoyan el proceso, las personas de la organización participarán activamente en él.
- Seleccionar el equipo de análisis: Los miembros del equipo deben tener las habilidades suficientes para dirigir la evaluación. Ellos también necesitan saber cómo establecer una buena comunicación con los demás integrantes, ya que esto les permitirá aumentar sus conocimientos y habilidades.
- Incluir en la evaluación las zonas de operaciones. Se debe tener en cuenta que, si el alcance es demasiado grande, será difícil analizar todos los datos. Si es demasiado pequeño, los resultados pueden no ser tan significativos.
- Seleccionar los participantes para que se incluyan funcionarios procedentes de múltiples niveles de organización que aportarán sus conocimientos. Es importante que estas personas puedan comprender sus zonas de operaciones

CORAS

Conocida como "*Construct a Platform for Risk Analysis of Security Critical System"*, fue creada en el 2001 por el SINTEF, un grupo de investigación noruego financiado por organizaciones del sector público y privado. Su aplicación se inicia con la confección de modelos, conformados por siete pasos, apoyados primordialmente en la realización de entrevistas con los expertos. Proporciona herramientas como un lenguaje de modelado unificado, una gama de casos base reutilizables y otras herramientas para la implementación de la metodología. [2]

CITICUSONE

Es una herramienta de software comercial de la entidad Citicus, la cual hace uso de la metodología FIRM del Foro de Seguridad de la Información. [2]

EBIO

Diseñada para la gestión de riesgos de seguridad de los sistemas de información, cuenta con cinco fases que responden a la necesidad del tratamiento de dichos riesgos dando información relevante para la toma de decisiones que encausen la mitigación del riesgo, mediante la consideración de los controles existentes. Integra la seguridad a los sistemas en funcionamiento. Por su flexibilidad, puede usarse en diversos procesos de seguridad de la información. [2]

NIST SP 800-30

Es una publicación del NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos) que brinda las guías y criterios para realizar la evaluación del riesgo de la seguridad de la información en los sistemas y organizaciones del ámbito federal. Mediante los siguientes tres niveles de jerarquía de gestión de riesgos:

- Preparación de la evaluación,
- Generación de la evaluación,
- Mantenimiento de la evaluación.

se le proporciona a las partes interesadas, directivos y ejecutivos, la información suficiente para la toma de decisiones y la ejecución de acciones necesarias para la mitigación de los riesgos identificados. [2]

MEHARI

Creada por el CLUSIF (Club de la *Sécurité de l'Information Français*), proporciona una metodología para la evaluación de riesgos en el ámbito de la seguridad de la información acorde a la norma ISO/IEC 27005:2018, brindando una serie de herramientas y elementos creados para la gestión de la seguridad en diferentes segmentos de tiempo y parametrizables según el nivel de madurez de la entidad. [2]

A continuación, se describirá en detalle, el estándar ISO/IEC 27005 para la Gestión de Riesgos de Seguridad de la Información:

ISO/IEC 27005 - Gestión de Riesgos de Seguridad de la Información

Esta norma ofrece los lineamientos para la gestión de riesgos de seguridad de la información en una entidad, basándose puntualmente en el sistema de gestión de seguridad de la información especificado en el estándar ISO/IEC 27001:2018, teniendo como ventaja la adaptación a todo tipo de empresas. Este estándar es uno de los más reconocidos a nivel de gestión del riesgo de la seguridad de la información.

Es importante mencionar que, durante la realización del presente trabajo, se publicó (octubre del 2022) una nueva versión de la ISO/IEC 27005:2022 *Information security, cybersecurity and privacy protection - Guidance on managing information security risks* [17], pero la misma no ha sido utilizada como base en el presente trabajo dado su reciente su publicación.

Cabe aclarar que el estándar ISO/IEC 27005:2018 no determina o invita al uso de alguna metodología para la gestión del riesgo en particular, siendo ésta una decisión exclusiva de la entidad. Esto es así dado que depende de varios factores como su tamaño, el ambiente en el que se desenvuelve, el grado de aplicabilidad de la metodología y muchos otros factores que son determinantes a la hora de tomar esta decisión. [2]. Cualquier actividad de una empresa involucra riesgos, para conocerlos y medirlos, toda entidad debe realizar la gestión de esos riesgos a partir de su identificación, análisis y evaluación. Posteriormente los tratará de acuerdo con sus criterios, de manera tal que no excedan su apetito de riesgo.

Es aquí donde el estándar ISO/IEC 27005:2018 toma importancia, proveyendo un marco para la gestión de riesgos, brindando una forma eficaz para evaluarlos, particularmente en el contexto de la implementación de un sistema de gestión de seguridad de la información. Sin embargo, no es una metodología, sino una guía que brinda los lineamientos para el correcto tratamiento de los riesgos, en base a los conceptos generales de la ISO/IEC 27001:2022. La norma está redactada de manera muy técnica y direccionada a las personas que trabajan día a día con la seguridad de la información, sus líderes y también a los jefes de áreas de seguridad de la información (CISO´s), personas que trabajen en el área de riesgos y auditores. A partir de su enfoque sistémico, desarrolla el proceso de gestión de riesgos, siendo así una guía para su implementación, mantenimiento y mejora continua. El proceso busca evaluar las amenazas, sin importar su tamaño o naturaleza, ayuda a reconocer los escenarios de riesgo en los que se desenvuelve la empresa, permite conocer las amenazas que podrían afectar a la entidad y las vulnerabilidades que posee, ofrece opciones acordes y efectivas para el tratamiento de los riesgos y, por último, establece los lineamientos para su revisión, control y comunicación de los resultados. Bajo un correcto proceso de documentación, proporciona información determinante para la organización en función de su entorno, generando un aumento de la madurez del sistema de gestión de seguridad de la información y su mejora continua [2]. La gran flexibilidad y adaptabilidad de este estándar habilita a aplicarlo de forma global o específica, siendo posible implementarlo en toda la organización o en áreas determinadas de la misma. Dependiendo de las necesidades, se manifiesta el grado de especificidad de la aplicación de la gestión de riesgos, permitiendo un conocimiento puntual de dichos riesgos, de los controles y de su eficacia. [2].

Términos Generales

Para poder contextualizar la información brindada en este trabajo es necesario inicialmente, familiarizarse con los conceptos y el lenguaje relacionados a este tópico. Esto es así dado que por la diversa variedad de interpretaciones dada a los conceptos que abarcan esta temática y las múltiples perspectivas de abordaje, es habitual que se presenten inconvenientes a la hora de interpretar y aplicar correctamente la gestión de riesgos.

Descripción del Estándar ISO/IEC 27005:2018

Estructura de la Norma

La norma ISO/IEC 27005:2018 proporciona una serie de lineamientos sobre cómo gestionar los riesgos brindando un marco eficaz. Mediante una serie de cláusulas describe el proceso de gestión de riesgos de la seguridad de la información, cada una de las cuales explica una parte esencial del proceso. De igual manera tiene una serie de anexos que brindan información adicional a la enunciada en las cláusulas que conforman el estándar. Cada una de ellas se encuentra segmentada de la siguiente manera: [2]

- **Requerimientos de Entrada**: Se refiere a la identificación de la información necesaria para la toma de acciones.
- **Acción**: es la definición de la actividad a realizar.
- **Guía de Implementación**: En esta sección la norma brinda pautas, detalles e información adicional para realizar la actividad e indica el correcto “deber ser” de la actividad.
- **Sección de Salida**: Describe e identifica parte de la información resultante una vez realizada la actividad.

Visión General del Proceso de Gestión de Riesgos

Para la gestión de riesgos de seguridad de la información es necesario un enfoque sistemático que permita identificar las necesidades de la organización con respecto a la seguridad de la información y crear un Sistema de Gestión efectiva de la Seguridad de la Información (SGSI). [2] Este enfoque debería ser adecuado para el entorno de la entidad y en particular, debería estar alineado con la gestión general de riesgos empresariales. La gestión de riesgos de seguridad de la información debe ser un proceso continuo que puede ser aplicado a la organización como un todo, a un área en particular, a cualquier sistema de información o a aspectos particulares de un sistema

complejo. Cabe destacar que no todas las áreas/sistemas demandan un análisis completo y detallado. Muchas veces es suficiente con un análisis de alto nivel para poder tener los resultados esperados. Usualmente en ámbitos corporativos donde se focaliza el esfuerzo a partir de objetivos claros y un alcance definido, se procede a realizar un análisis global donde para los hallazgos de alta criticidad, o en los cuales no se pueda brindar una solución sencilla, se realiza un análisis más detallado generando un grado más amplio a nivel de amenazas y posibilidades de mitigación. [2]

A continuación, se muestra gráficamente el proceso de gestión de riesgos:

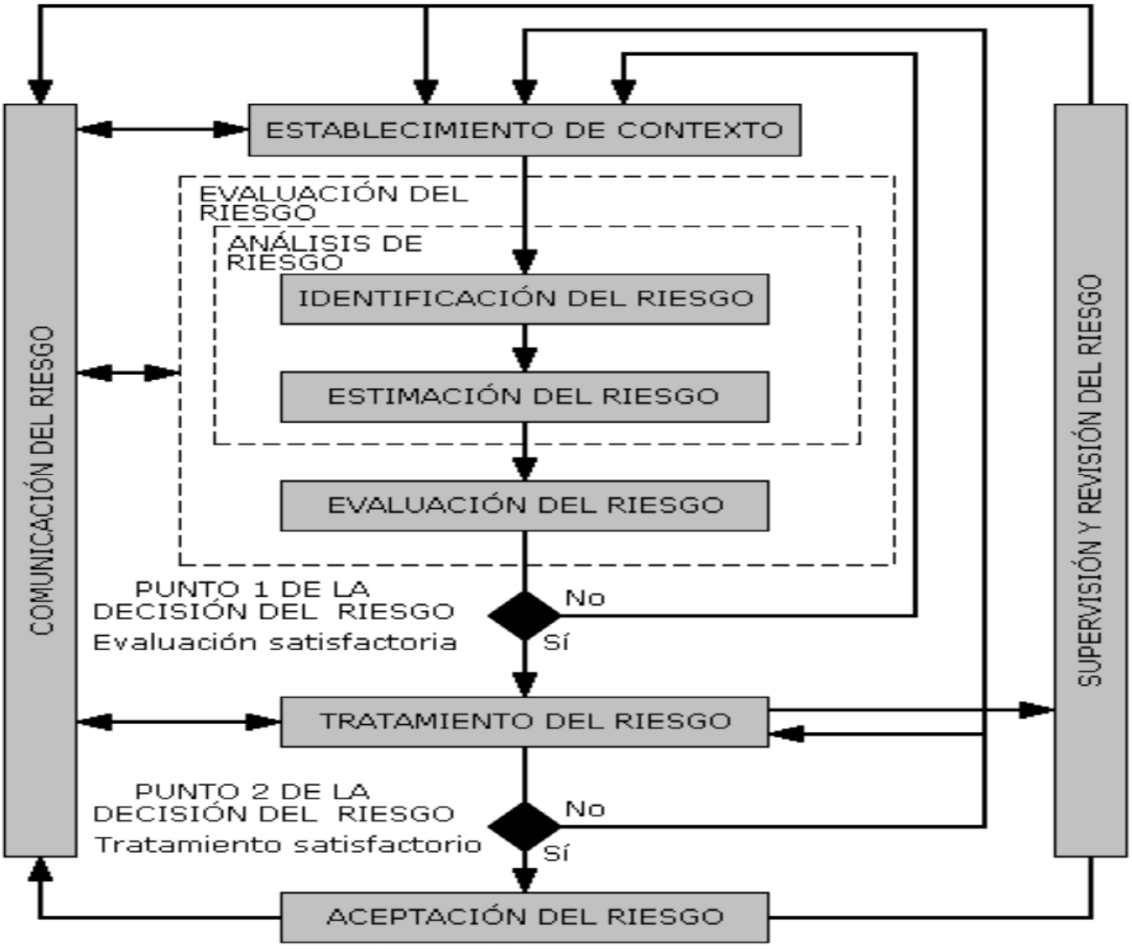

Figura 3 – Proceso de para la Gestión del Riesgo ISO/IEC 27005:2018 [2]

Como muestra la ilustración anterior, el proceso es iterativo, ya que es necesario realizar todos los pasos hasta obtener el nivel del riesgo y así poder compararlo con el apetito predefinido. Si el nivel de riesgo lo excede, se iniciará nuevamente el proceso hasta que dicho nivel quede por debajo de éste. También podría suceder que, al aplicar determinado tratamiento del riesgo, no se obtenga el nivel esperado de riesgo residual, lo cual demandará una nueva iteración relacionada con la aplicación de nuevos controles o cambios de estrategia en el tratamiento del riesgo. Por otro lado, encarar la gestión de riesgos desde un enfoque iterativo, permitiría aumentar la profundidad y el

grado de detalle de la evaluación en cada iteración. Los criterios a utilizar en cada parte del proceso deben ser materia de decisión exclusiva de los responsables de la entidad. Asimismo, una comunicación efectiva de la evaluación de riesgos a todas las partes interesadas posibilita una correcta implementación de controles, así como su seguimiento. Por último, la documentación del proceso es esencial, así como el correcto registro de los resultados obtenidos, necesarios para llevar control y seguimiento de la gestión realizada.

A continuación, se presentan las cláusulas que componen la norma, donde se describen los componentes de la gestión [2]:

Establecimiento del Contexto para la Gestión del Riesgo

Actualmente, la seguridad de la información abarca varios ítems relacionados entre sí, como son la continuidad del negocio, las tecnologías de la información y la ciberseguridad. [2]

Figura 4 – Correlación entre la Continuidad del Negocio, Ciberseguridad y las Tecnologías de la información [2]

Como se muestra en el gráfico anterior, la gestión del riesgo es una labor que debe ser afrontada de manera integral. Para ello, es necesario establecer previamente las bases de dicha gestión. Con relación al contexto de la gestión de riesgos, la norma hace referencia a los objetivos y al área en la que se le realizará la implementación. Es decir que su definición es flexible y los deja a disposición de la interpretación y necesidades de la entidad, entendiendo que cada caso es diferente y teniendo en cuenta que el enfoque que se puede aplicar dependerá de los recursos con los que se cuente. Para establecer el contexto interno y externo de la gestión de riesgos, es necesario definir los criterios a utilizar respecto de la evaluación de riesgos, de su impacto y de la aceptación

del riesgo, así como la definición de alcance, límites y el establecimiento del marco organizativo. [2]

Criterio de Evaluación del Riesgo: Cómo proceder con respecto a la evaluación del riesgo es una decisión que debe considerar varios temas relacionados con el negocio, como son los objetivos de la organización, el valor y criticidad de los activos informáticos a nivel operacional y estratégico, el entorno jurídico, legal, los requerimientos regulatorios asociados a la actividad de la organización y cualquier otro factor decisivo que considere la entidad. [2]

Criterio para Especificar las Consecuencias: Este criterio debe ser desarrollado en términos de la magnitud del daño o de los costos que podrían surgir de materialización de riesgos de seguridad de la información, tales como generación de daños personales, pérdidas financieras, interrupción del servicio, pérdida de reputación y/o imagen de la entidad o incumplimiento de regulaciones, requisitos contractuales y/o legales. En algunas entidades, la consecuencia se valora en términos del costo derivado del valor de los activos afectados y los daños producidos en el propio activo. Es importante resaltar que, a la hora de asignar valores para la consecuencia, éstos se expresen en magnitudes, ya que esto ayuda al proceso de evaluación y permite generar con mayor exactitud el umbral de riesgo o como usualmente se conoce, el apetito de riesgo. Cabe aclarar que también se puede realizar un análisis cualitativo, aunque es de menor precisión. [2]

Criterio de Aceptación del Riesgo (Apetito de Riesgo): Este criterio a menudo depende de las políticas, metas y objetivos de la organización, así como de las necesidades y expectativas de las partes interesadas. Se debe tener en cuenta que el criterio de aceptación puede ser diferente al evaluar diferentes riesgos y que también es posible la existencia de distintos niveles de apetito de riesgo. [2]

Alcance y Límites: Es necesario definir el alcance de la gestión de riesgos y se debe asegurar que se incluyen todos los activos relevantes. También deberán establecerse los límites para considerar los riesgos que pueden surgir fuera de ellos. Para definir tanto el alcance como los límites, la organización debe contemplar, entre otros, los objetivos estratégicos, las políticas, el ambiente socio-cultural, los procesos y procedimientos internos, el enfoque de seguridad de la información, la legislación y normativa aplicable y la estructura organizacional. [2]

Establecimiento del Marco Organizativo: Todo lo anterior genera los pilares necesarios para la creación del proceso de gestión del riesgo, el cual debe estar contenido en un marco organizativo y estructural, con los recursos necesarios y el establecimiento de funciones, roles y responsabilidades. Adicionalmente, se debe

identificar o crear las relaciones necesarias para el correcto flujo de trabajo de la gestión de riesgos con las partes interesadas, las áreas de involucradas y la gerencia alta y media. [2]

Valoración del Riesgo

En este punto, la norma ISO/IEC 27005:2018 determina la valoración de los riesgos de seguridad de la información como un proceso compuesto por la identificación de todos los elementos partícipes y la definición del análisis del riesgo. Los elementos a identificar son los activos, las amenazas, las vulnerabilidades, los controles existentes y las consecuencias. En base a los elementos identificados se valora el nivel de riesgo a partir de una posibilidad real de ocurrencia. La valoración que se produce en este proceso puede ser de carácter cuantitativo o cualitativo. Es importante resaltar que todas estas actividades generarán un alto volumen de información debido a la gran cantidad de datos a manejar y todas las posibles combinaciones a tener en cuenta a la hora de evaluar. Esto hace imperativo la implementación de una metodología y un proceso estructurado, sistemático y riguroso de evaluación de riesgos y el uso de herramientas automatizadas de gestión que implementen alguna metodología con el agregado de listas de activos, amenazas, controles y sus combinaciones posibles. [2]

Introducción a la Identificación del Riesgo

El propósito de la identificación de riesgos es encontrar los eventos que puede causar daño y profundizar respecto a cómo, dónde y por qué dichos eventos pueden suceder. A continuación, se detallan los pasos que indica la norma para lograr la identificación de riesgos. [2]

1. Identificación de Activos

Los activos pueden ser de diversa índole y de diferentes fuentes. A continuación, se hace mención a las diferentes categorías de activos de información: [2]

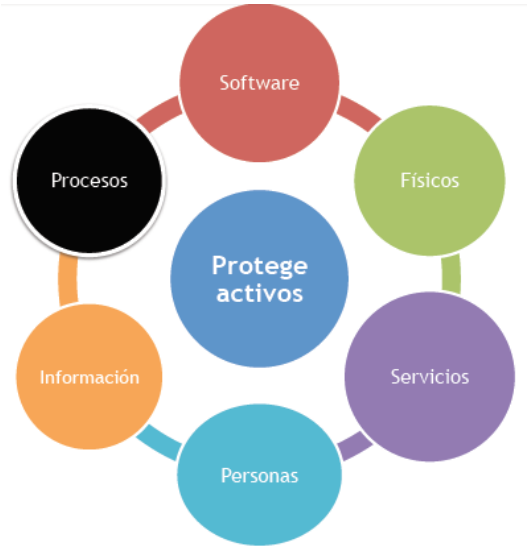

Figura 5 – Categorías de Activos [2]

Como ejemplos de las categorías mencionadas en la ilustración anterior es posible citar, entre otros; la información en cualquier soporte que la entidad genera o procesa; el hardware y software con los que se realiza el procesamiento, envío o salvaguarda de la información; los servicios para la ejecución de transferencia y control de la información; los utilitarios y sistemas de información; el capital humano; y el conocimiento que genera exclusividad para utilizar y mantener la propiedad sobre algún proceso u objeto y en consecuencia, también una ventaja competitiva. Teniendo en cuenta esto, la cantidad de elementos a considerar, clasificar y analizar es de un volumen considerable, por lo cual es aconsejable hacer uso de software especializado para esta labor, el cual debe contar con una diversa gama de activos definidos. Para identificar los activos es recomendable hacer uso de lineamientos apropiados. Como ejemplo, es posible considerar los propuestos por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC), que se comentan a continuación: [2]

- **Inventario de Activos**: Cada activo debe estar identificado, clasificado y registrado a un nivel de detalle razonable y justificable para la gestión de riesgos. Con las diversas iteraciones de esta labor se va profundizando y encontrando un nivel razonable con el cual se puede establecer un estándar de inventario de activos.
- **Propiedad de los Activos**: Cada activo debe tener asociado un dueño o propietario. Éste será responsable de la gestión del activo durante todo su ciclo de vida, así como de la implementación de los controles necesarios, acorde a la clasificación del activo.

- **Clasificación de Activos**: La clasificación debe indicar el valor del activo respecto de su sensibilidad y criticidad en términos de su confidencialidad, integridad y disponibilidad.
- **Tratamiento de Activos**: Es la definición de controles acordes a su clasificación, con base en las buenas prácticas de seguridad.

La identificación de activos a través de su inventario proveerá uno de los datos necesarios para el análisis de riesgo. La siguiente gráfica, muestra la relación de las actividades del proceso de gestión de activos de la información: [2]

Figura 6 – Categorías de Metodologías para la Gestión de Activos de información. [2]

La cantidad de activos relevados, clasificados y tratados impacta directamente en el análisis de riesgos. Cuanto mayor sea el detalle y la cantidad de información relevada, el proceso de análisis tomará más tiempo. Sin embargo, optimizará las posteriores actividades del proceso. Su límite está dado por las definiciones previas, como alcance, área de aplicación, procesos y procedimientos, enfoque de seguridad de la información, legislación, normativas que la entidad necesite aplicar. Es importante mencionar que la norma ISO/IEC 27005:2018 tiene una serie de anexos como información adicional de apoyo y referencia. Puntualmente, puede citarse el anexo B6 en el que se encuentra información como ayuda y guía para identificar los activos y llevar a cabo su valoración. [2]

2. Identificación de Amenazas

Una amenaza tiene el potencial de causar daños a los activos de información y, por lo tanto, a las organizaciones que los gestionan. Las amenazas pueden ser de origen natural, técnico o humano y podrían ser accidentales o deliberadas. Las amenazas explotan o aprovechan vulnerabilidades, quebrantando la seguridad de un activo de

información. Algunos ejemplos de amenaza son los ataques informáticos; el hurto o el fraude; los eventos físicos como terremotos, inundaciones o incendios; la falta de disposiciones corporativas y técnicas como la ausencia de certificados digitales o de cifrado de canales de comunicación; así como también la inadecuada gestión de los recursos tecnológicos. Como se puede deducir de los ejemplos anteriores, las fuentes pueden ser tanto internas como externas, siendo además necesario identificar correctamente sus consecuencias. Ello debido a que una sola amenaza puede afectar de manera transversal a más de un activo y la consecuencia podría ser diferente para cada uno de ellos. El relevamiento de las amenazas y de las vulnerabilidades debe ser una labor conjunta y preferentemente realizada por personas con diversos ámbitos de conocimiento. Una fuente clara de esta información es el propietario o dueño del activo de información, el cual conoce su naturaleza y los diversos procesos que interactúan con él, así como los incidentes de seguridad reportados. Otro recurso importante para llevar a cabo esta labor es el anexo C7 de la norma ISO/IEC 27005:2018 o los catálogos de amenazas producidos por diferentes entidades. Asimismo, las herramientas informáticas dedicadas al análisis de riesgos brindan un catálogo de amenazas generalmente asociadas a los activos que pueden sufrirlas. [2]

3. Identificación de Controles Existentes

Previamente al análisis de riesgos, es necesario identificar los controles ya implementados, conocer los activos a los que protegen, validar la documentación relacionada y garantizar su correcto funcionamiento. La inadecuada implementación de los mismos puede derivar en la generación de vulnerabilidades. Este relevamiento evitará generar esfuerzo, trabajo y costos adicionales por redundancia en la implementación de controles ya existentes. Las actividades necesarias para determinar la eficacia del control son, entre otras, las siguientes: [2]

- Validación de la documentación pertinente y relacionada al control existente. Usualmente se puede encontrar la información en reportes, pruebas de funcionamiento realizadas anteriormente y métricas de seguimiento.
- Revisión en conjunto con el personal responsable de la seguridad de la información y los usuarios que interactúan con el activo de información.
- Realización de las pruebas y verificaciones necesarias para garantizar la existencia y su correcto funcionamiento e implementación.
- Revisión de los informes de las auditorías, tanto internas como externas.

A partir de esta valoración, si el control es ineficaz o insuficiente, se deberá decidir el uso de controles complementarios o bien modificar el control, una vez realizada la evaluación de riesgos. [2]

4. Identificación de Vulnerabilidades

Una vulnerabilidad es una debilidad de un mecanismo de seguridad o control sobre un activo, que puede ser explotada por una amenaza. Es necesario identificar las vulnerabilidades asociadas a los activos informáticos. Cabe aclarar que la presencia de una debilidad no asegura que se generará un daño. Es necesario que exista una amenaza para explotarla y de no existir dicha amenaza, puede no ser requerida la implementación de controles para la mitigación del riesgo. Sin embargo, la norma recomienda el seguimiento y control de la misma. Algunas fuentes para la identificación de vulnerabilidades pueden ser las siguientes: [2]

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

La norma ISO/IEC 27005:2018 en su anexo D8 desarrolla algunos los métodos de valoración y ejemplos de vulnerabilidades. Asimismo, existen herramientas específicas en el mercado que pueden ayudar con el relevamiento de esta información. [2]

5. Identificación de Consecuencias

Ente concepto hace referencia a los efectos, a partir de la materialización de un riesgo, que se producen sobre uno o varios activos. La norma ISO/IEC 27005:2018 cita algunos ejemplos, como la pérdida de la eficacia, la generación de condiciones adversas de operación, las pérdidas del negocio, la afectación de la reputación y los daños físicos y lógicos sobre los activos. Las consecuencias pueden ser temporales o permanentes, como, por ejemplo, en el caso de destrucción de un activo. Esta actividad identifica las consecuencias para la organización que pueden ser resultado de un escenario en el que se produjo un incidente, ocurrido a partir de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades. Todo escenario de incidente que puede

afectar a uno o varios activos, deriva en una o más consecuencias, que pueden ser de distintos tipos, desde monetarias hasta degradación de credibilidad. Esta consecuencia se determina acorde a especificaciones definidas en los criterios al establecer el contexto, tal como se explicó previamente. La ISO/IEC 27005:2018 brinda una serie de recomendaciones para poder evaluar las consecuencias operativas, a saber: [2]

- Tiempo de investigación y reparación.
- Pérdida de tiempo.
- Pérdida de oportunidad.
- Pérdida de salud y seguridad.
- Costos financieros asociados a la reparación del perjuicio.
- Daños en imagen, reputación y buen nombre.

Cabe mencionar que éstos no son los únicos conceptos de los que puede hacer uso la organización, ya que depende de los criterios propios de cada entidad. [2] El siguiente gráfico muestra la relación entre los elementos a identificar: [2]

Figura 7 –Relación entre conceptos que hacen al riesgo. [2]

Análisis del Riesgo

- **Métodos para el Análisis de Riesgo**

La norma ISO/IEC 27005:2018 sugiere aplicar determinados métodos de trabajo y hacer uso de herramientas tecnológicas que permitan el rápido procesamiento de información obtenida en los pasos previos. Estos métodos se aplican para obtener un valor cuantitativo, cualitativo o también, una combinación de ellos. [2]

- **Método Cualitativo**: Hace uso de técnicas como encuestas, formularios, entrevistas, lluvia de ideas, evaluación de especialistas y expertos, análisis y valoración, haciendo uso de grupos multidisciplinarios entre otras técnicas. Se

basa en el conocimiento, la percepción y la experiencia para la toma de decisiones, dada la imposibilidad de realizar cálculos numéricos y un análisis cuantitativo, o la razón más usual, porque no es justificable la asignación de recursos para un análisis detallado. Se utilizan escalas de calificación tales como alto, medio o bajo. [2]

- **Método Cuantitativo**: A partir de una escala numérica definida y de cálculos matemáticos, genera un resultado con base en valores de la probabilidad de ocurrencia del riesgo, los cuales surgen de múltiples fuentes. Puede hacer uso de técnicas como el análisis de probabilidad, simulación computacional o análisis de consecuencias. Sin embargo, la calidad de estos resultados depende del modelo numérico usado y las consecuencias ante la materialización de un riesgo. [2]
- **Método Semi-Cuantitativo**: Se aplican las técnicas referidas en la definición del método cualitativo pero el valor de las escalas es numérico. Al igual que el método mencionado, éste es fácilmente susceptible a errores debido a que depende de interpretaciones personales. [2]

- **Valoración de las Consecuencias y de la Probabilidad de Ocurrencia**

El siguiente paso en el análisis de riesgos es la evaluación de las consecuencias. La norma recomienda tener en cuenta el valor estimado en el relevamiento de los activos para la valoración de las consecuencias, tomando en cuenta el costo de tener el activo comprometido, la pérdida o la necesidad de remplazarlo, el tiempo y los costos financieros. La posibilidad de ocurrencia de un evento se debe analizar a partir de la identificación de los actores que intervienen en la gestión de riesgos. Como se mencionó anteriormente, existen muchas fuentes de información para determinar la probabilidad de ocurrencia. La norma refiere algunos parámetros a tener en cuenta y posibles fuentes de información para el cálculo de este valor. A partir de los conceptos mencionados anteriormente, la valoración del riesgo se obtiene mediante la combinación de la probabilidad de un escenario de incidente y sus consecuencias. [2]

Evaluación del Riesgo

Para realizar la evaluación de riesgos se tendrá en cuenta los criterios definidos al establecer el contexto. Las decisiones generadas en este punto deben tener en cuenta la implementación de métodos adecuados, como lo informa el anexo E9 de la norma ISO/IEC 27005:2018. Este proceso toma como base el nivel de aceptación del riesgo definido por la organización. La norma recomienda tener en cuenta para la evaluación del riesgo, las propiedades de la seguridad de la información, los requerimientos legales,

las normativas aplicables y el grado de importancia del activo para los procesos del negocio. [2]

Tratamiento del Riesgo

Las opciones de tratamiento de riesgo son: modificar, aceptar, compartir o evitar los riesgos, las cuales se definen más adelante. A continuación, se presenta un gráfico que muestra la relación entre los diferentes niveles de riesgo. [2]

Figura 8 – Tratamiento del riesgo en Sistemas de Gestión de la Seguridad de la Información. [2]

La norma ISO/IEC 27001:2022, a partir de los informes generados en la evaluación de riesgos, requiere que se desarrolle el documento denominado “Declaración de Aplicabilidad”, que indica el perfil de seguridad de la organización detallando los controles actuales y las razones de su existencia. En comparación con la evaluación de riesgos realizada, se definirán los controles faltantes, generando así el plan de tratamiento de riesgos, que expresa cómo se van a abordar los cambios a realizar para llegar al nivel de riesgo deseado. En este documento se debe indicar todos los detalles necesarios para la implementación de cada control. Este plan de acción debe ser aprobado por la dirección e impulsado por la alta gerencia para garantizar su cumplimiento. Se requiere cumplir con los siguientes apartados en el plan de tratamiento del riesgo: [2]

- Operatoria eficaz y eficiente de la organización.
- Controles internos efectivos.
- Conformidad con las normativas, leyes y reglamentos aplicables.

Cabe señalar que mediante las acciones previamente explicadas se deben tratar todos los riesgos cuyo nivel exceda el apetito de riesgo definido por la organización y de acuerdo a la prioridad establecida. [2]

Estrategia del Tratamiento de Riesgos

En este punto se explican las opciones de tratamiento mencionadas previamente. La ISO/IEC 27005:2018 hace referencia al tratamiento de riesgos en la unidad 9, donde indica mediante un diagrama de flujo cuáles son sus opciones riesgo. [2]

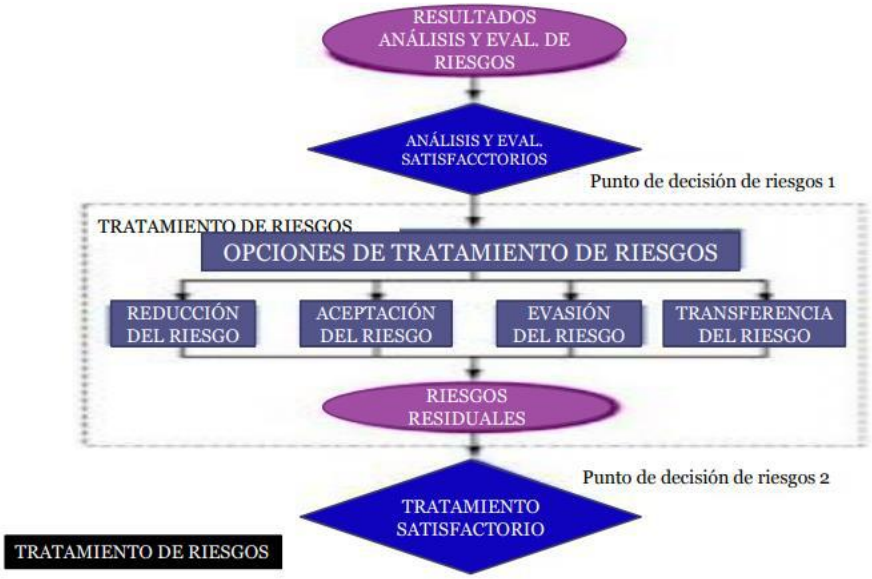

Figura 9 – Actividades para el tratamiento del riesgo ISO/IEC 27005:2018. [2]

Como se puede observar, una vez realizado el análisis y evaluación de los riesgos, se procede al tratamiento. Esto equivale a adoptar alguna de las siguientes opciones: [2]

- **Modificación**: Mediante la implementación de controles técnicos o de gestión se trata de disminuir la posibilidad de ocurrencia o la consecuencia de un escenario de riesgo. Se debe tener en cuenta que es necesario controlar constantemente la implementación y asegurar que todas las medidas implementadas sean efectivas y se ejecuten acorde al plan de tratamiento de riesgos.
- **Transferencia del Riesgo** (Compartir el Riesgo): Un claro ejemplo es la tercerización de servicios en distintas modalidades tales como, por ejemplo, *Software as a Service* (SaaS), *Platform as a Service* (PaaS) y *Infrastructure as a Service* (IaaS). Es decir, se realiza la transferencia de riesgo, tercerizando su tratamiento. Cabe aclarar que esta opción no disminuye la responsabilidad organizacional sobre los resultados del servicio.

- **Eliminación del Riesgo**: No es posible eliminar el riesgo a menos que se elimine la acción que lo genera. Tal vez sea posible encontrar una acción que reemplace a la original y cuyo riesgo puede ser tratado.
- **Retención del Riesgo**: Esta opción refiere a la convivencia con el riesgo. Ya sea, porque se encuentra dentro de los niveles permitidos para su aceptación o por la imposibilidad de tomar acción para su mitigación. Esto puede generarse por diferentes razones como, por ejemplo, altos costos o imposibilidad tecnológica o física. Se debe considerar que se está asumiendo la responsabilidad por las pérdidas, o la carga financiera de las pérdidas o sus consecuencias dentro de la organización.

Plan de Tratamiento del Riesgo

El plan de tratamiento de riesgos debe ser documentado de manera clara y concisa y debe contener los siguientes elementos [2]

- Detalle de cómo implementar los controles.
- Responsables.
- Programa de trabajo.
- Resultados esperados.
- Presupuesto.
- Indicadores de desempeño.
- Definición del proceso de revisión.

Para este último punto, se debe definir un mecanismo para evaluar las salvaguardas contra los criterios de desempeño, objetivos y las responsabilidades individuales necesarias, en pro de la realización del plan, acorde a lo proyectado. [2]

Aceptación del Riesgo

El objetivo general siempre debe ser la mitigación de los riesgos como sea posible, esto puede desencadenar nuevas oportunidades que pueden hacer a un riesgo atractivo para la organización. La adopción de nuevas tecnologías para el tratamiento de los riesgos puede generar un diferencial importante a nivel competitivo a pesar del costo de su implementación. Esto genera nuevas variables para el análisis del riesgo, como se indicó anteriormente, temas como el costo versus la oportunidad son objeto de análisis y mediante un estudio riguroso puede hacer que el criterio de la aceptación del riesgo varíe y sea necesario realizar excepciones. Cuando, por el contrario, el riesgo residual después de su tratamiento evidencie que no se encuentra sobre los niveles de

aceptación y esto genere implementaciones y toma de decisiones que conlleven a que financieramente sea inviable su tratamiento, igualmente la norma ISO/IEC 27005:2018 exige que deben ser generadas las excepciones específicas y claras del porqué de la excepción. Como se indica, ya sean por sus efectos positivos o negativos, el criterio de aceptación del riesgo puede variar después del análisis gestión del riesgo, por lo cual los criterios de aceptación del riesgo no es simplemente validar si el riesgo está dentro del apetito de riesgo de la entidad. En la práctica se evidencia que en varios casos no es posible la opción de tratamiento indicada o que cumpla con todo lo necesario para la reducción del riesgo, y de igual forma, se generaran beneficios que conlleven a nuevas oportunidades para la entidad. Por lo cual es importante hacer la revisión de los criterios de aceptación del riesgo mediante una mezcla del tratamiento del riesgo y de la aceptación de los riesgos residuales. Lo anterior conlleva a que se debe documentar de manera rigurosa cada decisión y su justificación, aún más cuando se deba aplicar excepciones por cualquier razón. Usualmente, una muestra clara de estas excepciones refiere directamente al presupuesto. Dado que éste siempre tiene limitaciones es adecuado priorizar los riesgos para atender primero los más importantes. A posteriori, deberá quedar documentado que fue necesario asumir riesgos por falta de presupuesto. [2]

Consulta y Comunicación del Riesgo

Ésta es una actividad que tiene como objetivo lograr un acuerdo, en la alta dirección y entre las partes interesadas, respecto de la manera de tratar los riesgos, intercambiando opiniones y compartiendo información. Una efectiva comunicación entre las partes interesadas es importante porque asegurará que los responsables de implementar la gestión de riesgos entenderán el motivo de la toma de determinadas decisiones, así como la razón de ejercer acciones particulares. Como se ha visto a lo largo de este documento, la labor de la gestión de riesgos no refiere exclusivamente a los analistas de riesgos, sino es una labor mancomunada y colaborativa de todas las personas que interactúan en la entidad, lo cual hace que la comunicación sea un pilar de todo el proceso. Una vez se han evaluado los riesgos, el siguiente paso a considerar es la comunicación de los resultados obtenidos y del plan de tratamiento. Es importante considerar, en las diversas soluciones para la mitigación del riesgo, la percepción de las personas involucradas debido a que ello puede impactar tanto en la evaluación como en los planes de tratamiento. Se recomienda crear un plan de comunicación para todas las personas involucradas, ya sean internas o externas a la entidad, en donde se informen los temas más relevantes del riesgo, el cómo se verán afectados y los

procesos, procedimientos y responsabilidades de cada uno en su mitigación. Esto pretende generar el consenso necesario entre los interesados para la gestión del riesgo. La comprensión del porqué de las decisiones y el apoyo y colaboración del personal para llevar a cabo el plan de tratamiento de riesgos permitirá la retroalimentación de todas las partes y la colaboración mutua para el alcance de los objetivos trazados. [2]
Como se informa en apartados anteriores, la comunicación del riesgo es un proceso que se realiza en cada etapa de la gestión, ya que es necesaria en si misma desde la recolección de la información, hasta la puesta en marcha del plan de tratamiento, lo cual la convierte en punto clave de todo el proceso. Por lo cual se debe documentar e identificar las apreciaciones de todas las partes interesadas y asegurar que sean comprendidas y tenidas en cuenta, ya que generan consecuencias sobre todo el proceso, las decisiones y la implementación de las mismas. El alcance de resultados depende en gran medida de la comunicación efectiva, desde el inicio al fin. Esto brindará garantías para el cumplimiento de objetivos, toma de decisiones, implementación del plan de tratamiento de riesgos, concientización, coordinación del personal y apoyo de las diversas áreas a partir de los cambios a realizar. La organización puede valerse de métodos comunicacionales para la difusión efectiva de la gestión de riesgos, así como un comité de comunicación que pueda evaluar la información emitida por las partes interesadas con respecto a la gestión del riesgo. [2]

Control y Revisión del Riesgo

Nada puede mejorarse sin conocer su estado a través del tiempo. Esto solo puede darse a partir del seguimiento y la supervisión de la puesta en marcha de los controles, lo cual generará las correcciones que fueran necesarias para su mejoramiento. La evaluación y la verificación del alcance de los objetivos propuestos, no solo para la gestión de los riesgos sino para todo el sistema de gestión de la seguridad de la información, mediante el control y la revisión, busca encontrar las carencias y problemas que podría tener el plan de tratamiento. Así como cambios que se presenten en el contexto, nuevas vulnerabilidades, cambios en la probabilidad de ocurrencia, consecuencias y amenazas en el transcurrir del tiempo. El seguimiento permite controlar la eficiencia y efectividad de las medidas tomadas para la mitigación del riesgo, el contexto del riesgo y la vigencia de los controles implementados. Llevar a cabo el control generará nueva información valiosa para el ciclo de mejora continua del sistema de gestión de riesgo, y es parte integral de todo el modelo de trabajo. Es aplicable en todas las etapas y su intervención es esencial para prevenir, advertir y retroalimentar cada proceso. La dinámica propia de la entidad influye en este punto. El cambio de los objetivos o estrategia corporativa, la

adquisición de nuevas empresas, la adopción de nuevas tecnologías, la adquisición y generación de nuevos activos, el cambio en las normativas y leyes amerita a que el control sea una labor continua. De la mano del control y de la revisión se encuentra la mejora continua. Es usual que el enfoque o los criterios de evaluación sean afectados por los cambios en los riesgos, haciendo necesario generar otro ciclo de análisis con los cambios necesarios, o bien cambios en la metodología de análisis, cambios en las herramientas y demás, aplicables al ciclo de gestión de riesgos. Una ratio de tiempo usual para la revisión es de un año. [2]

Principales Cambios en la ISO/IEC 27005:2022

Si bien, como se mencionó previamente, dada la reciente aparición de la nueva versión del Estándar ISO/IEC 27005 publicada en octubre de 2022, el presente Trabajo Final se basó en la versión anterior de 2018. Sin embargo, a los fines de complementar el análisis efectuado, se incluye a continuación una breve síntesis de las principales diferencias entre ambas versiones.

La nueva revisión de la norma ISO/IEC 27005:2022 refuerza el vínculo con el SGSI (ISO/IEC 27001) al proponer un enfoque adicional basado en eventos. Este marco permite captar escenarios de riesgo con un análisis de mayor nivel teniendo en cuenta el ecosistema de la organización y la relación entre los procesos y la información. Esto permite realizar evaluaciones preliminares de los riesgos para la seguridad de la información cuando no se dispone de una arquitectura ya definida. Asimismo, la adición de los criterios de activación que orientan sobre cuando iniciar una actividad, un paso del marco, o cuando actualizarlo, lo que permite mantener una evaluación actualizada y dinámica de los riesgos para la seguridad de la información. [18]

A continuación, se detallan los principales cambios observados en esta versión:

- Alinea el texto con la ISO/IEC 27001:2022 y la ISO 31000:2018;
- Unifica la terminología con la empleada en la ISO 31000:2018;
- Ajusta las cláusulas a la disposición de la norma ISO/IEC 27001:2022 (impacto se sustituye por consecuencia)
- Introduce la definición de escenario de riesgo y los conceptos asociados, en lugar del escenario de incidente.
- Contrasta el enfoque basado en eventos con el basado en activos para la identificación de riesgos. Es probablemente el cambio más importante de la norma.

- Introduce un criterio de activación para mantener una evaluación actualizada y dinámica.
- Hace hincapié en la supervisión de los escenarios de riesgo (vínculo con la norma ISO 27035-1:2016 y las actividades SOC/SIEM).
- Actualiza los anexos, ya que suprime varios anexos antiguos e introduce nuevos.
- Destaca la explotación de vulnerabilidades dentro del enfoque basado en activos, lo que podría abrir la puerta a la asignación de CVE (Vulnerabilidades y Exposiciones Comunes) a escenarios operativos.

En conclusión, se puede afirmar que la nueva versión refuerza la relación con la norma ISO/IEC 27001. En otras palabras, se hace mayor hincapié en que las dos normas son dependientes entre sí, ya que la ISO/IEC 27005 proporciona lineamientos sobre cómo gestionar los riesgos de seguridad de la información necesarios, proceso necesario para el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información, objetivo central de la ISO 27001.

Implementación de las Metodologías de Riesgo Según el Estándar ISO/IEC 27005:2018

Este estándar de buenas prácticas es muy claro y fácil de seguir y de acoplar con alguna de las diversas metodologías mencionadas. Al ser un proceso secuencial y claro en las definiciones de cada etapa, permite anticipar fácilmente el mapeo de la norma con las diferentes fases, procesos y procedimientos de cada metodología, en este aspecto lo primero que se debe tener en cuenta son los 5 aspectos de la ISO/IEC 27005:2018 para la gestión del riesgo: [2]

1. Establecimiento del contexto.
2. Evaluación del riesgo
    A. Identificación del riesgo.
    B. Estimación del riesgo.
    C. Valoración del riesgo.
3. Tratamiento del riesgo.
4. Aceptación del riesgo.
5. Comunicación del riesgo.

Es fácil deducir cómo los procesos de cada metodología se ubican en cada paso descrito por la norma, ya que cada metodología utiliza los conceptos y los términos definidos en ella. La diferencia radica en cómo se llevan adelante los pasos, a partir del enfoque que tienen las metodologías. Es decir, la metodología permite realizar un

análisis de riesgos de seguridad de la información que, entre otras cosas, abarca toda la organización, brinda más herramientas y métodos para las labores a ejecutar. Es posible ejecutar de manera más efectiva acciones tales como: [2]

- Establecimiento de la lista de activos relevantes.
- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Cálculo del nivel de riesgo en base a las variables que lo determinan.
- Análisis de consecuencia si se produce la amenaza.
- Niveles de riesgo acordes al análisis realizado.
- Relevamiento de los controles y salvaguardas actuales.
- Listado de nuevas salvaguardas y controles a implementar a partir de lo relevado.
- Creación de plan de acción para mitigar el riesgo.

Cada metodología se vale de las normas ISO para marcar las pautas de su ejecución y estructura, estableciendo el ciclo de gestión de riesgos de la información. Sin embargo, son fácilmente identificables ciertas etapas que componen el proceso, las cuales se detallan a continuación: [2]

- **Relevamiento de los activos de información:** Esto refiere al proceso de identificación, categorización y valoración considerando los criterios asentados en las normativas ISO como los son la disponibilidad, integridad y confidencialidad. [2]
- **Relevamiento de las amenazas:** Esto refiere a la manera en que esta metodología determina a qué amenazas están expuestos los activos. Es decir, cada una de ellas procede de una forma diferente en este paso. Sin embargo, cumplen con la identificación de las amenazas existentes en el contexto de riesgo. Una de las diferencias más marcadas refiere a los criterios de valoración, ya sean cualitativos o cuantitativos. [2]
- **Evaluación del Riesgo:** El cómputo referente a la evaluación del riesgo puede ser uno de los ítems más notorios marcados como diferencia. Sin embargo, cada método cumple con la valoración de la consecuencia en un activo generado por una amenaza que explota las vulnerabilidades relevadas. Proceso usualmente apoyado en las herramientas y software de uso de cada metodología. [2]
- **Lista de Salvaguardas:** Como se vio anteriormente, cada metodología genera un listado de mecanismos de mitigación de los riesgos relevados. Estas salvaguardas y contramedidas están en línea con el anexo F de la ISO/IEC

27005:2018, el cual especifica las restricciones para definir la modificación de los riesgos, entre las que se encuentran las operativas, técnicas, culturales, éticas y legales. [2]

- **Análisis del Riesgo Residual:** Una vez aplicadas las contramedidas y salvaguardas sugeridas, se procede a la evaluación de riesgo remanente después de la mitigación. Se valida si se encuentra por debajo del nivel aceptado, calculando la nueva consecuencia contra su mitigación. Como refiere la norma, en el proceso de gestión de riesgo, cada metodología presenta un ciclo iterativo que se realiza hasta que el riesgo disminuya y sea aceptable para la organización. [2]

En términos generales, la automatización de las metodologías permite reducir los tiempos de ejecución de las actividades requeridas para la gestión de riesgos y quizás lo más importante, minimizar los errores. Las fases o procesos de las metodologías mencionadas cumplen con la iteración continua del análisis del riesgo, la evaluación de los riesgos residuales después de la implementación de salvaguardas para poder asegurar la correcta mitigación, así como la mejora continua a partir de la evolución de la entidad, como lo especifica la norma. Otro punto importante, entre los contemplados por el estándar, es la generación de informes de tratamiento de riesgos, tema en el que las metodologías presentan la información de manera priorizada, lo cual facilita la toma de decisiones. Después del análisis realizado sobre los modelos descritos se puede ver que las metodologías se encuentran altamente relacionadas con el proceso de gestión de riesgos, por lo cual su implementación encajada sobre el proceso de análisis y evaluación del riesgo cumple con lo requerido por la norma ISO/IEC 27005:2018. Cada uno de sus capítulos se asemeja a las diferentes fases o procedimientos de las metodologías, cumpliendo en diverso grado con los requerimientos propuestos y las salidas o resultados esperados. La agrupación de estos capítulos sobre cada metodología no impide ni dificulta su cumplimiento. Por lo contrarío automatiza y optimiza las labores a desempeñar, da un orden lógico secuencial y una secuencia que caracteriza a la metodología, a los procedimientos que hacen al análisis de riesgos. [2]

EVALUACIÓN DE LA INDUSTRIA FERROVIARIA EN RELACIÓN A SU CONSIDERACIÓN DE INFRAESTRUCTURA CRITICA

Los medios y redes de transporte permiten el desarrollo y crecimiento del país, ya que a través de ellos se movilizan y trasladan tanto personas como bienes y productos. Las

vías de comunicación están conformadas por las redes viales de carreteras y autopistas, las redes ferroviarias, los canales fluviales, los puertos, los aeropuertos y el transporte urbano en general. A medida que las poblaciones van generando nuevas necesidades, la ciencia y la tecnología van avanzando para poder satisfacerlas. Por ello, durante la segunda revolución industrial, la implementación del ferrocarril como medio de transporte ha sido un factor crucial para el desarrollo del comercio, puesto que las empresas pudieron empezar a disminuir sus costos y aumentar su productividad. Este medio se ofrece como transporte rápido, económico y más seguro. El ser humano constantemente demanda bienes y servicios, lo cual promueve el aumento de la productividad. Gracias a este medio de transporte se puede trasladar bienes y servicios a las poblaciones lejanas, a fin de satisfacer sus necesidades. [13] El transporte en general cumple una función de integración y comunicación entre los sectores productivos, sociales y territoriales, y permite el desenvolvimiento de todas las actividades de un país, así como la integración regional. Asimismo, la construcción del ferrocarril permite reducir los accidentes de tránsito que a diario se registran en todo el territorio nacional y, su masiva utilización permite reducir las emisiones de contaminación hacia el ambiente atmosférico. [13] Los países más desarrollados del mundo hacen importantes inversiones en sus sistemas ferroviarios, único sistema de transporte terrestre con enorme capacidad de transportar personas o cargas con bajo impacto para el medio ambiente, con una pequeña tasa de siniestralidad y con alta eficacia en los traslados. Por tanto, es de suma importancia incrementar la inversión y mantenimiento de un sistema de transporte ágil, moderno, rápido y económico como es el ferrocarril, para el desarrollo de las economías regionales, la comunicación de los pueblos, el crecimiento de la nación y la complementación económica en verdaderos corredores binacionales.

Por otra parte, desde el inicio de la era industrial, el ferrocarril fue una de las herramientas fundamentales para la expansión de las economías y la ocupación de territorios. [13] La investigación tecnológica y la inversión han logrado ferrocarriles más veloces y económicos que reducen los costos de transporte en tramos de media distancia. Por tanto, las políticas nacionales de transporte deben contemplar la situación y las perspectivas del ferrocarril, así como los proyectos de crecimiento a largo plazo. [13] La Unión Internacional de Ferrocarriles es la asociación mundial para la cooperación entre los principales actores del sector ferroviario internacional. Su objetivo es avanzar hacia la estandarización y la mejora de los sistemas de construcción y explotación de ferrocarriles interoperables. En los últimos años la organización ha rediseñado sus objetivos y ha puesto especial énfasis en cuestiones como la liberalización y

globalización del sector ferroviario mundial, o los nuevos retos que le plantea al ferrocarril su papel clave en un escenario de desarrollo sostenible y lucha contra el cambio climático. La Asociación Latinoamericana de Ferrocarriles es una entidad reconocida por las Naciones Unidas como organización no gubernamental, constituida por la mayoría de las empresas ferroviarias e industriales latinoamericanas, lo que otorga la representatividad de esta región en el Consejo Mundial de la Unión Internacional de Ferrocarriles. Tiene como premisa: potenciar un transporte ferroviario seguro, eficiente y económico, fomentando y fortaleciendo los ejes de integración latinoamericanos, a través de los flujos de intercambio que permiten absorber la multiplicación de los tráficos. Para alcanzar este objetivo, se promueve en los niveles públicos una política de transporte que asegure la participación del modo ferroviario en un contexto de equidad. [13]

Por otro lado, los sistemas ferroviarios han evolucionado significativamente gracias a las nuevas tecnologías y sistemas de comunicación. A pesar de que la seguridad en la industria ferroviaria siempre ha estado relacionada con la seguridad operativa, debido a la creciente integración de las TIC (Tecnologías de la información y la comunicación) y la expansión de IoT (Internet de las Cosas), el número de riesgos cibernéticos ha aumentado constantemente durante la última década. Igualmente, los sistemas de control de trenes y los sistemas de señalización cada vez son más autónomos y dependientes de estas tecnologías. La ciberseguridad trata de proteger los sistemas contra el robo o el daño, defendiéndolos de los ataques y riesgos externos e internos, en particular como resultado de actos criminales o terroristas. [8] Hoy en día, la seguridad en IoT afronta retos relativos a la autenticación, detección de intrusiones, privacidad de los datos, integridad de los datos y comunicaciones seguras. Más aún, los sistemas de control y señalización cada vez son más autónomos y tienen una mayor dependencia de los sistemas TIC y de las comunicaciones por radio, lo que genera nuevas vulnerabilidades. Es por ello que la seguridad es un tema de vital importancia en las infraestructuras ferroviarias. [8].

El Sistema Ferroviario

Los sistemas ferroviarios modernos tienen una infraestructura específica de control y señalización (por ej. Enclavamientos electrónicos). En concreto, en Europa, para garantizar la interoperabilidad, se creó el sistema ERTMS (*European Rail Traffc Management System*), el cual fue diseñado en los años 90. Se compone del sistema de señalización por radio ETCS (*European Train Control System*) y del estándar de radio

móvil GSM-R (*Global System for Mobile Communications Railways*). ETCS contempla tres niveles distintos según cómo se obtenga la información para la gestión de los tramos de vía (por ej., euro balizas en el nivel 1 o mediante GSM-R en los niveles 2 y 3). GSM-R está basado en GSM, una tecnología 2G que al día de hoy está obsoleta para el soporte de servicios avanzados de datos. GSM-R está siendo reemplazado por tecnologías 4G/5G de conmutación de paquetes como LTE (*Long Term Evolution*). [8]

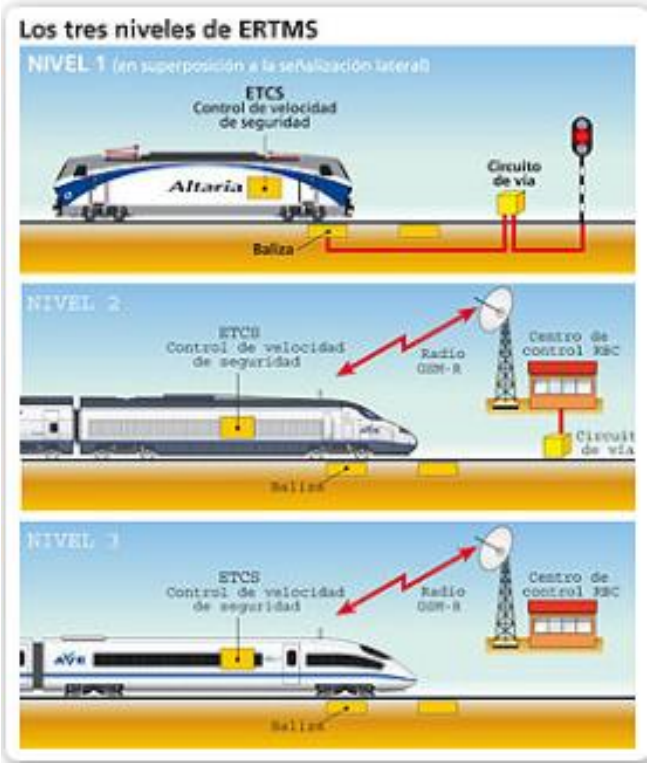

Figura 10 – Sistema Europeo de Gestión del Tráfico Ferroviario (ERTMS)

Teniendo en cuenta esta migración, las políticas de seguridad y las estrategias de diseño deben revisarse considerando escenarios de riesgos futuros. Cada operador ferroviario se enfrenta al desafío de proteger su propia infraestructura reduciendo su vulnerabilidad a los ciberataques. En la mayoría de los casos, se utilizan tecnologías y soluciones de software heterogéneas que producen datos muy diversos. El riesgo cibernético se ve también exacerbado por la enorme cantidad de datos resultante de un número cada vez mayor de dispositivos IoT, procesos y servicios. Por tanto, la protección de tales entornos es compleja y multidimensional. [8]

Por otro lado, las tecnologías involucradas están integradas en sistemas de comunicaciones de datos conectados a internet mediante servidores, lo que implica un riesgo de acceso por personal no autorizado. Además, los operadores ofrecen capacidades extras a terceras partes (por ej., servicios de *streaming* a bordo), lo que facilita que potenciales atacantes externos puedan tener acceso. Un diseño adecuado

de la arquitectura de la infraestructura ayuda a mejorar la resiliencia, pero es esencial integrar la seguridad en todos los aspectos de la solución a lo largo de su ciclo de vida. [8] Esto las expone a una serie de vulnerabilidades que se acentúan ante la falta de mantenimiento y la carencia de estándares y controles acordes que, entre otros motivos, incrementan sus posibilidades de ser víctimas de ciberataques. La falta de concientización y la desinformación en la materia produce que muchos atacantes opten por poner su foco en las personas en vez de las tecnologías, provocando que sean utilizados involuntariamente como medio para acceder ilegítimamente o causar un daño en los sistemas utilizados en el sector. Esto podría, además, impactar gravemente en otras áreas críticas, como la economía, el medio ambiente e incluso la salud de la población, debido al alto grado de dependencia que tienen con el sistema de transporte. Si bien escasean los estándares internacionales y específicos en cada modalidad o subsector, las organizaciones y los países están cooperando para compartir información, generar normas, recomendaciones, directivas y especificaciones técnicas que ayuden a fortalecer la ciberresiliencia. En este proceder se pone de manifiesto el hecho de que comprenden la gravedad de la temática y se encuentran expuestos a vulnerabilidades, amenazas y ataques. [3] Esto puede causar accidentes y congestión de tráfico, impacto en las cadenas de suministro, destruir, interrumpir o retrasar los movimientos de mercancías e inclusive, derivar en impacto ambiental, lesiones personales, muertes, consecuencias psicológicas, o generación de escenarios masivos de pánico. [8]

Tecnologías Utilizadas

Hoy en día, con el uso de sistemas de control operacional, los sistemas ferroviarios modernos tienen enclavamientos electrónicos, sistemas de señalización basados en radio y en el estándar de comunicaciones móviles GSM-R, desarrollado especialmente con infraestructuras de señalización altamente específicas que cuentan con un difícil acceso para los delincuentes cibernéticos. Pero estas tecnologías complejas funcionan integradas en las redes de comunicaciones de datos basadas en internet y por lo tanto se ejecutan en los servidores correspondientes como cualquier otra aplicación. Aquí es donde los expertos ven un riesgo de ataques e intervenciones de los usuarios no autorizados, lo cual no constituye sólo un peligro hipotético. Nextgov, el boletín gubernamental estadounidense de tecnología, publicó que un grupo desconocido podría haber manipulado señales ferroviarias en el noroeste de los Estados Unidos en diciembre de 2011. A pesar de que el incidente no tuvo un impacto dramático, reveló la vulnerabilidad de TI. [6] El sector ferroviario en la Unión Europea está migrando sus

servicios a la tecnología digital, incorporándola en procesos tales como la señalización, la venta de pasajes y la supervisión del suministro eléctrico de la red vial. Los principales sistemas que se utilizan son ventas, distribución y relaciones comerciales (compra de boletos o reserva de asiento), señalización (barreras, semáforos, etc.), comando y control (para el movimiento y frenado de trenes), telecomunicaciones (sistemas de radio, red, etc.), confort y servicios al pasajero (anuncios, iluminación, elevadores, etc.), servicios auxiliares (energía, luces de emergencia, etc.), seguridad y mantenimiento (control de acceso, video vigilancia, sistemas de reporte, etc.). Los sistemas utilizan las mismas redes, protocolos y activos digitales que las demás áreas, como, por ejemplo, sensores, cámaras de video y PC. A esto se suman los dispositivos que están intercomunicados a través del IioT (Internet industrial de las Cosas - *Industrial Internet of Things*). Además, usan GPS (Sistema de Posicionamiento Global), GPRS (Servicio General de Paquetes Vía Radio), GSM-R (Sistema Global de Comunicaciones Móviles para Ferrocarriles), según sea el caso. Por ejemplo, en Europa emplean el último al pertenecer al ERTMS (Sistema Europeo de Gestión del Tráfico Ferroviario) y en Estados Unidos, GPS al implementar PTC (Control Positivo de Tren - *Positive Train Control*). Por último, también utilizan SCADA (Supervisión, Control y Adquisición de Datos) para controlar sus sistemas críticos, desde el control del suministro eléctrico de los motores hasta la gestión del equipamiento de las estaciones como ascensores, escaleras mecánicas y ventilación. [3]

Actores

En el sector ferroviario, existen principalmente tres perfiles de actores/atacantes con diversas motivaciones: [3]

- **Ciberterroristas**: este tipo de actores poseen una motivación ideológica. Sus objetivos son destruir vidas humanas e infraestructuras con el fin de instaurar el terror. Por ello es imprescindible controlar sus acciones.
- **Hacktivistas**: motivados ideológicamente, sus objetivos no son letales e incluyen, por ejemplo, alteración de sitios web por *defacement (*cambia la apariencia visual), robo de información y filtración de datos. Utilizan los ataques de denegación de servicio, conocidos bajo la sigla “DoS” (*Denial of Service*) e infiltraciones en servidores web, entre otros.
- **Cibercriminales**: persiguen objetivos económicos. El transporte les atrae por dos motivos. En primer lugar, porque se trata de un sector con un alto perfil público y, en segundo lugar, debido a su importancia estratégica.

Según el informe de Thales [3] existen 12 grupos de atacantes activos (en distintas regiones/países) que operan contra el sector ferroviario. De éstos, 4 son considerados los más peligrosos. Concretamente, 3 están patrocinados por países: ATK4, ATK14 y ATK35 y el restante es un cibercriminal/hacktivista (ATK140). Ver ilustración siguiente:

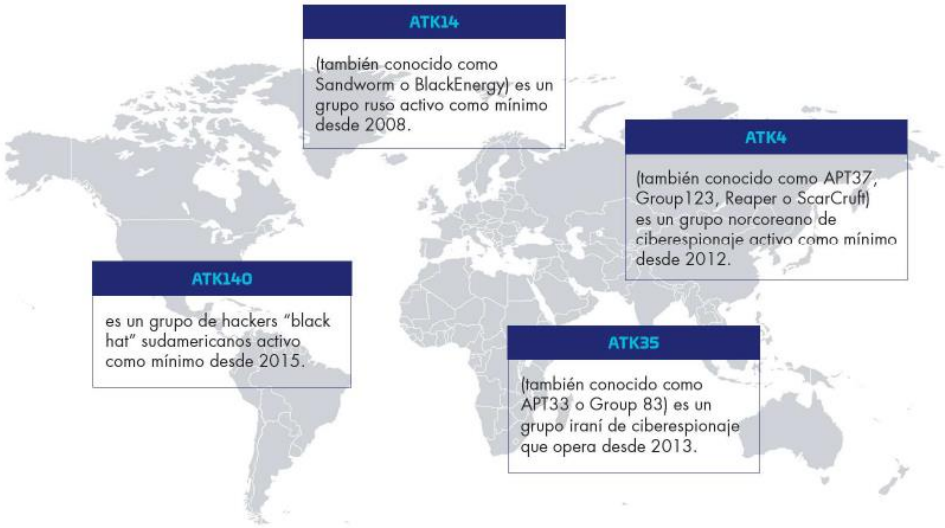

Figura 10 – Principales grupos de atacantes alrededor del mundo. [3]

Visión Global

Unión Europea

En noviembre del año 2020, ENISA (Agencia de la Unión Europea para la Ciberseguridad) emitió un informe sobre la ciberseguridad en el ferrocarril con el objetivo de evaluar el cumplimiento y las dificultades que presentan los estados miembros al implementar la directiva NIS (normativa de la Unión Europea). [3] Según dicho informe, las tendencias que se registran son las siguientes: [3]

- La implementación general de las medidas de seguridad en materia de gobernanza es heterogénea entre los distintos Estados miembros.
- Los OES (Operadores de Servicios Esenciales) maduros llevan aplicando las medidas de gobernanza desde hace mucho tiempo mientras que los restantes, recién comienzan a implementarlas.
- Las medidas básicas de ciberseguridad tales como la comunicación con las autoridades competentes y los equipos de respuesta a incidentes de seguridad informática parecen estar implementadas. Sin embargo, las que requieren experiencia técnica avanzada muestran un nivel más bajo de implementación, ya que es necesaria una considerable experiencia y madurez en ciberseguridad (por ejemplo, en correlación de registros y análisis).

Además, el informe menciona las principales dificultades y problemas que enfrenta el sector para cumplir con la directiva NIS: [3]

- Las partes interesadas en el ferrocarril dependen de proveedores con estándares técnicos y capacidades de ciberseguridad dispares, especialmente para tecnología operativa.
- Los sistemas TO para los ferrocarriles están obsoletos y suelen estar distribuidos por la red ferroviaria (estaciones, vías, etc.) lo cual dificulta alinearlos con los requisitos actuales de ciberseguridad, así como gestionarlos adecuadamente.
- Se observa una baja concientización digital y de ciberseguridad en el sector. En general, el nivel de sensibilización del personal sobre la necesidad de adoptar medidas de ciberseguridad sigue siendo baja.
- En cuanto a la transformación digital del sistema ferroviario, la mayoría de los OES ferroviarios están actualmente incorporando dispositivos conectados a internet (IoT). Estos dispositivos se incluyen en los sistemas, sin haber sido adecuadamente configurados, lo que generalmente está ligado a la aparición de nuevas vulnerabilidades.
- Existe un marcado riesgo en materia de ciberseguridad en la cadena de suministro, debido a que los OES dependen en gran medida de sus proveedores y/o terceros para actualizaciones del sistema, de la administración de parches y de la incorporación de nuevos componentes, entre otros.

Actualmente, ENISA junto a ERA (Agencia Ferroviaria de la Unión Europea) están trabajando de forma conjunta debido a que la Unión Europea destaca los beneficios del ferrocarril como medio de transporte, siendo sostenible, inteligente y seguro. Por lo tanto, la ciberseguridad es un requisito clave ya que permite que los servicios se desplieguen y se aprovechen las bondades de un paradigma digital conectado. En marzo del 2021, ambas agencias (por segundo año consecutivo) realizaron un Webinar donde debatieron sobre los últimos avances y desafíos en ciberseguridad que enfrenta el sector. Algunos temas tratados fueron los siguientes: [3]

- Desarrollo de políticas.
- Importancia del desarrollo de normas y certificaciones para el sector ferroviario.
- Formas de compartir información y cooperar para tener un sector ferroviario más ciberseguro en la Unión Europea.

La UIC (Unión Internacional de Ferrocarriles) realizó varios eventos y publicaciones para abordar temas de ciberseguridad en el sector ferroviario como, por ejemplo, una serie de directrices para la ciberseguridad en los ferrocarriles. Otra iniciativa es el proyecto

SAFETY4RAILS, que comenzó el 1° de octubre 2020 y está planificado a 2 años. Esta iniciativa busca proporcionar métodos y sistemas para aumentar la seguridad y la recuperación del transporte ferroviario interurbano. Su objetivo es aumentar la resiliencia, a través de la IA (Inteligencia Artificial) y herramientas automatizas de la infraestructura ferroviaria frente a amenazas, tanto de ciberseguridad como naturales. Para ello, ofrece un conjunto de herramientas que abordan la gestión del riesgo y de las crisis, la respuesta de las partes interesadas a incidentes y la recuperación del sistema. En julio del 2021 se publicó oficialmente la primera especificación técnica de ciberseguridad destinada al ferrocarril CLC/TS 5070118. La primera sigla se corresponde con CENELEC (Comité Europeo de Normalización Electrotécnica) y la segunda a *Technical Specification*. El objetivo de la especificación es garantizar que las características RAMS: Fiabilidad (*Reliability*), Disponibilidad (*Availability*), Mantenibilidad (*Maintianability*) y Seguridad (*Safety*) de los sistemas/ subsistemas/equipos ferroviarios no se puedan reducir, perder o comprometer en el caso de ciberataques intencionales. Este documento se aplica al dominio de las comunicaciones, la señalización y el procesamiento, el material rodante (unidades) y las instalaciones fijas. Proporciona a los interesados del sector como operadores ferroviarios y proveedores de productos, orientación y especificaciones sobre cómo se gestionará la ciberseguridad en el contexto del ciclo de vida de EN 50126-1 RAMS. Adicionalmente, esta norma ofrece una guía para que, en todas las etapas del ciclo, se apliquen los cinco atributos mencionados precedentemente. La prioridad y alcance del atributo correspondiente a la seguridad es que funcione sin fallos catastróficos, sin considerar ataques intencionales. De allí la utilidad de la CLC/TS 50701. [3] El TS ha sido aprobado por los 34 organismos nacionales de normalización miembros del CEN-CENELEC. El TS se ha desarrollado inicialmente para la industria europea, pero puede utilizarse como documento de referencia en otras partes del mundo. Sin embargo, no puede garantizarse que en otras partes del mundo no haya desarrollado también un documento equivalente". [3] Europa busca implementar un sistema ferroviario (ERTMS), en el que la señalización y las comunicaciones entre vía y equipos de a bordo sean compatibles en todo el continente y permita la interoperabilidad de las circulaciones ferroviarias entre los diversos estados de la Unión. Esto actualmente no es posible debido a las diferencias existentes en el ancho de las vías y en los sistemas tecnológicos, entre otros. Este sistema consta básicamente de dos tipos de tecnologías: Uno de ellos es el ETCS (*European Train Control System*) relacionado a la señalización (en infraestructura y en trenes), aportando datos sobre la velocidad máxima en cada

punto o distancia hasta la próxima baliza, así como el cálculo y la supervisión de la velocidad de circulación del tren en cada momento. [3].

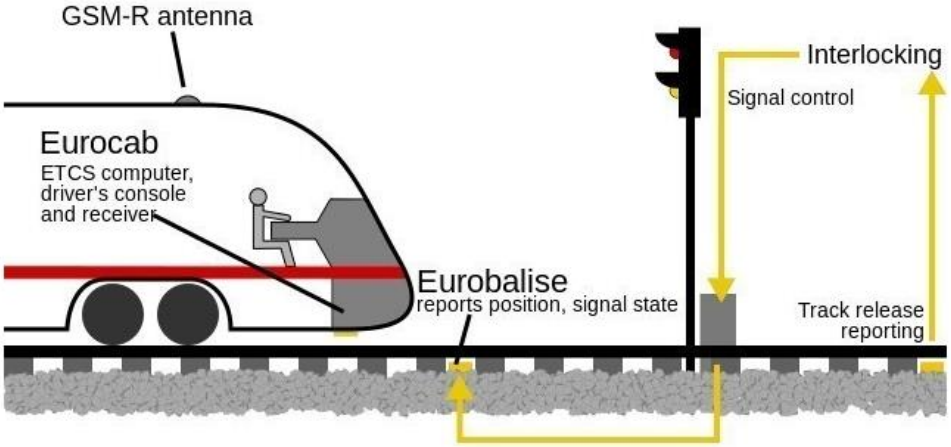

Figura 11 – Diagrama ETCS Nivel 1 [9]

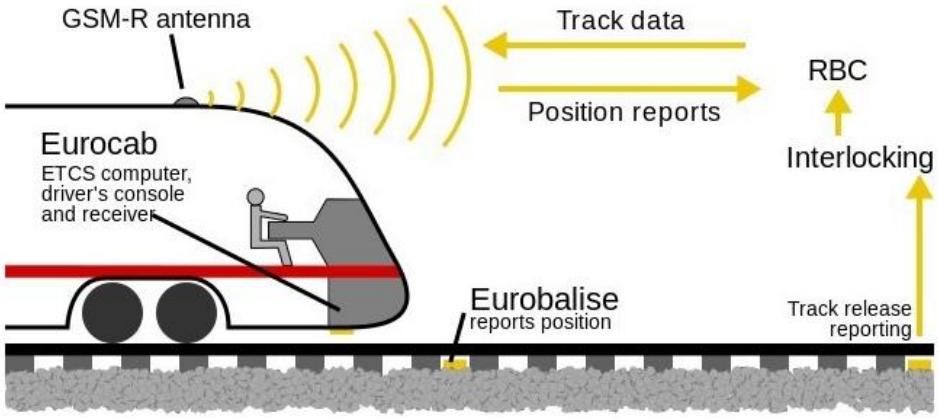

Figura 12 – Diagrama ETCS Nivel 2 [9]

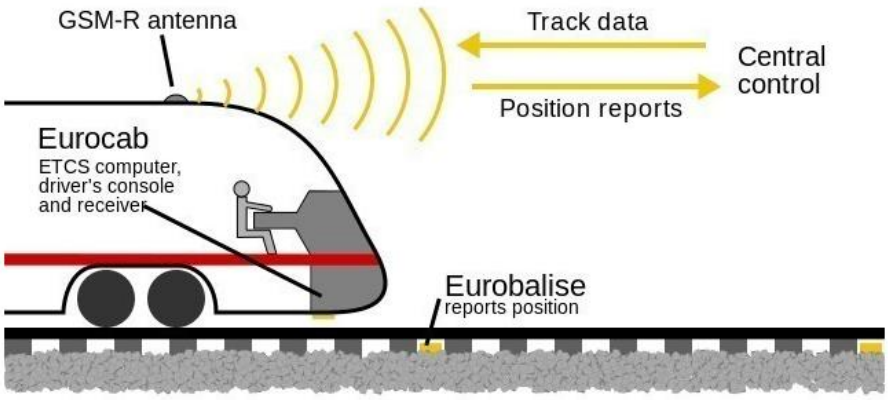

Figura 13 – Diagrama ETCS Nivel 3 [9]

El otro es el GSM-R (Sistema Global de Comunicaciones Móviles para Ferrocarriles) que regula aspectos relativos a las comunicaciones entre el tren y los operadores del CTC (Centro de Control de Tráfico) [3].

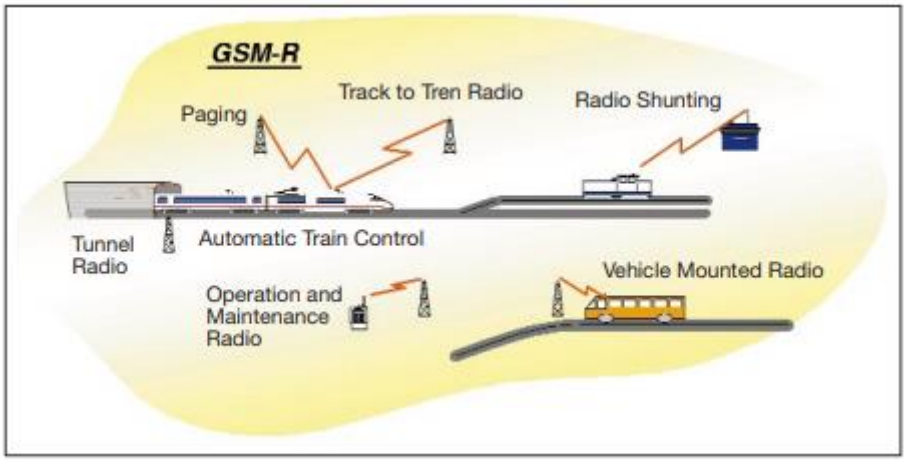

Figura 14 – Diagrama GSM-R [10]

Estados Unidos

El DHS (Departamento de Seguridad Nacional de los Estados Unidos) a partir del 31 de diciembre del 2021 exige a las entidades ferroviarias de mayor riesgo que informen incidentes cibernéticos al gobierno, identifiquen a los encargados de ciberseguridad y elaboren un plan de contingencia y recuperación en caso de que sean víctimas de ciberataques. La TSA (Administración de Seguridad en el Transporte) estableció mandatos de ciberseguridad a los sectores de transporte ferroviario a través de una directiva de seguridad publicada a fines de 2021. El DOT (Departamento de Transporte de los Estados Unidos) y la Administración Federal del Ferrocarril, redactaron en junio del 2020 un informe denominado “gestión de riesgos de ciberseguridad para ferrocarriles conectados” (*Cyber Security Risk Management for Connected Railroads*) en el que se desarrolla una metodología que permite identificar posibles amenazas, vulnerabilidades y consecuencias de ciberataques para cada caso. Incluso recomienda estrategias para mitigar riesgos. [3] Estados Unidos utiliza PTC, que consiste en un sistema de control para incrementar la seguridad de los trenes en todo el país y prevenir colisiones entre trenes y descarrilamientos provocados por exceso de velocidad y cambios de vía. Se trata de una tecnología basada en GPS que transmite material audiovisual que comunica las zonas conflictivas en el recorrido del tren. Entre ellas, avisa sobre señales cercanas y límites de velocidad. [3]

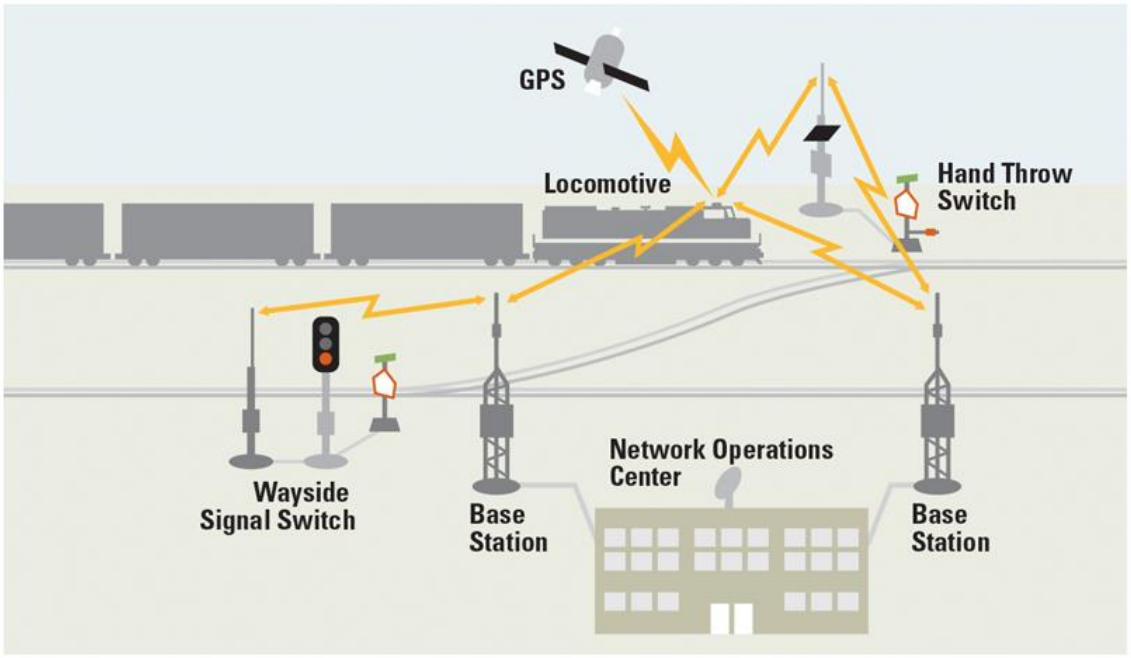

Figura 15 – Diagrama PTC [11]

Argentina

Argentina pasó una época donde el ferrocarril tuvo presencia y fortaleció el modelo productivo agroexportador de entonces, tanto en los puertos como en el interior del país. Aquel parque ferroviario lamentablemente sufrió un progresivo deterioro por falta de inversiones y mala administración, llegándose a clausurar muchas líneas en décadas pasadas. Hoy en día, en lo que respecta a tecnología, se encuentra lejos de lo esperado. A modo de ejemplo se puede mencionar el sistema de frenado, la señalización y la seguridad que aún se manejan a través de relés, motivo por lo cual, al ser puramente mecánico y no digital, se tienen en cuenta aspectos relacionadas a la seguridad física y el error humano (*safety*), pero se excluyen actos mal intencionados o de ciberseguridad (*security*). Asimismo, no cuentan con sistemas SCADA o tecnologías como las utilizadas en la Unión Europea (ERTMS) o los EEUU (PTC). Incorporar tecnologías como las que se utilizan en esos países sería, dada la coyuntura actual, una inversión muy costosa y difícil de implementar. [3] El sistema ferroviario utiliza GPS, cámaras e interfaces web y procesa y almacena un volumen importante de datos personales. [3]

Figura 16 – Diseño propio

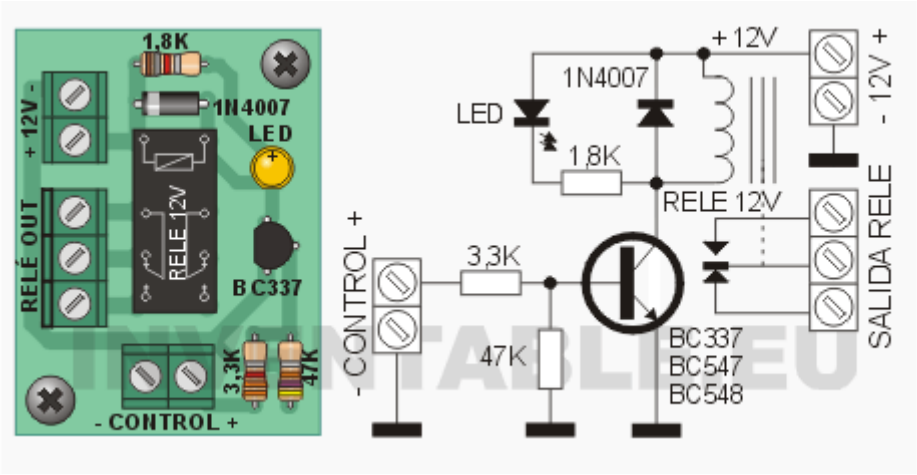

Figura 17 – Diagrama Relé con transistor [12]

No obstante, en lo que respecta a ciberseguridad, actualmente, Trenes Argentinos promueve una conducta responsable en esta materia mediante la implementación de varias iniciativas que se encuentran alineadas a las leyes/normas vigentes para organismos públicos. Entre estas normas, se encuentran las siguientes: [3]

- **Resolución N° 829/2019 de la Secretaría de Gobierno de Modernización:** que aprueba la Estrategia Nacional de Ciberseguridad, en cuya introducción se menciona al transporte en general.
- **Resolución N° 1523/2019 de la Secretaría de Gobierno de Modernización:** que aprueba la definición de CI y de CII, así como también la enumeración de los criterios de identificación y la determinación de los sectores alcanzados.

- **Decisión Administrativa N° 532/2021 de la Jefatura de Gabinete de Ministros**: relacionada con la implementación de acciones relativas a la ciberseguridad y a la protección de las CII, así como también a la generación de capacidades de prevención, detección, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078.
- **Disposición N° 1/2021 de la Dirección Nacional de Ciberseguridad:** con el objetivo de coordinar la gestión de incidentes de seguridad a nivel nacional y prestar asistencia en aquellos que afecten a las entidades y jurisdicciones del Sector Público Nacional y a las CII declaradas como tales.
- **Declaración Administrativa N° 641/2021 de la Jefatura de Gabinete de Ministros:** Establece los requisitos mínimos de seguridad de la información para organismos del Sector Público y la obligación de reportar los incidentes de seguridad para los organismos alcanzados por la normativa. Fue publicada en el Boletín Oficial el 25 de junio de 2021.

El intenso uso de las TIC conlleva un notable aumento de los riesgos y amenazas a los activos de información y a los sistemas esenciales utilizados para brindar de manera eficiente y constante los servicios que se prestan desde Trenes Argentinos y es por ello que están trabajando en el cumplimiento de las normativas antes mencionados, en pos del desarrollo de una cultura de ciberseguridad.

Infraestructura Crítica Ferroviaria

La mayoría de las CI, entendidas como aquellas que son esenciales para el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad, el bienestar económico o social de las personas, utilizan tecnologías de información y proveen servicios imprescindibles para la población. Una alteración del funcionamiento de esta infraestructura podría provocar graves consecuencias a la población y al Estado. [1] La red ferroviaria es considerada una de las industrias más críticas del mundo, ya que estas tienen el objetivo de ofrecer una experiencia segura y cómoda para los pasajeros. En el ferrocarril, como en todos los modos de transporte, el objetivo a proteger son las personas. Pero para ello hay que proteger, del mismo modo, los elementos por los que éstas discurren. Cuando se cita a la vía, también hay que considerar las instalaciones sobre las que éstas discurren, tales como puentes, viaductos, taludes, pasos subterráneos, saltos de carnero y toda una pléyade de obras

menores. Asimismo, hay que proteger los cerramientos cuando se trate de vías de alta velocidad; las instalaciones estratégicas a ella asociadas, tales como catenaria, semáforos, señales y, en general, todos los sistemas de seguridad en la circulación. También hay que proteger estaciones, sus accesos y salidas, incluidos los andenes y los vehículos estacionados, así como las instalaciones más alejadas como puedan ser talleres y bases de mantenimiento. En la República Argentina, cada día 3 millones de personas viajan en tren o subte y se moviliza el 5% del PBI por ferrocarril. Por esta razón es fundamental optimizar todas las áreas de la red ferroviaria para la implementación de la TI. [4]

Criticidad de la Industria

Según un informe realizado por VERTIV (Empresa líder en Soluciones Innovadoras de Continuidad Digital y Principal Proveedor de Infraestructura Digital Critica en el Mundo), el transporte colectivo (aéreo y ferroviario) se encuentra en el puesto número 2 según su criticidad. Casi todas las etapas del transporte aéreo, desde las reservas hasta el control del tráfico aéreo y los sistemas de control de vuelo, dependen en gran medida de la tecnología. Incluso una pequeña demora en un aeropuerto puede provocar un efecto dominó en toda la red y dejar a los pasajeros varados a cientos de kilómetros de sus destinos. El caos que puede surgir tras una interrupción del transporte aéreo fue evidente cuando una erupción volcánica en Islandia en 2010 dejó en tierra cientos de vuelos de todo el norte de Europa, lo que creó un efecto dominó en todo el sistema de transporte aéreo que mantuvo a miles de pasajeros varados durante días. El transporte ferroviario es similar al aéreo en cuanto a la repercusión de las caídas de las instalaciones, aunque suele estar más localizado y ser más inmediato. Esto causa mayor angustia y desorden social entre los viajeros que dependen del ferrocarril para viajar cortas distancias. La industria del transporte colectivo obtuvo una alta puntuación dado el impacto que cualquier tipo de disrupción puede ocasionar en la salud de los seres humanos y en el orden social, su efecto dominó sobre otros servicios y la repercusión pública. Al analizar qué aspectos convierten una industria en crítica, se identificaron 15 criterios que tienen en cuenta el impacto potencial de la pérdida de disponibilidad de los sistemas críticos, ponderados en base a la gravedad del impacto. Posteriormente, se utilizaron estos criterios para crear una definición de criticidad que un grupo de expertos en CI de VERTIV empleó para clasificar las industrias. Estos criterios son los siguientes: [7]

- Impacto de las caídas de las instalaciones sobre la salud de los seres humanos.

- Impacto financiero de las caídas de las instalaciones en términos de pérdida de ventas y de oportunidades.
- Orden social, el cual depende de la disponibilidad.
- Posible impacto medioambiental de las caídas de las instalaciones.
- Una parte significativa de la actividad, y los recursos de la empresa o las filiales afectadas depende de la disponibilidad.
- Costo de recuperación, incluidas reparaciones, sustituciones de activos afectados y medidas alternativas necesarias durante las caídas de las instalaciones.
- Inmediatez del impacto.
- Efecto dominó causado por las caídas de las instalaciones.
- Alcance (local, regional, nacional, mundial) probable de los efectos de las caídas de las instalaciones.
- Investigación subjetiva de la criticidad de la industria.
- Impacto del daño a la reputación causado por las caídas de las instalaciones en el mercado competitivo.
- Falta de disponibilidad, lo cual provoca frustración y angustia.
- Caídas de instalaciones, que conllevan el riesgo de una alta indignación pública o de los medios.
- Duración probable del impacto (sobre el funcionamiento, no sobre la reputación).
- Priorización de la disponibilidad según la industria.

Esto se debe a que, aunque el mundo creció de un modo cada vez más digital, aún seguimos dependiendo en gran medida de las industrias tradicionales, como los servicios públicos, el transporte colectivo y las telecomunicaciones, las cuales proporcionan los servicios cotidianos que nos permiten actuar en nuestras vidas personales y laborales. [7] Al mismo tiempo, la creciente digitalización creó interdependencias nunca vistas entre las industrias críticas. En casi todos los casos, las caídas de las instalaciones en una sola industria afectan a muchas otras. Por ejemplo, las interrupciones en la red eléctrica provocan un efecto dominó en todas las industrias; las demoras en el transporte aéreo o ferroviario interrumpen el comercio; y la caída de una co-ubicación se extiende a otras empresas e inhabilita el servicio de transmisión de video al que recurrimos para relajarnos tras un duro día de trabajo. Conforme se mantiene esta tendencia y emergen nuevas industrias esenciales, la CI que las respalda adquiere más importancia que nunca; y es por ello que estas industrias deben seguir invirtiendo en las tecnologías, procesos y servicios necesarios para mantener operativos

los sistemas críticos. Quizá nunca la humanidad será capaz de eliminar todos los desastres naturales o el error humano, pero con la planificación y la inversión adecuadas, será posible crear un mundo en el cual las tecnologías críticas siempre funcionan. [7] Es importante mencionar que todos los sistemas electrónicos para la seguridad vial de trenes y subtes tienen un costo muy elevado, siendo factores que limitan el mantenimiento y las actualizaciones. Esta situación ha favorecido que ocurran graves accidentes, aumentando la importación de sistemas de seguridad ferroviaria, lo que implica enormes gastos y depender de tecnología importada. El desarrollo de este tipo de sistemas es complejo por ser sistemas críticos que requieren el uso y seguimiento de una gran cantidad de normativas internacionales. En particular, los sistemas ferroviarios están compuestos por distintos componentes de software, hardware y humanos, que interactúan con su entorno de maneras muy variadas. Un fallo en uno de estos componentes o subsistemas puede llegar a tener asociados distintos niveles de peligros, pudiendo causar pérdidas financieras, daño al equipamiento, daños ambientales, lesiones a personas o en los peores casos pérdidas de vidas humanas. Por ello estos sistemas se encuentran regulados por distintas normativas cuyo fin es preservar la calidad y la seguridad operativa ferroviaria [4].

EVALUACIÓN DE RIESGO DE LA INDUSTRIA FERROVIARIA

Consideraciones de la Industria

A continuación, se mencionarán algunos aspectos relevantes de la industria ferroviaria que deben ser considerados en toda evaluación de riesgo de la industria.

Identificación de Activos

En el ferrocarril, como en todos los modos de transporte, el objetivo a proteger son las personas. Pero para ello hay que proteger, del mismo modo, los elementos por los que éstas discurren. Es decir, hay que considerar todas las instalaciones, tales como puentes, viaductos, taludes, pasos subterráneos, saltos de carnero y toda una pléyade de obras menores. Asimismo, es necesario asegurar los cerramientos cuando se trate de vías de alta velocidad; las instalaciones estratégicas a ella asociadas, tales como catenaria, semáforos, señales, y en general todos los sistemas de seguridad en la circulación. Así como también hay que proteger estaciones, sus accesos y salidas, incluidos los andenes y los vehículos estacionados, así como las instalaciones más alejadas como puedan ser talleres y bases de mantenimiento. En la República Argentina

la mayor parte del funcionamiento del sistema ferroviario es controlado en forma electromecánica mediante relés. Estos relés son considerados elementos críticos, al punto que, en la jerga, se denominan “relés vitales”, ya que su falla puede ocasionar graves accidentes. Asimismo, no cuentan con sistemas SCADA (acrónimo de *Supervisory Control And Data Acquisition,* se emplea para realizar un software que permite controlar y supervisar procesos industriales a distancia) ni con ninguna tecnología similar. No obstante, el sistema ferroviario utiliza GPS, cámaras e interfaces web y procesa y almacena un volumen importante de datos personales. Es por ello que alguien con mala intención puede sabotear o cometer actos terroristas que podrían afectar a una gran cantidad de personas.

Identificación de Amenazas

El aumento notable de la utilización de la tecnología ya mencionada incrementa enormemente la exposición a ciberataques. Si bien no hay registros a la fecha de eventos cibernéticos graves en sistemas críticos del sector ferroviario, se han producido problemas crecientes en áreas como la venta de pasajes, la comunicación a los pasajeros, la señalización y la video vigilancia. Los ciberataques no solo comprometen la seguridad, sino también causan perjuicios a la reputación de los operadores y tienen posibles implicaciones legales en el marco del RGPD (Reglamento General de Protección de Datos) de la Unión Europea, si se vulneraran los datos personales o sensibles de empleados y/o pasajeros. Uno de los principales desafíos para el sector ferroviario es que sus vulnerabilidades no pueden minimizarse o eliminarse fácilmente. Esto se debe a que los activos están muy dispersos, son heterogéneos y suelen tener una utilización que excede la vida útil recomendada por el fabricante. Esto dificulta el despliegue rápido de parches y el mantenimiento. Además de protegerse contra ataques externos, no deben descartarse tampoco los ataques internos. [3] Si bien hoy en la industria ferroviaria, tal como mencionamos anteriormente, no se cuenta con sistemas SCADA, es importante mencionar que varios sistemas industriales de este tipo ya han sido objeto de hackeo, con graves consecuencias sobre la operación que, en algunos casos, implicó riesgos contra la vida. Algunas de las razones para que esto haya ocurrido es que estos sistemas fueron diseñados en la década del 60 y operaban en ambientes aislados con tecnología propietaria. Por lo tanto, no fueron pensados para ser seguros a nivel informático. No obstante, con el advenimiento de internet comenzaron a compartir información con sistemas corporativos, lo cual provocó nuevos riesgos debido a que muchos emplean software de base y programas muy antiguos que carecen de las últimas actualizaciones de seguridad y en la mayoría de los casos, son

difíciles de actualizar. Además, estas redes necesitan controles adicionales y compensatorios para su protección, de modo de minimizar los riesgos a los que se exponen. También el informe muestra en una matriz las tácticas y técnicas más utilizadas para atacar el sector. Dicha matriz utiliza MITRE ATT&CK11 y describe las 12 tácticas que un atacante puede utilizar: acceso inicial, ejecución, persistencia, escalación de privilegios, evasión de defensa, acceso a credenciales, descubrimiento, movimiento lateral, colección, comando y control, ex filtración e impacto. Cada una de esas tácticas tiene entre 9 y 68 técnicas identificadas por MITRE para lograr esos pasos u objetivos. [3]

Escenarios de Ataque

A continuación, se describen dos escenarios posibles de ataque. El primero se denomina “Triton” y puede afectar a los sistemas SCADA del sector energético. El segundo refiere a cómo infectar objetos industriales como, por ejemplo, cámaras CCTV (Circuito Cerrado de Televisión) con el objetivo de tomar el control de un sistema. [3] Triton es un malware muy sofisticado y peligroso, elaborado para manipular sistemas de control industrial utilizados en CI. Se descubrió a finales de 2017, luego de provocar un apagón accidental de una planta petroquímica de Arabia Saudita. Se cree que este ataque fue perpetrado por el grupo ATK91, el cual estaría vinculado al gobierno ruso. Un ataque de este tipo en la infraestructura ferroviaria podría utilizarse para neutralizar/espiar las comunicaciones entre la MTU (Unidad Terminal Maestra) y el PLC (Controlador Lógico Programable) mediante un ataque de *man in the middle* (hombre en el medio). También es factible comprometer el PLC del sistema de control industrial o SCADA, tomando previamente el mando de la unidad maestra con el fin de enviar comandos legítimos pero dañinos. A pesar de que no existen indicios de este tipo de ataques, se estima que hay como mínimo 30 grupos que utilizan APT (Amenazas Persistentes Avanzadas), técnicamente capaces de realizarlo. [3]

El segundo escenario involucra a dispositivos periféricos y busca comprometer con un *malware* algún dispositivo accesible como, por ejemplo, una terminal dispensadora de pasajes o una cámara CCTV disponible en una estación o unidad de control ferroviario. Para ejemplificar el segundo escenario, imaginemos que en el ataque se utiliza el *malware* Mirai13, el cual una vez que infectó un equipo, escanea la red para conectarse a otros dispositivos vulnerables con el fin de controlarlos. Para ello, usa una tabla de contraseñas por defecto. Los dispositivos de bajo costo como cámaras y *routers*, ofrecen escasa seguridad nativa y utilizan protocolos y software muy conocidos por los desarrolladores y atacantes. Esto puede aprovecharse a través del alquiler de *botnets*

o de la contratación de ciberdelincuentes especializados. Cabe mencionar que las redes ferroviarias contienen miles de sensores accesibles y que suelen cubrir enormes áreas geográficas, lo cual dificulta su gestión en materia de seguridad física y lógica. Imaginemos que una cámara instalada para supervisar una estación de ferrocarril fue expuesta accidentalmente a internet. De este modo, a través del dispositivo se tiene acceso a los sistemas de TI y de TO de la empresa, ya que este periférico podría encontrarse afectado por cualquiera de las vulnerabilidades que se publican cada año en Internet. [3]Una vez que el atacante ha penetrado en la red de su víctima, puede: [3]

- Cortar la entrada de vídeo e incluso reproducir una falsa grabación.
- Espiar las comunicaciones, obtener información sobre el funcionamiento del sistema o interceptar datos de los clientes y/o empleados.

Como se explicó, las consecuencias pueden ser importantes y abarcar retrasos generalizados en los viajes, pérdidas económicas originadas en las demandas de rescate, robo/exposición de datos y daños a la reputación, por citar algunos. [3]

Ataques conocidos en el ámbito ferroviario

Los ataques terroristas contra los sistemas ferroviarios de San Petersburgo (Rusia), Tokio (Japón), Mad-hya Pradesh (India), Wurzburgo (Alemania), Madrid (España), Londres (Reino Unido) y Bombay (India) representan ejemplos de que los sistemas de transporte público son vulnerables a diferentes tipos de ataques. Los ataques pueden causar accidentes y congestión de tráfico, impacto en las cadenas de suministro, pueden destruir, interrumpir o retrasar los movimientos de mercancías y llegan a derivar en impacto ambiental, lesiones personales, muertes, impacto psicológico, o pánico. Históricamente, los trabajos de investigación han indicado que, entre las tácticas adoptadas para atacar sistemas de tren y metro, la forma preferida y más común es el uso de bombas, seguida de ataques armados, sabotajes e incendios. Por ejemplo, un ataque físico dirigido a cuatro líneas ferroviarias diferentes en la red francesa en 2008 mostró que acciones sutiles pueden causar incidentes graves. En dicho caso, barras de metal en las catenarias causaron retrasos en 160 TGVs, Eurostar y Thalys. Este método es tan solo un ejemplo de los ataques relativamente sencillos que pueden interrumpir el tráfico ferroviario, pero cuya probabilidad de éxito puede ser disminuida y, sus consecuencias, mitigadas. Existen ataques más sofisticados, y proyectos como SECRET que los han estudiado, concluyendo que, por ejemplo, es más probable que se provoque una perturbación de los intercambios de información entre trenes y centros de control con ataques electromagnéticos que la falsificación de los datos. Por otro lado, en la bibliografía y en los medios de comunicación se recogen numerosos ejemplos de

ataques cibernéticos recientes. Por ejemplo, en 2003 se culpó al virus informático Sobig de la parada del tráfico en 23 estados del Este de EE.UU. gestionados por la empresa CSX. En 2008, un adolescente fue capaz de descarrilar cuatro tranvías en Lodz (Polonia) usando un control remoto. En 2011, hackers atacaron ordenadores en el Noroeste de EE.UU. parando la señalización ferroviaria de *Pacific Northwest* durante dos días. En España, en 2013 se pusieron de manifiesto las deficiencias de seguridad de los sistemas de Renfe y del Metro Madrid, comprometiéndose las máquinas expendedoras de billetes, y accediéndose a terminales y a la red de cámaras de vigilancia. Es más, un atacante podía obtener el listado de tarjetas de crédito de los clientes, expedir un abono de transporte con tarifa de la tercera edad, y capturar y clonar las tarjetas de acceso RFID (permite determinar quién entra o sale de un local específico en un momento dado. Sistema automatizado que identifica a una persona, autentica sus datos y permite el acceso tras la verificación) del personal. Este último tema ha sido estudiado recientemente en sistemas de transporte y entornos IoT, dando lugar a una metodología para auditar la seguridad de dichos sistemas de acceso. Ya en 2015, Corea del Norte fue sospechoso de hackear un operador ferroviario de Seúl infestando docenas de terminales con *malware* durante meses. También ese año fueron expuestas vulnerabilidades en el controlador WinAC RTX del sistema de protección SIBAS que permitían controlar dispositivos sin autenticación. Además, cuatro grandes ataques cibernéticos en la red ferroviaria del Reino Unido fueron desvelados por una empresa de seguridad privada en 2016. [8]

Identificación de Vulnerabilidades

Las vulnerabilidades más relevantes del sistema ferroviario están relacionadas con debilidades en sistemas de control y señalización, sistemas de información, procedimientos del sistema, configuración y mantenimiento, desarrollo de software, la red de comunicaciones, y la de formación y sensibilización. [8] Asimismo, se considera que el acceso y los sistemas de control son los elementos más vulnerables. Efectivamente, casos como el de StuxNet demuestran que el equipamiento industrial indebidamente aislado puede convertirse en un riesgo. A ello se suma la complejidad de actualizar ese equipamiento cuando los elementos están geográficamente dispersos o se encuentran en sistemas embebidos. [8] El gráfico siguiente muestra las principales vulnerabilidades de los sistemas ferroviarios, en las cuales se pueden observar los distintos tipos de ataques y los dispositivos afectados:

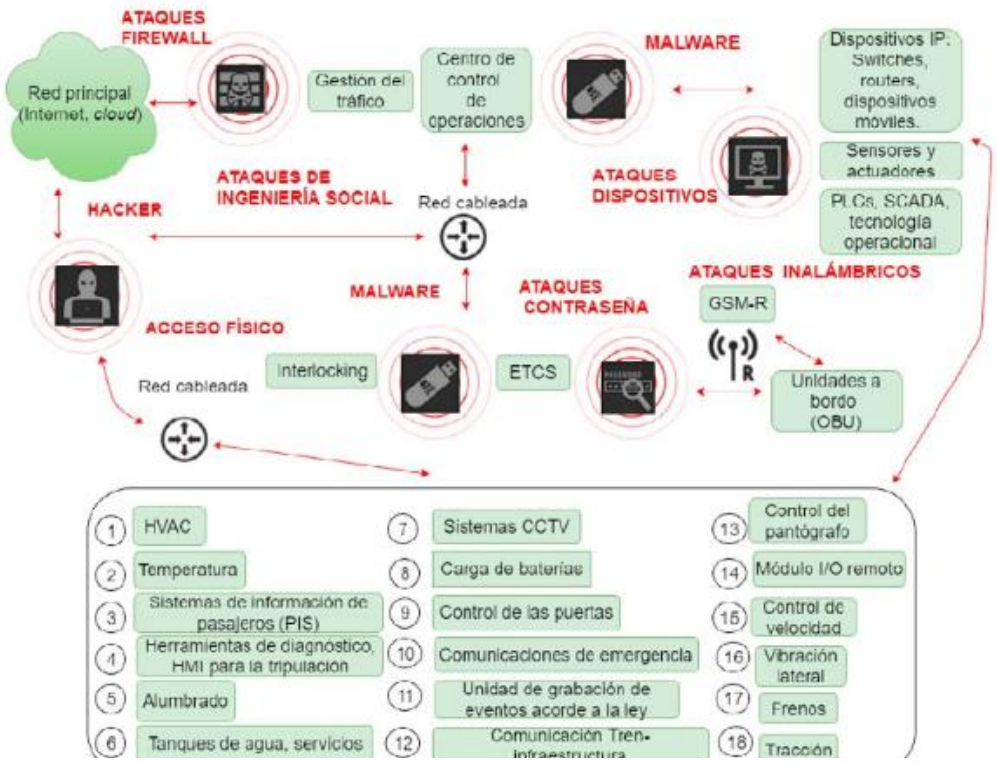

Figura 18 – Vulnerabilidades de los sistemas ferroviarios [8]

Los sistemas cibernéticos utilizados en las redes ferroviarias pueden estar sujetos a accesos no autorizados a través de diversos medios: remotamente, a través de internet o redes de comunicación no seguras; mediante el contacto directo con la infraestructura (por ej., a través de un puerto USB); y localmente, a través del acceso no autorizado a la infraestructura física o una amenaza interna (por ej., infiltración). [8] Los sistemas de enclavamiento basados en computadoras (CBI, *Computer-based Interlocking*) son sistemas de señalización diseñados para prevenir rutas conflictivas. En estos sistemas pueden producirse ataques cuando un actor malicioso tiene acceso físico al sistema o usa ingeniería social para engañar a alguien para acceder al sistema y ejecutar código malicioso (por ej., insertar un USB infectado). Un atacante puede tener como objetivo sistemas que conectan varios componentes del CBI o hacia el exterior. Algunas empresas como DB Netze (Alemania) proporcionan tarjetas SIM especiales con GSM-R que se usan para conectar trenes a centros de control, pero un atacante podría interferir en la conexión entre el tren y el centro de control con un *jammer* GSM. En concreto, dicho atacante podría parar los trenes automáticamente si la conexión entre el módem del tren y el centro de control se pierde en zonas donde se usa ETCS nivel 2 o 3. Dado que los sistemas ferroviarios están diseñados con un enfoque a prueba de

fallos, la interferencia de las señales conduciría a paradas, pero el fallo de las operaciones de comunicación puede causar muchos más problemas. Además, el uso cada vez mayor de WSN (*Wireless Sensor Networks*) y redes inalámbricas como base para la infraestructura de comunicaciones también plantea riesgos adicionales. [8] Por otro lado, ERTMS es vulnerable a *eavesdropping* (escuchas ilegales) y ataques tipo *replay* (en la cual una transmisión de datos válida es maliciosa o fraudulentamente repetida) debido a las debilidades de GSM-R, cuyo algoritmo de cifrado ha sido crackeado. Respecto a la integridad de los mensajes y la autenticación, ERTMS es vulnerable durante la distribución de claves que se requiere desde el KMC (*Key Management Center*) al ERTMS (de hecho, algunos aspectos del procedimiento implican el envío físico de claves por medios como un USB). Por otro lado, se hace uso de un algoritmo CBC-MAC (*Cipher Block Chaining-Message Authentication Code*) basado en el cifrado 3DES, el cual es vulnerable a ataques MitM (*Man-in-the-Middle*). Esto además introduce vulnerabilidades adicionales en la posterior derivación de las claves de sesión. [8] Los trenes en movimiento se comunican con un sistema de control ferroviario vía red GSM-R, que es básicamente GSM con todas sus características especiales incluyendo la clonación de SIM, la saturación, las actualizaciones de software, los comandos SMS (con un código PIN por defecto 1234), etc. Las credenciales por defecto, o incluso las credenciales cifradas están por aquí y por allá en las redes ferroviarias. Y por supuesto, todo está interconectado y suele estar conectado a internet. [5] Las características de gestión *over-the-air* presentes en algún equipamiento GSM-R también introducen riesgos de seguridad (i.e., actualizaciones de firmware). [8] Respecto a los módems GSM-R, se han detectado vulnerabilidades respecto a la ejecución de código remoto, como la falta de protección frente a *cross-site request forgery* (CSRF) (tipo de *exploit* malicioso de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía) o al cross-site scripting (XSS). (vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar) En el caso de módems con soporte SMS, los atacantes pueden leer los mensajes y enviarlos.[8] Otras vulnerabilidades detectadas permiten determinar la localización, interceptar y enviar peticiones USSD (*Unstructured Supplementary Service Data*), la lectura de tráfico HTTP y HTTPS reemplazando certificados SSL, o la existencia de puertos USB con la característica *autorun* activada, lo que permite a los ingenieros hacer actualizaciones de software y configuraciones fácilmente, pero que introduce riesgos. [8]

Controladores en los sistemas de automatización

Eurostar, un tren de alta velocidad que conecta Bruselas, Londres y París, es un buen ejemplo de lo complicadas que son estas cuestiones. La señalización, el control y la protección de los sistemas en este caso incluye a los sistemas belgas, franceses e ingleses con los que el tren debe ser compatible. Todos estos sistemas son de algún modo vulnerables. Por ejemplo, la versión moderna del sistema de automatización en los trenes Siemens (que son operados no solo por Deutsche Bahn, sino también por empresas que operan en España, Rusia, China y Japón) está basado en controladores Siemens WinAC RTX. Son básicamente ordenadores x86 con Windows que ya fueron protagonistas de la saga cibernética de Stuxnet. [5]

Enclavamiento de Señalización

Las vulnerabilidades también pueden encontrarse en los CBI, complejo sistema responsable de controlar los interruptores del ferrocarril. Por ejemplo, los modernos certificados de homologación para nuevos equipos utilizados en el procesador de seguridad en el sistema del metro de Londres, incluyen extraños requerimientos como Windows XP o incluso el *Service Pack* 6 de Windows NT 4.0 o superior, los cuales se encuentran obsoletos, sin soporte y por lo tanto vulnerables, por lo que su utilización no es recomendable. Otro problema con la seguridad de los sistemas informáticos de enclavamiento es que el software suele estar gestionado por un equipo que no cuenta con los conocimientos y experiencia suficientes y, por tanto, el proceso de autenticación que implementa y configura no es seguro e inclusive puede registrar fallas básicas como utilizar un *post-it* amarillo con el nombre de usuario y contraseña pegado a su computadora laboral. Si es hackeado, puede hacer volcar un vehículo de cientos de toneladas moviéndose a 100 km/h hacia otro gran transporte que se mueve a la misma velocidad en dirección opuesta, por citar un posible caso de dimensiones relevantes [5]

Pasos a Nivel (Uso de Relés para el Control y la Seguridad de los Sistemas)

En la República Argentina, la mayor parte del funcionamiento del sistema ferroviario es controlado en forma electromecánica mediante relés. Esto incluye, por ejemplo, el accionamiento automático de las barreras en los pasos a nivel o los sistemas de cambio de vía. En nuestro país hay alrededor de 1.000 dispositivos con estos accionamientos automáticos (pasos a nivel y sistemas de cambio de vía), cada uno de los cuales presenta características particulares, con entre 10 y 50 de estos relés. Si se considera

que cada relé tiene un precio de mercado de alrededor de 1.500 dólares y que la mayor parte de los relés instalados en Argentina ya ha cumplido su tiempo de vida, estimado en veinte años, se comprende la relevancia del problema, más aún si se considera que en muchos otros sistemas ferroviarios se utiliza este mismo tipo de relés, lo que eleva la cuenta total significativamente. Es importante mencionar que, si bien en la actualidad los sistemas electrónicos en muchos casos han reemplazado a los relés, en otros casos se siguen utilizando relés para el control y la seguridad de los sistemas ferroviarios. Por ejemplo, el subterráneo de la ciudad de Nueva York, uno de los más importantes del mundo, basa su funcionamiento casi exclusivamente en relés ferroviarios de seguridad. En parte esto se debe a que los sistemas basados en relés son simples de reparar incluso por operarios con conocimientos moderados, para lo cual sólo deben contar con herramientas básicas y un número acotado de modelos de relés. Esto implica un elevado nivel de mantenibilidad y disponibilidad. Por otra parte, los relés se siguen utilizando porque presentan un nivel de seguridad muy elevado, avalado por decenas de años de uso en los que no han presentado fallas significativas. Esto indica elevado rendimiento en términos de fiabilidad, disponibilidad y seguridad. [4]

Pasos a Nivel (Barreras Automáticas)

En la República Argentina hay 14.000 cruces ferroviarios con paso a nivel. De este total sólo 3% cuenta con un sistema automático de control de barreras, mientras que 7% es accionado manualmente y el 90% restante no cuenta con ningún tipo de barrera. Esta situación se debe principalmente al alto costo asociado a la instalación y mantenimiento de las barreras automáticas. Todos los equipos electrónicos para la seguridad vial en trenes y subtes son importados y muy costosos. Por ejemplo, una barrera automática instalada puede costar más de 100.000 dólares, debido a las exigentes normas de la serie EN5012X que debe certificar. [4] En Argentina no hay prácticamente instalados sistemas electrónicos que permitan detectar en forma automática la rotura de alguno de los brazos de la barrera o fallas en los sistemas electromecánicos de las barreras. Así, muchas veces, la detección de las fallas y problemas ocurre recién cuando se produce un accidente. [4]

Desarrollo de Aplicaciones

En la República Argentina los sistemas electrónicos para la seguridad vial de trenes y subtes son importados. Su costo muy elevado lo que dificulta el mantenimiento y actualización. Sin embargo, una falla en estos sistemas puede ocasionar distintos

niveles de peligro, pudiendo causar pérdidas financieras, daño al equipamiento, daños ambientales, lesiones a personas y en los peores casos, pérdida de vidas humanas.

Interfaces

En la actualidad, el estudio de las interfaces entre subsistemas es uno de los asuntos que requiere un mayor esfuerzo de análisis, por ser una de las principales fuentes de fallas e incidencias del sistema ferroviario actual. Uno de los motivos que favorecen la ocurrencia de fallas relacionadas con las interfaces es la dificultad para identificar las relaciones existentes entre los diversos subsistemas, pues en ocasiones dichas relaciones no son directas, requiriéndose complejos estudios en los que, habitualmente, es necesaria la colaboración entre diferentes profesionales y empresas.

Análisis de Consecuencias

Los ataques contra los sistemas ferroviarios como los que se mencionaron al inicio del trabajo son claros ejemplos que ilustran el hecho de que los sistemas de transporte público son, al día de hoy, vulnerables. Los ataques o incidentes pueden causar accidentes y congestión de tráfico, impacto en las cadenas de suministro o la destrucción o interrupción de los movimientos de mercancías o pueden producir daño medioambiental, lesiones personales, muertes o pánico. Reducir sus vulnerabilidades, tanto respecto a la infraestructura (por ejemplo, bolardos retráctiles, pilares estructuralmente reforzados) como a aumentar su resistencia a los ataques, es la principal tarea de cara a la protección del transporte. [8] Los ciberataques pueden clasificarse dependiendo del objetivo, la motivación y la capacidad de mitigación. La siguiente tabla presenta un resumen de los principales ciberataques, incluyendo nivel de riesgo. Este se representa como el producto de la probabilidad e impacto, considerando el conocimiento necesario para realizar el ataque y la capacidad de detección de acuerdo con la metodología de análisis de amenazas propuesta por la ETSI (Instituto Europeo de Normas de Telecomunicaciones). [8]

Tipo	Descripción	Técnicas de mitigación	Nivel de riesgo
Eavesdropping	Ataque pasivo realizado en redes con cables o inalámbricas no correctamente segmentadas. Recoge información para realizar futuros ataques más complejos.	Depende de la robustez de GSM-R.	Posible × Bajo = Menor
Denegación de servicio (DoS)	Ataques activos físicos (jamming).	Técnicas de espectro ensanchado o MIMO-OFDM.	Probable × Medio: forzar modo degradado, Crítico
DoS o Ataques distribuidos (DDoS)	Ataques activos lógicos (mensajes con retardo, en secuencia incorrecta, borrado), replay *flooding* attacks.	Protección adicional de ATP (*Automatic Train Protection*). ERTMS introduce timestamps para los mensajes, la confidencialidad depende del cifrado de GSM-R.	Posible × Medio: forzar modo degradado, Alto
Spoofing o robo de identidad	Ataques activos MitM. Inyección de paquetes en una red no autorizada, adoptando el rol de una entidad autorizada.	Autenticación e integridad, cifrado AES, deshabilitar carga del sistema con USB/CD.	Posible × Alto: conducción equivocada, Crítico
Ataques de ingeniería social	Engañar para acceder al sistema. Escalada de privilegios al obtener credenciales. Ejecución de malware.	No realizar entrega física del material. Formación en centros de capacitación de seguridad.	Posible × Medio: Medio
Infección de elementos de campo y equipamiento (dispositivos IP, sensores/actuadores, PLCs, SCADA)	Ataques activos que explotan las vulnerabilidades conocidas / desconocidas de los sistemas usando virus, detección de listas de control de acceso, malware o puertas traseras.	Software de protección (antivirus, cifrado) dificulta un alto rendimiento en tiempo real. Deshabilitar SNMP.	Probable × Medio: Alto

Figura 19 – Principales cibertataques [8]

Identificación de Controles

Las autoridades y la industria ferroviaria han puesto en marcha un número considerable de medidas y planes contra amenazas identificadas. Además, los operadores ferroviarios deben cumplir un conjunto de normas europeas (CENELEC EN 50126, EN 50128 y EN50129, entre otras) para satisfacer los requisitos de fiabilidad, disponibilidad, mantenibilidad y seguridad (RAMS) y normas internacionales para asegurar la seguridad de la información (por ejemplo, ISO 27001, NIST SP800-53 [14], ISA/IEC 62443 o APTA). [8] Si bien cada infraestructura y cada solución de seguridad es única, el cumplimiento de las regulaciones nacionales e internacionales de seguridad es necesario, como así también lo es realizar un análisis exhaustivo sobre cómo diseñar y proteger los sistemas de información. El proyecto europeo Cyrail (2016-2018), por ejemplo, persigue sentar las bases para mejorar el nivel de seguridad operacional del sistema ferroviario europeo. Por otro lado, es esencial desarrollar y mantener soluciones integradas y servicios de valor añadido, para proteger información sensible en cualquier momento dado. [8] El paradigma IoT habilita la posibilidad de introducir nuevas herramientas de monitorización que representan una forma productiva de detectar, analizar y reaccionar ante las amenazas, combinando todos los sistemas y herramientas basados en TIC en distintos módulos sobre una sola plataforma y pantalla. [8]

Una herramienta de monitorización debe seguir el flujo de datos de los sistemas ferroviarios internos y recopilar mediante sensores la información crítica de forma automática para pasarla a un operador que, en caso de un evento inesperado o ataque, pueda obtener inmediatamente la ubicación y el tipo de la alarma en la pantalla e iniciar las contramedidas planificadas. Por ejemplo, los problemas causados por la gran escala de las redes ferroviarias pueden abordarse mediante sistemas de monitorización y localización, políticas de control de tráfico, y sistemas de gestión de seguridad. [8] Las CI y las áreas pueden ser aseguradas mediante sistemas de control de acceso, alarmas y detección de intrusiones, sistemas de CCTV de imagen térmica, video-análisis inteligente, y otras tecnologías. Además, puede establecerse una comunicación continua con el personal y los pasajeros en las estaciones o trenes mediante sistemas PIS (*Passenger Information Systems*). La consciencia situacional (*situational awareness*) puede lograrse utilizando comunicaciones inalámbricas tren-estación y equipos de seguridad sobre el terreno. Sin embargo, no debe olvidarse que las intercomunicaciones, cámaras IP, puntos de acceso inalámbrico y demás nodos activos de la red deben ser *segurizados*. [8] Por otro lado, conviene mencionar que los centros de capacitación están estrechamente vinculados a las herramientas de monitorización. Durante los últimos años se ha confirmado que incluso los mejores sistemas reactivos fracasan en casos de emergencia real debido al personal inexperto, a planes de contingencia anticuados y a sistemas obsoletos. Esto no solo se refiere a los aspectos técnicos de una emergencia, sino también a las implicaciones legales y regulatorias. Los ejercicios asistidos por ordenador pueden ayudar a asegurar el funcionamiento operativo. Estas contramedidas pueden ser mejoradas mediante auditorías funcionales o la introducción de la gestión de crisis para minimizar los impactos operacionales, financieros y de imagen. Además, se pueden establecer perfiles de protección, canales de cooperación con las autoridades pertinentes o mecanismos de resiliencia (i.e., almacenar equipos para casos de emergencia). [8] Deben contemplarse servicios de ciberinteligencia con el objetivo de recopilar y analizar información que indique los puntos débiles, ataques planificados o cualquier otra actividad indeseada en la infraestructura TIC interna. Con este conocimiento, es posible desarrollar nuevas formas y reglas sobre los componentes de seguridad, y analizar sus resultados. Por otro lado, pueden incorporarse pruebas de penetración (*pentesting*) en las que se realizan ataques controlados para evaluar la robustez de la infraestructura de TIC y el cumplimiento de determinadas políticas de seguridad. [8] Respecto a las balizas, existen protecciones contra transmisiones erróneas y/o interferencias, pero no contra la suplantación o subversión de balizas. También debe garantizarse la autenticación para

la interlocución entre las balizas y el sistema general. [8] En cuanto a ERTMS, se recomienda la creación de un mecanismo criptográfico más robusto, de un nuevo esquema de distribución de claves, y de un nuevo módulo de integridad y almacenamiento de claves. En concreto, se recomienda el uso de criptografía simétrica con el algoritmo AES-CMAC con una clave de 128-bit para autenticación e integridad, y un cifrado asimétrico para el intercambio de claves y la negociación, usando un esquema basado en TLS (*Transport Layer Security*) y una infraestructura PKI (*Public Key Infrastructure*) con CA (*Certificate Authority*) federadas. [8] Existen diferentes esquemas para llevar a cabo comunicaciones seguras entre trenes, incluso para cuando se están atacando las comunicaciones GSM-R. En particular, el sistema propuesto incluye dos protocolos seguros de gestión de claves: uno para la creación de un canal autónomo con criptografía asimétrica y un segundo, simétrico, para canales cuasi autónomos. Ambos sistemas son ligeros en términos de computación y sobrecarga de comunicaciones. Además, el esquema presentado es compatible con otros sistemas de comunicación de transporte. Otras usan esquemas de actualización de clave que limitan el posible impacto de un ataque en la clave actual mediante una separación lógica de la actualización y el uso de la clave. [8]

Pasos a Nivel (Uso de Relés para el Control y la Seguridad de los Sistemas)

Las buenas prácticas ferroviarias y el sentido común indican que deben existir razones de peso para reemplazar los relés por sistemas electrónicos. Para poder ser utilizados en aplicaciones ferroviarias, los relés deben ser certificados de acuerdo a determinadas normas. En particular, Trenes Argentinos Sociedad del Estado solicitó en 2017 al Grupo de Investigación en Calidad y Seguridad de las Aplicaciones Ferroviarias (GICSAFe) dependiente del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) el desarrollo de un sistema electrónico para realizar el ensayo que permita validar que un relé es capaz de alcanzar la vida útil mecánica mínima de diez millones de ciclos sin carga, de acuerdo a lo indicado en el apartado 5.5.3 de la norma UNE-EN 50578, “Aplicaciones ferroviarias. Relés de señalización de corriente continua”. [4] Como resultado del trabajo se desarrolló un sistema automático para ensayos de ciclo de vida de relés ferroviarios de seguridad que se utilizarán en distintos proyectos para la empresa Trenes Argentinos. Este permite alinearse con las normas ferroviarias más importantes, como la serie UNE-EN 5012X, las ISO 9000 y las normas IPC referidas al diseño de hardware. Asimismo, mejora el diseño del hardware al aplicar la norma IPC 7351 y mejoras en el software al aplicar la norma UNE-EN 50128. Esta solución permite alcanzar adecuados niveles de fiabilidad, disponibilidad y mantenibilidad, mejorando

notablemente mediante la aplicación de normas de desarrollo de hardware y software. [4].

Desarrollo de Aplicaciones

Los sistemas se encuentran regulados por distintas leyes y normativas, como la ISO 9001 (Requisitos para un sistema de gestión de la calidad) y la EN 50126 (Aseguramiento de fiabilidad, disponibilidad, mantenibilidad y seguridad ferroviaria). Las características más importantes que se buscan reforzar son la fiabilidad, disponibilidad, mantenibilidad y seguridad (RAMS por sus siglas en inglés) de los sistemas ferroviarios durante todo su ciclo de vida. Algunos de los principales organismos que regulan esta actividad son el *Comité Européen de Normalisation Electrotechnique* (CENELEC) en Europa y la *International Electrotechnical Commission*(IEC) a nivel internacional. [4] Las principales normas propuestas por CENELEC orientadas a los sistemas ferroviarios son las siguientes: [4]

- **EN 50126**: Aplicaciones ferroviarias. La especificación y demostración de fiabilidad, disponibilidad, mantenibilidad y seguridad (RAMS). Está orientada al cumplimiento de las características RAMS del sistema en general.
- **EN 50128**: Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Software para sistemas de control y protección del ferrocarril. Se centra en la calidad de los aspectos software de los sistemas de ferrocarriles.
- **EN 50129**: Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos relacionados con la seguridad para la señalización. Aplica a los aspectos de calidad del hardware de los sistemas ferroviarios.

En la actualidad, para instrumentar estas buenas prácticas, organizaciones como la NASA, *Ansaldo Signal* o *Siemens Rail Transportation* utilizan una combinación de metodologías y formas de trabajo provenientes de distintos campos del conocimiento para lograr una sólida vinculación y para mejorar la calidad y seguridad de los sistemas críticos que desarrollan, dedicando tiempo, recursos y esfuerzo a esta tarea. [4]En primer lugar, es indispensable el desarrollo de procedimientos conforme la normativa EN 50126 y de un sistema de gestión de calidad basado en ISO 9001 que asegure la mejora continua de estos procedimientos. [4] A continuación, se presenta la metodología propuesta por el CONICET-GICSAFe para el desarrollo de aplicaciones críticas ferroviarias acorde a la normativa EN 50126. [4]

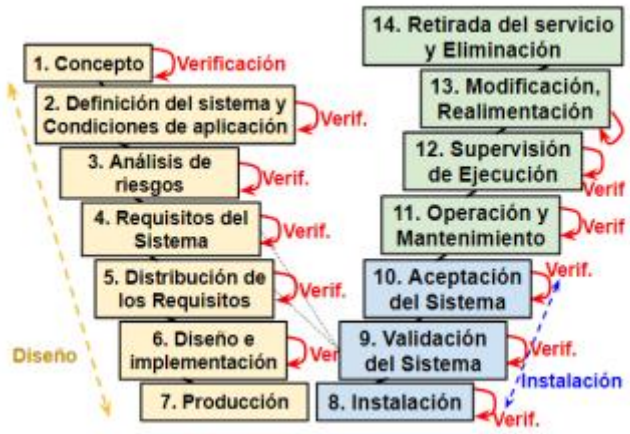

Figura 20 - Ciclo de vida del desarrollo de una aplicación ferroviaria sugerido por EN 50126 [4]

Interfaces

En función de los tipos de subsistemas que se relacionan, las interfaces se pueden clasificar de la siguiente forma:

- Interfaces entre distintos equipos de un mismo subsistema (por ejemplo, interfaz entre dos enclavamientos ferroviarios gestionados cada uno de ellos por distintos tecnólogos).
- Interfaces entre distintos subsistemas (por ejemplo, entre el subsistema de energía y el subsistema de comunicaciones, ambos constituyentes del sistema ferroviario).
- Interfaces entre distintos modos de transporte (este es el caso, por ejemplo, de las estaciones intermodales en las que ocasionalmente podrían interferir entre sí determinados equipos de comunicaciones, verse afectadas las vías de evacuación por la coexistencia de ambos modos de transporte, etc.).
- Interfaces entre los distintos modos de transporte con otros servicios públicos o privados (por ejemplo, líneas aéreas o ferroviarias que puedan afectar a equipamientos de hospitales, estaciones de comunicaciones, etc.).
- Interfaces entre los sistemas y equipos tecnológicos, con las personas que los diseñan, operan, mantienen e incluso, con los procedimientos que deben seguir las personas que tienen algún tipo de interacción con los distintos equipos. Probablemente este sea uno de los casos de más difícil estudio, debido a la complejidad derivada del estudio de los factores humanos y organizacionales.

De lo expuesto anteriormente se observa la necesidad del desarrollo de estudios específicos centrados en el análisis de las interfaces entre los distintos subsistemas a todos los niveles y que podrían dar lugar a fallas o ataques de ciberseguridad. Un primer

paso podría ser el desarrollo de una matriz genérica que identifique las distintas interacciones entre todos los subsistemas y sistemas que puedan relacionarse de una o de otra forma con el sistema ferroviario, de forma que pueda particularizarse para cada uno de los casos específicos que pudieran existir en las aplicaciones de dicho sistema. En dicha matriz deberían ponerse de manifiesto todas las posibles interacciones entre los distintos subsistemas, y entre estos con sistemas externos al ferroviario, así como una primera clasificación de su criticidad, atendiendo a criterios de seguridad y de disponibilidad. En el caso de la Interfaz con el factor humano, ésta se debería tratar de una forma distinta, pues resulta complicada su integración como un factor más dentro de dicha matriz, dado que, en este caso, el estudio de dichas interfaces es mucho más complejo al intervenir muchos más parámetros derivados de la propia complejidad del comportamiento humano que la mera consideración de los sistemas tecnológicos, como único factor. Para este caso, se debería desarrollar una metodología de estudio del factor humano de forma integrada con el estudio de seguridad de los correspondientes subsistemas, que pudiera ser utilizada en cada aplicación específica del sistema ferroviario.

Aplicación Metodológica

Teniendo en cuenta los conceptos adquiridos, se analizará a continuación la situación de la industria ferroviaria en Argentina. Para el presente estudio, se utilizó como base el estándar ISO/IEC 27005:2018 dado que es fácil de seguir y de acoplar con alguna de las diversas metodologías del mercado antes mencionadas (CRAMM, MAGERIT, OCTAVE, CORAS, etc.). Como ya se mencionó anteriormente, este estándar aplica un proceso secuencial en el que se debe tener en cuenta los siguientes aspectos para la gestión del riesgo: [2]

1. Establecimiento del contexto.
2. Evaluación del riesgo
    A. Identificación del riesgo.
    B. Estimación del riesgo.
    C. Evaluación del riesgo.
3. Tratamiento del riesgo.
4. Aceptación del riesgo.
5. Comunicación del riesgo.

Asimismo, se considera relevante complementar el estándar con la metodología MAGERIT por su concepto sencillo y eficaz a la hora de generar los requisitos mínimos

para la protección de la información. Esta es una metodología apropiada para las entidades que están iniciando su sistema de gestión de seguridad de la información ya que encamina los recursos y esfuerzos mediante la priorización de la resolución de los riesgos con mayor criticidad. Además, al estar en línea con el estándar de la ISO/IEC 27001:2022, se adecua perfectamente con su ciclo de mejora continua. Esta metodología contempla las siguientes actividades:

1.Identificar y valorar los activos de información de la Institución.

2.Identificar y valorar las amenazas a las que están expuestos estos activos de información.

3.Identificar las salvaguardas actuales con las que cuenta la organización.

4.Evaluar el impacto posible sobre los procesos de la organización, si es que alguna amenaza se materializa.

5.Informar a los encargados y proponer un Plan de Mejora para una buena gestión de los riesgos y tomar decisiones con motivos justificados.

Objetivo

Evaluar los riesgos a los que están expuestos los activos de información de la industria ferroviaria y los impactos que generaría la materialización de una amenaza.

Caso de Estudio

Establecimiento del Contexto.

Entender el Negocio

En primera instancia, se procede a relevar la actividad de la organización del caso de estudio. Se trata de la Operadora Ferroviaria del Estado, la cual fue creada por el Artículo 7º de la Ley Nº 26.352 (Reordenamiento Ferroviario), contribuyendo a la integración territorial en el marco del Sistema Multimodal de Transporte. En forma directa, Trenes Argentinos gestiona las líneas urbanas de pasajeros Sarmiento, Mitre, San Martín, Roca, Belgrano Sur y Tren de la Costa; los servicios regionales de Entre Ríos, Salta, Chaco, Neuquén y Córdoba; y los servicios de larga distancia Buenos Aires - Mar del Plata, Buenos Aires - Córdoba, Buenos Aires - Rosario, Buenos Aires - Bahía Blanca, Buenos Aires - Junín, Buenos Aires - Bragado y Buenos Aires - Tucumán. Asimismo, mantiene un acuerdo operativo con la empresa Casimiro Zbikoski para la prestación del servicio Posadas - Encarnación. [16]

A continuación, se presenta su misión, visión y valores:

Misión

- Consolidar y fortalecer el desarrollo y transferencia del conocimiento y cultura ferroviaria en los recursos humanos y técnicos que componen el sistema ferroviario nacional, como así también en los que se integren en el futuro. [16]
- Incorporar nuevas tecnologías y modalidades de gestión que contribuyan al mejoramiento de la prestación del servicio ferroviario en todo el territorio nacional. [16]
- Establecer y generar los vínculos científico-tecnológicos, mediante acuerdos de cooperación a nivel nacional e internacional, que permitan perfeccionar, consolidar y fortalecer el estado de conocimiento ferroviario. [16]
- Continuar con la preservación y difusión del patrimonio histórico documental ferroviario, a través de la guarda y protección del archivo, procesamiento de datos e información histórica. [16]
- Prestar los servicios de administración y gestión de los recursos humanos a aquellas empresas que se encuentren en estado de transformación, liquidación y/o que los accionistas indiquen en el futuro. [16]

Visión

- Lograr el más alto estándar de entrenamiento técnico y profesional, como un desarrollo integral del capital humano ferroviario, aprovechando la tecnología y conocimientos disponibles a nivel nacional e internacional, a través de la generación de procesos de formación que permitan prestar servicios tanto a actores públicos como privados, siendo una institución de referencia en la materia. [16]

Valores

- Confiabilidad.
- Creatividad e Innovación.
- Compromiso.
- Profesionalismo.
- Respeto y Reconocimiento

Organigrama

La organización está estructurada en las siguientes Gerencias Generales:

- Gerencia General de Asuntos Jurídicos
- Gerencia General Administrativo
- Gerencia General Compras, Abastecimiento y Logística
- Gerencia General de Recursos Humanos
- Gerencia General Desarrollo Comercial
- Gerencia General Operativo

A continuación, se presenta el organigrama correspondiente:

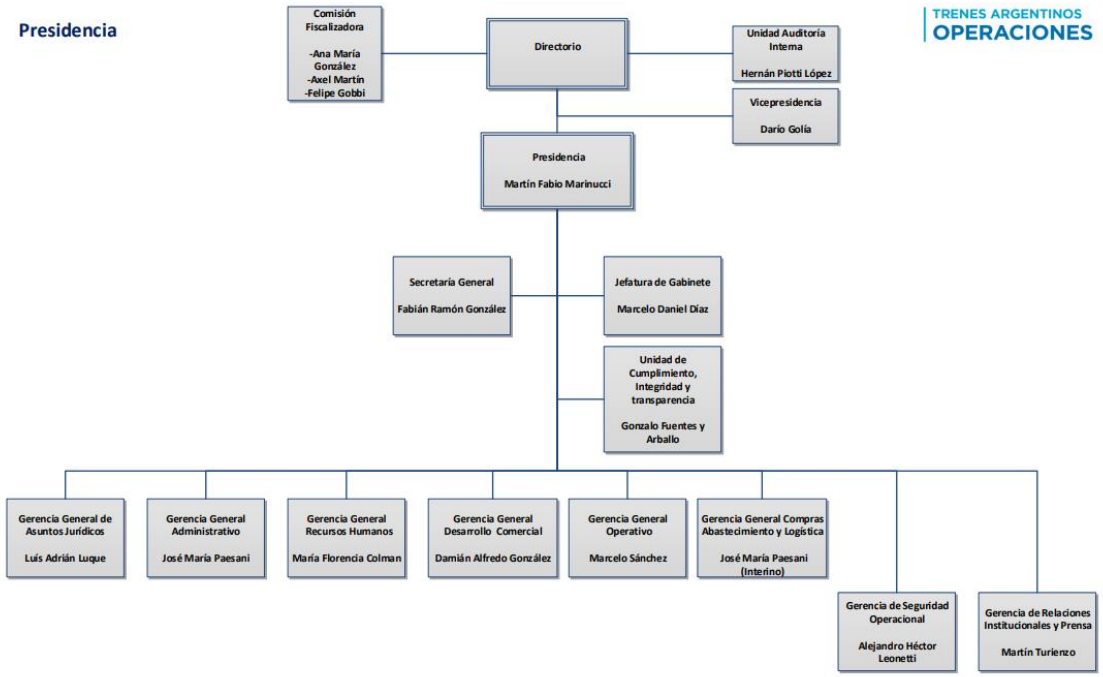

Figura 21 – Organigrama de Trenes Argentinos [16]

Todas las áreas del negocio dependen en gran medida de los sistemas computadorizados para el funcionamiento del tren, la entrega de productos, procesamiento de transacciones, contabilidad y preparación de informes sobre información gerencial.

La organización administra:

- 5 líneas en el Área Metropolitana de Buenos Aires - AMBA
- 9 servicios Larga Distancia
- 7 servicios Regionales
- 116 partidos, alcanzados en 13 provincias, cubriendo una población de 26 millones de habitantes.
- 182 millones de pasajeros transportados en 2021

- 161 millones de pasajeros transportados en 2022 (Hasta julio inclusive)
- 407 estaciones
- 4.623 km de vías por las que circulan nuestros servicios
- 24.180 empleados

Respecto a los aspectos tecnológicos, se estructuran 2 áreas tecnológicas:

- La gerencia de Tecnología de la Información, Innovación y Telecomunicaciones abocada a la operación, dependiente de la Gerencia General de Operaciones
- La gerencia de Sistemas y Procesos abocada a la gestión (*Back Office)*, dependiente de la Gerencia General Administrativa

Definir el Universo de Activos Informáticos

En el ferrocarril, el objetivo a proteger en primer lugar, son las personas y es por ello que para hacer una adecuada evaluación de riesgo se debería de contemplar todos los elementos por los que las personas transitan (puentes, viaductos, cerramientos, catenaria, semáforos, señales, estaciones, accesos y salidas, talleres, bases de mantenimiento, etc.). Sin embargo, teniendo en cuenta las dimensiones de la organización se acotará a sus principales aplicaciones, las cuales se encuentran distribuidas en 5 centros de procesamiento de datos, 3 internos para la gestión del *Front Office* y 2 externos para el *Back Office*. Las aplicaciones analizadas se detallan en el anexo I.

Evaluación del Riesgo

Para la evaluación de riesgo se utilizó un análisis cualitativo dado que no se persigue ningún fin lucrativo y la información fue obtenida a través de entrevistas y cuestionarios, aplicados a los responsables de cada área.

Valoración de los Activos

Esta tarea tiene como objetivo identificar la dimensión en la que resulta valioso el activo para la organización. Para ello se consideraron las siguientes dimensiones respecto a los datos:

- Disponibilidad
- Integridad
- Confidencialidad

En base a ello se ponderaron los valores a fin de determinar el impacto que podría ocasionar en la organización. A continuación, se presentan los niveles considerados junto a una breve descripción del concepto.

Nivel de Confidencialidad	Valor	Nombre	Descripción
NC MB	0	Nivel de confidencialidad muy bajo.	La información es pública/no es importante
NC B	1	Nivel de confidencialidad bajo.	Información Interna
NC M	2	Nivel de confidencialidad medio	De hacerse pública se ve comprometidas ventajas competitivas o un atacante puede utilizarla para comprometer activos relevantes de la organización (ejemplo contratos/ inventario)
NC A	3	Nivel de confidencialidad alto.	De hacerse pública la información dañaría la imagen y se sufriría una pérdida de confianza. información muy relevante para el proceso datos personales
NC C	4	Nivel de confidencialidad crítico.	Se maneja información sensible para el negocio como ser sueldos o datos médicos

Nivel de Integridad	Valor	Nombre	Descripción
NI MB	0	Nivel de integridad muy bajo.	El proceso de negocio no se ve afectado
NI B	1	Nivel de integridad bajo.	La falla puede afectar a procesos de soporte
NI M	2	Nivel de integridad medio	Se producen errores que afecta al proceso de negocio ligeramente, ocurren errores en el proceso y se requiere re trabajo
NI A	3	Nivel de integridad alto.	Se produce relentización de actividades, mal funcionamiento del servicio, se ve afectado severamente al proceso de negocio, podrían existir errores graves en la entrega del servicio
NI C	4	Nivel de integridad crítico.	El servicio no puede funcionar/ser entregado. La imagen de la empresa se ve afectada (calidad del servicio).

Nivel de Disponibilidad	Valor	Nombre	Descripción
ND B	0	Nivel de disponibilidad muy bajo.	El proceso de negocio no se ve afectado

Nivel de Disponibilidad	Valor	Nombre	Descripción
ND M	1	Nivel de disponibilidad medio.	El proceso de negocio afecta a algunos usuarios que ven el servicio interrumpido. (al menos 500 usuarios) La falla afecta a las tareas del usuario
ND A	2	Nivel de disponibilidad alto.	El servicio no puede funcionar o ser entregado. La imagen de la gerencia se ve afectada, hay impacto en los usuarios que se quejan con sus Gerentes Generales por la mala calidad del servicio.

Se aplicó la siguiente tabla para obtener el nivel de impacto asociado

Nivel Impacto	Valor Impacto
Critico	10
Mayor	8
Medio	6
Menor	4
Despreciable	2

Caracterización de las Amenazas y de los Salvaguardas

El objetivo de esta actividad es identificar las posibles amenazas que se pueden materializar sobre los activos y las salvaguardas que presenta la organización para mitigar el riesgo de modo estimar la frecuencia de ocurrencia, es decir la probabilidad de ataque. Las amenazas están clasificadas en cuatro grupos:

- Desastres naturales
- De origen industrial
- Errores y fallas no intencionados
- Ataques deliberados

Las salvaguardas son medidas, procedimientos o mecanismos que reducen el riesgo de la materialización de una amenaza. Es por ello que, para poder ponderar las probabilidades de ataque, se utilizó el siguiente criterio:

Probabilidad de Ataque	Valor Probabilidad	Características
Probable	0,9	Ausencia de un Marco de Control a Nivel Entidad: - Ausencia de políticas, estándares y procedimientos - Ciertos de controles a nivel Infraestructura (Base de Datos, Sistema Operativo, Red) - Ausencia de controles a nivel ITGC (Desarrollo de Sistemas,

Probabilidad de Ataque	Valor Probabilidad	Características
		Acceso lógico, Acceso Físico, Soporte, Backup&Restore, Seguridad) - Ausencia de controles a nivel Aplicación (Autorización, SA [Acceso sensitivo], SOD [Segregación de funciones], etc.)
Bastante común	0,7	Marco débil de Control a Nivel Entidad: - Ausencia o debilidad de políticas, estándares y procedimientos - Ausencia o debilidad de ciertos de controles a nivel Infraestructura (Base de Datos, Sistema Operativo, Red) - Ausencia o debilidad de ciertos de controles a nivel ITGC (Desarrollo de Sistemas, Acceso lógico, Acceso Físico, Soporte, Backup&Restore, Seguridad) - Ausencia de controles a nivel aplicación (Autorización, SA, SOD, etc.)
Improbable	0,5	Marco Regular de Control: - Ausencia de documentación de algunas políticas, estándares y procedimientos - Cumplimiento de los estándares y procedimientos definidos - Controles claves a nivel Infraestructura (Base de Datos, Sistema Operativo, Red) - Controles claves a nivel ITGC (Desarrollo de Sistemas, Acceso lógico, Acceso Físico, Soporte, Backup&Restore, Seguridad) - Ciertos controles a nivel Aplicación (Autorización, SA, SOD, etc.)
Inusual	0,3	Razonable Marco de Control: - Documentación de algunas políticas, estándares y procedimientos - Cumplimiento de los estándares y procedimientos definidos - Controles claves a nivel Infraestructura (Base de Datos, Sistema Operativo, Red) - Controles claves a nivel ITGC (Desarrollo de Sistemas, Acceso lógico, Acceso Físico, Soporte, Backup&Restore, Seguridad) - Controles claves a nivel Aplicación (Autorización, SA, SOD, etc.)
Raro	0,1	Adecuado Marco de Control: - Validación periódica de las políticas, estándares y procedimientos - Validación periódica del cumplimiento de los estándares y procedimientos definidos - Validación periódica del cumplimiento de los Controles claves a nivel Infraestructura (Base de Datos, Sistema Operativo, Red) - Validación periódica del cumplimiento de los Controles claves a nivel ITGC (Desarrollo de Sistemas, Acceso lógico, Acceso Físico, Soporte, Backup&Restore, Seguridad) - Validación periódica del cumplimiento de los Controles claves a nivel Aplicación (Autorización, SA, SOD, etc.)

Finalmente se ponderó el riesgo teniendo en cuenta el impacto financiero y en la sociedad que ocasionaría la materialización de dichas amenazas mediante tres niveles: Bajo, Medio y Alto.

Como resultado de dicho análisis se obtuvo la siguiente matriz de riesgo, en la que los números representan la cantidad de riesgos identificados y los colores, su criticidad:

Figura 22 – Matriz de Riesgo Valorada

Los criterios de la valoración empleada y el detalle del análisis realizado, se detallan en el anexo I.

CONCLUSION

A lo largo del presente trabajo se han descripto las CII como aquellos sistemas y servicios de TIC y de operación que soportan infraestructuras esenciales para el desarrollo de la sociedad y contribuyen a garantizar el normal funcionamiento de los servicios prestados por los estados. Todas estas infraestructuras tienen la particularidad

de mostrar que una disrupción en su seguridad tiene el potencial de impactar directamente en la sociedad en su conjunto o en una parte significativa de ella. Asimismo, se ha resaltado la criticidad del ferrocarril en su función de integración y comunicación entre los sectores productivos, sociales y territoriales y al permitir el desenvolvimiento de todas las actividades de un país, así como la integración regional; alcanzar los objetivos de sostenibilidad ambiental y constituirse en una pieza clave del sistema de transporte para asegurar la movilidad de los habitantes de nuestro país. Como otras modalidades del transporte, la industria ferroviaria se encuentra expuesta a riesgos de seguridad que deben ser tratados y requieren la adopción de adecuadas medidas de protección para su mitigación.

Por ello, el uso de una metodología de evaluación de riesgos es de gran utilidad dado que permite contar con pasos definidos en detalle, con documentación precisa, con herramientas e infraestructuras alineadas y con una identificación clara de las amenazas, lo que permitirá definir controles precisos. Además, facilita el accionar de las organizaciones en cuanto a la toma de decisiones frente a entornos sumamente cambiantes. El estándar ISO/IEC 27005:2018 y esperablemente, su versión 2022, establece un proceso de análisis y gestión de riesgo integral, sin dejar de lado aspectos relevantes como la comunicación, el seguimiento y la mejora continua. Como se explicó, este estándar puede complementarse con el uso de las metodologías descriptas en el trabajo para facilitar su implementación mediante la descripción de procedimientos específicos para las acciones a ejecutar.

Como resultado del presente trabajo, se ha observado cómo la Gestión de Riesgos cumple un rol preponderante en las organizaciones dado que les permite hacer una identificación clara de sus activos más importantes, valorarlos según los riesgos asociados y en base a ello, disponer de una visión integral de las amenazas y vulnerabilidades que pueden afectar de forma más grave la prestación de sus servicios. Asimismo, al complementarlo con ciertas metodologías, como por ejemplo Margerit, habilita el despliegue de una serie de pasos estructurados para todo el proceso de análisis de riesgos, identificación y valoración de los activos, determinación de las amenazas, conocimiento de las salvaguardas actuales y asistencia en la implementación de los futuros controles para monitorear y mitigar los riesgos encontrados. Todo esto teniendo en cuenta los factores de seguridad y criticidad de los activos para la creación de normativas de seguridad, tanto para los recursos informáticos, como para sus empleados y usuarios.

En el caso de estudio, se han evaluado los riesgos del subsector de transporte ferroviario y se han presentado aquellos a los que se encuentra expuesto el sistema.

Del análisis efectuado se observa que, en Argentina, la industria ha desarrollado estrategias, políticas y planes específicos para el sector administrativo (*Back Office*) pero no así en la parte operativa (*Front Office*). Esta situación puede deberse a que la parte administrativa se encuentra más regulada por auditorías externas e internas, las cuales no suelen hacer foco en los aspectos operativos. En nuestro país, la Sindicatura General de la Nación de la República Argentina – SIGEN es el órgano rector del sistema de control interno que coordina actividades orientadas a verificar que la gestión del sector público nacional alcance los objetivos de gobierno. Considerando la importancia que tiene la industria ferroviaria, como ya se mencionó, sería conveniente que esta entidad pueda incorporar dentro de su planificación además de los aspectos administrativos, cuestiones relacionadas con la seguridad la faceta tecnológica de la infraestructura critica.

Asimismo, resulta imprescindible la incorporación de tecnología y dispositivos que mejoren la ciberseguridad, el desarrollo de planes de contingencia adecuados, la utilización de sistemas de monitorización IoT que reduzcan las vulnerabilidades de la infraestructura, el uso de servicios de ciberinteligencia y pentesting y la introducción de criptografía más robusta y de protocolos de gestión de claves seguros para GSM-R/ERTMS. Por ello, es importante iniciar un proceso virtuoso en el cual se impulse una articulación y colaboración entre los distintos subsectores del transporte, con organizaciones gubernamentales nacionales y entidades internacionales como la UIC (Unión Internacional de Ferrocarriles), la ERA (Agencia Ferroviaria de la Unión Europea), el TSA (Administración de Seguridad en el Transporte), el DOT (Departamento de Transporte de los Estados Unidos) y la Administración Federal del Ferrocarril, para compartir experiencias, buenas prácticas, recomendaciones y para la creación de estándares y especificaciones, así como la realización de encuentros periódicos, foros y mesas de trabajo con grupos de expertos.

Todos los subsectores o modalidades del transporte moderno alrededor del mundo se encuentran expuestas a vulnerabilidades en materia de ciberseguridad. Por ello, resulta evidente que se requerirán capacitaciones y recomendaciones a alto nivel, así como estándares internacionales y medidas de cumplimiento obligatorias específicas para cada caso. Estas medidas requerirán una constante revisión y adaptación debido al impacto social, ambiental y humano de los incidentes, al incremento de la digitalización y a la evolución del panorama de riesgos a los cuales, Argentina se encontrará inevitablemente expuesta.

En los últimos años nuestro país ha elaborado y publicado un conjunto escaso pero relevante de normas destinadas a mejorar la ciberseguridad. Entre ellas, puede citarse

una Estrategia Nacional de Ciberseguridad, que a la fecha se encuentra en revisión, la cual incluye entre sus objetivos la protección de las CII del país.

En el mismo sentido, se elaboraron y aprobaron una serie de requisitos mínimos de seguridad para organismos de la Administración Pública Nacional para la protección de las Infraestructuras que respaldan servicios críticos. Lamentablemente, Trenes Argentinos, si bien forma parte del Sector Público Nacional no se encuentra alcanzado por dicha normativa. En consiguiente, no está obligado a cumplir con las medidas de seguridad mínimas requeridas, como, por ejemplo, disponer de una Política de Seguridad como base para la adopción de las medidas necesarias para fortalecer la ciberseguridad en su ámbito.

Como conclusión final, es evidente que aún hay mucho camino por recorrer, en términos de adecuación a las normativas aplicables al ferrocarril, el desarrollo de un plan de acción para implementar las buenas prácticas que resulten adecuadas y la implementación de un proceso virtuoso de gestión de riesgos. Es importante también, tener en cuenta las recomendaciones internacionales e impulsar el relevamiento y la investigación continua y profunda para fortalecer la ciberresiliencia y replicar las acciones e iniciativas de buenas prácticas que han demostrado ser valiosas en otros países y regiones del mundo.

ANEXO I

Mapa de Riesgos Aplicaciones.xlsx

GLOSARIO

- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. [2]
- **Apetito de Riesgo**: Cantidad y tipo de riesgo que una organización está dispuesta a buscar o retener.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización. (ISO/IEC 27000:2022) [2]
- **Confidencialidad**: Propiedad que la información no se pone a disposición o se divulga a individuos, entidades o procesos no autorizados. (ISO/IEC 27000:2022) [2]
- **Consecuencia**: Resultado de un acontecimiento que afecta a los objetivos (ISO *Guide* 73:20095). Una consecuencia puede ser cierta o incierta y, en el contexto de la seguridad de la información, suele ser negativa. (ISO/IEC 27000:2022) [2]
- **Control**: Medida para modificar el riesgo (ISO *Guide* 73:2009). Puede incluir políticas y procedimientos, directrices, prácticas o estructuras organizativas que pueden ser de carácter administrativo, técnico, de gestión o legal. [2]
- **Disponibilidad**: Propiedad de ser accesible y utilizable a petición de una entidad autorizada. (ISO/IEC 27000:2022) [2]
- **Integridad**: Propiedad de exactitud y completitud. (ISO/IEC 27000:2022) [2]
- **ITGC**: Son Controles Generales de Tecnología de Información que se aplican a todos los sistemas, componentes, procesos y datos de una determinada organización o entorno de tecnología de la información.
- **Nivel de Riesgo**: Magnitud de un riesgo o combinación de riesgos, expresada en términos de la combinación de consecuencias y su probabilidad. (ISO *Guide* 73:2009)
- **Objetivo**: Resultado que debe alcanzarse. (ISO/IEC 27000:2022) [2]
- **Probabilidad** (*likelihood*): Posibilidad de que algo suceda. (ISO *Guide* 73:2009) [2]
- **PTC:** es una tecnología que se superpone al hardware y software existentes en los trenes. Por mandato legal, el PTC tiene por objeto evitar colisiones entre trenes, descarrilamientos causados por una velocidad excesiva, incursiones no autorizadas de trenes en tramos de vía donde se realizan actividades de mantenimiento y la circulación de un tren a través de un cambio de vía dejado en una posición incorrecta.

- **Riesgo**: Efecto de la incertidumbre sobre los objetivos. (ISO *Guide* 73:2009) El riesgo se caracteriza a menudo por la referencia a "acontecimientos" potenciales (tal como se definen en la Guía ISO 73:2009, 3.5.1.3) y "consecuencias" (tal como se definen en la Guía ISO 73:2009, 3.6.1.3), o una combinación de los mismos. [2]
- **Riesgo Residual**: Riesgo remanente después de su tratamiento. (ISO *Guide* 73:2009) [2]
- **Vulnerabilidad**: Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 27000:2022) [2]

BIBLIOGRAFIA CONSULTADA

[1] Trabajo Final de Especialización: Tema: Infraestructuras Críticas
Título: El Quinto Dominio Sobre Infraestructuras Criticas
Autor: Simón ROBERTS Año de Presentación: 2022
Tutor: Darío RIZZO

[2] Trabajo Final de Especialización: Tema: ANÁLISIS DE METODOLOGÍAS DE LA GESTIÓN DEL RIESGO APLICABLES A LA NORMA ISO/IEC 27005:2018.
Autor: David Chacón Prieto. Año de Presentación: 2020
Tutor del Trabajo Final: Marcia Maggiori.

[3] Tesis de Maestría: Tema: Ciberseguridad en el sector transporte, focalizado en los subsectores ferroviario, de aviación civil y marítimo.
Título: Análisis de ciberseguridad para el transporte ferroviario, de aviación civil y marítimo de Argentina. Año de Presentación: 2022
Autor: Ing. Marcos H. Martínez. Directora de Tesis: Mg. Patricia Prandini.

[4] CASE 2018
Congreso Argentino de Sistemas Embebidos - 15 al 17 de agosto de 2018
Universidad Tecnológica Nacional - Facultad Regional Córdoba, Argentina
Fecha de catalogación: 30/7/2018
Página Web: http://www.sase.com.ar/case/ediciones/case2018/

[5] ¿Se puede hackear un tren?
Página Web: https://www.kaspersky.es/blog/train-hack/7426/
(Consultada el 30/07/2022).

[6] CyberRail: fin a los ataques cibernéticos en una infraestructura crítica
Página Web: https://magazine.mafex.es/cyberrail-fin-a-los-ataques-ciberneticos-en-una-infraestructura-critica/
(Consultada el 30/07/2022).

[7] Clasificación de las industrias más críticas del mundo
Página Web: https://www.vertiv.com/es-latam/about/news-and-insights/articles/pr-campaigns-reports/IndustriasCriticas/?utm_source=print&utm_medium=campaign%20page&utm_campaign=Ranking%20the%20World%27s%20Most%20Critical%20Industries
(Consultada el 01/08/2022).

[8] El reto de la ciberseguridad: análisis en las infraestructuras ferroviarias

Página Web: https://www.researchgate.net/publication/324222663_El_reto_de_la_ciberseguridad_analisis_en_las_infraestructuras_ferroviarias
(Consultada el 03/08/2022).

[9] *Mobility and Transport*
Página Web: https://transport.ec.europa.eu/transport-modes/rail/ertms/how-does-it-work/etcs-levels-and-modes_en
(Consultada el 04/08/2022)

[10] Sistema de Comunicaciones GSM-R: El Estándar Ferroviario de Comunicaciones
Página Web: https://www.coit.es/sites/default/files/archivobit/pdf/trubio.pdf
(Consultada el 04/08/2022)

[11] *Leading the Way in PTC*
Página Web: https://www.bnsf.com/in-the-community/safety-and-security/positive-train-control.page
(Consultada el 04/08/2022)

[12] COMO CONTROLAR UN RELÉ CON UN TRANSISTOR
Página Web: https://www.inventable.eu/controlar-rele-con-transistor/
(Consultada el 04/08/2022)

[13] El sistema ferroviario en el desarrollo de la nación
Página Web: https://www.americaeconomia.com/analisis-opinion/el-sistema-ferroviario-en-el-desarrollo-de-la-nacion
(Consultada el 05/08/2022)

[14] OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*)
Página Web: http://apuntesseguridadit.blogspot.com/2014/03/octave-operationally-critical-threat.html
(Consultada el 10/08/2022)

[15] *10 STEPS TO DO IT YOURSELF CRAMM*
Página Web: http://www.itsmsolutions.com/newsletters/DITYvol2iss8.htm
(Consultada el 10/08/2022)

[16] Trenes Argentinos
Página Web: https://www.argentina.gob.ar/transporte/trenes-argentinos-capital-humano/mision-vision-y-valores#:~:text=Lograr%20el%20m%C3%A1s%20alto%20est%C3%A1ndar,prestar%20servicios%20tanto%20a%20actores
(Consultada el 16/09/2022)

[17] ISO/IEC 27005:2022
Information security, cybersecurity and privacy protection — Guidance on managing information security risks
Página Web: https://www.iso.org/standard/80585.html
(Consultada el 18/01/2023)

[18] *ISO/IEC 27005:2022 what is new?*
Página Web: https://www.linkedin.com/pulse/isoiec-270052022-what-new-paul-varela/?trk=pulse-article
(Consultada el 18/01/2023)