Telefónica Tech

NextDefense Insights

Guardianes de la frontera digital

Ciberresiliencia en infraestructuras críticas

Un informe imprescindible sobre ciberseguridad y resiliencia en entornos críticos.

Resumen

Este informe representa un análisis exhaustivo de los desafíos cibernéticos globales en un contexto de profundos cambios geopolíticos, fundamentado en la historia de las ciberamenazas a las infraestructuras críticas, para desentrañar la fórmula que permite fortalecer la ciberresiliencia y optimizar las estrategias de ciberdefensa en entornos críticos.

Mediante el examen de casos de uso reales, explora la seguridad en entornos operativos (OT), sanitarios, infraestructuras de defensa nacional y la protección de redes 5G e IoT. Este informe proporciona conocimientos y estrategias valiosas para salvaguardar ecosistemas vitales, poniendo en contexto y de forma comprensible el estado de la ciberseguridad en estos entornos de alta criticidad.

CONTENIDO

1. Ciberresiliencia para infraestructuras críticas

La misión de Telefónica Tech como Guardianes de la Frontera Digital resulta imprescindible.

Las sociedades contemporáneas dependen en gran medida de infraestructuras críticas para su funcionamiento cotidiano, y es nuestro deber asegurarnos de que estas **infraestructuras estén resguardadas en un entorno digital en constante evolución.**

La digitalización avanza a un ritmo vertiginoso, superando en muchos casos la capacidad de garantizar la seguridad de los activos y sistemas esenciales que respaldan estas infraestructuras críticas. Las estrategias de ciberseguridad tradicionalmente centradas en las tecnologías de la información TI no son suficientes para proteger los sistemas ciberfísicos.

Los sistemas ciberfísicos integran las tecnologías de la información (TI) y las tecnologías operativas (OT) para habilitar la comunicación y la interacción entre los elementos físicos y el entorno digital. Se utilizan en una amplia gama de aplicaciones, desde fábricas hasta dispositivos médicos, coches conectados, vehículos militares y sistemas de defensa, entre otros. En este contexto, **las amenazas cibernéticas acechan a nuestros activos críticos.**

Si bien la ciberseguridad ya es un requisito fundamental en las especificaciones de las redes 5G, es esencial comprender que debemos ir más allá de las características nativas de seguridad de estas redes para garantizar una **protección integral, de extremo a extremo (end-to-end).** En este informe, exploraremos en detalle los **desafíos y soluciones que deben abordarse para fortalecer la seguridad de las infraestructuras críticas en la era digital**, reforzando así nuestra posición como Guardianes de la Frontera Digital.

1.1 Nuestra Misión

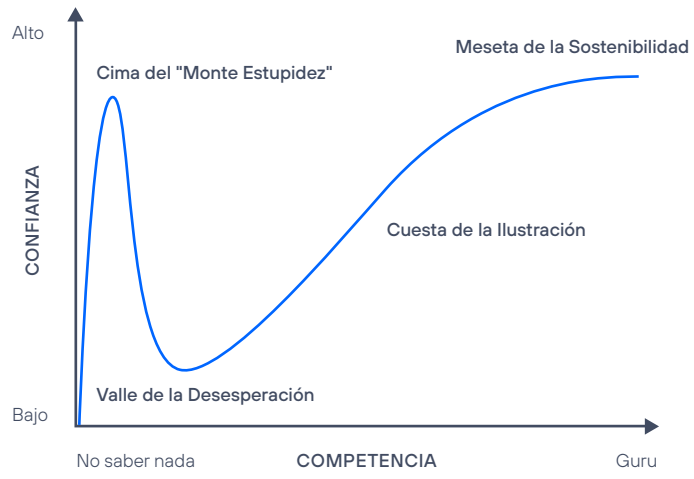
¿Cuál es nuestra misión como guardianes de la frontera digital en la que nuestro mundo físico se está digitalizando?

Nuestra misión es la de facilitar la adopción de las tecnologías digitales a las personas, en los procesos y sobre las infraestructuras de nuestros clientes al tiempo que garantizamos su resiliencia.

1.2 El efecto Dunning-Kruger

¿Podría ser que las naciones occidentales, generalmente percibidas como potencias avanzadas tecnológicamente, estén inadvertidamente cayendo presas del **efecto Dunning-Kruger**? ¿Hemos subestimado las capacidades e intenciones de nuestros adversarios desencadenando así amenazas cibernéticas y una agitación geopolítica sin precedentes?

EFECTO DUNNING-KRUGER



El efecto Dunning-Krueger es un sesgo cognitivo que lleva a las personas a sobrestimar su competencia.

Si examinamos la extensión de nuestra ingenuidad en relación con el panorama geopolítico y nuestros ciberadversarios descubrimos realidades impactantes y subrayaremos las consecuencias de esta ingenuidad en las infraestructuras críticas.

1.3 El estado soberano del siglo XXI

¿Operas en un país soberano? ¿Es tu organización resiliente? ¿Es tu infraestructura resiliente?

En la actualidad, la soberanía de los países occidentales se ve desafiada en múltiples frentes, especialmente en el contexto de las tensiones geopolíticas a las que se enfrentan. Esta lucha por mantener una soberanía plena se extiende a diversos aspectos cruciales, entre los cuales se destacan:

1. SOBERANÍA ENERGÉTICA:

Garantizar la independencia energética es un pilar fundamental de la soberanía de un país. La dependencia de fuentes de energía extranjeras puede poner en riesgo la autonomía y seguridad de un estado, así como su capacidad de respuesta en tiempos de crisis.

2. CAPACIDAD DE DEFENSA:

La capacidad de defensa de un país es esencial para que preserve su soberanía. La inversión y el desarrollo de fuerzas armadas capaces y modernas son vitales para la disuasión y la protección contra posibles amenazas externas.

3. CAPACIDADES DE CIBERSEGURIDAD:

Es un componente crucial de la soberanía de un estado. Las amenazas cibernéticas pueden socavar la infraestructura crítica, los sistemas de defensa y la privacidad de los ciudadanos, lo que pone de manifiesto la importancia de contar con una estrategia de ciberseguridad robusta y eficaz.

4. SEGURIDAD DE LA CADENA DE VALOR DE LOS CHIPSETS:

La dependencia de componentes críticos de suministradores extranjeros puede poner en riesgo la seguridad y la soberanía tecnológica.

Sin embargo, más allá de estos aspectos individuales, la pregunta fundamental que se plantea es la siguiente:

¿Son nuestros países capaces de proteger sus infraestructuras nacionales claves frente a ciberamenazas globales?

La confiabilidad de estas infraestructuras es un elemento crucial en la protección de la soberanía de un estado, ya que su vulnerabilidad podría exponer a un país a amenazas tanto internas como externas.

En un mundo cada vez más dependiente de tecnologías avanzadas, la soberanía de un estado no solo depende de su capacidad para resistir las amenazas tradicionales, sino también de su habilidad para proteger sus activos digitales y asegurar la continuidad de sus infraestructuras críticas.

Para mantener una soberanía plena en la era moderna, es esencial abordar estos desafíos con enfoque y determinación. La inversión en soberanía energética, defensa, ciberseguridad y la seguridad de la cadena de valor tecnológica es esencial para garantizar la autonomía y seguridad de un estado en el mundo actual.

1.4 Quinto dominio: importancia estratégica

El concepto 'quinto dominio' se refiere a la ciberseguridad como un nuevo ámbito de protección y defensa en el contexto de un estado soberano. Tradicionalmente, los cuatro dominios de protección y defensa han sido la tierra, el mar, el aire y el espacio. Sin embargo, con el crecimiento exponencial de las amenazas cibernéticas, se reconoce cada vez más la importancia de considerar la ciberseguridad como un quinto dominio.

En este quinto dominio, el ciberespacio, los estados soberanos deben desarrollar capacidades y estrategias para proteger sus infraestructuras críticas, salvaguardar la integridad de sus sistemas de información y contrarrestar las amenazas cibernéticas que podrían afectar su seguridad nacional.

Esto implica la implementación de políticas y regulaciones, la colaboración con el sector privado, la inversión en tecnologías avanzadas y la formación de profesionales especializados en ciberseguridad. El quinto dominio se ha convertido en un componente esencial en la protección y defensa de un estado soberano en la era digital.

1.5 El estado soberano del siglo XXI

En un entorno digital cada vez más desafiante, la capacidad de una organización para proteger sus infraestructuras clave contra intrusiones cibernéticas se vuelve esencial. En este contexto, surgen varias preguntas:

- **¿Es capaz tu organización de proteger sus infraestructuras clave frente a las intrusiones cibernéticas?**
- **¿Dispone de una infraestructura ciber soberana?**
- **¿De qué hablamos cuando hablamos de ser un operador de infraestructuras ciber soberanas?**

Para comprender mejor esta noción, es importante conocer los distintos tipos de infraestructuras críticas, su importancia y profundizar en lo que significa ser un operador de infraestructuras ciber soberanas.

2. Infraestructuras críticas y su importancia

Las infraestructuras críticas son los pilares invisibles sobre los que se sostiene el funcionamiento de naciones enteras, proporcionando servicios esenciales. Su importancia radica en su capacidad para respaldar la economía, la seguridad y la calidad de vida de la sociedad.

Las infraestructuras críticas abarcan diversos ámbitos, entre los que destacamos:

- **Tecnologías operacionales (OT)**
- **Infraestructuras sanitarias**
- **Sistemas de seguridad y defensa**
- **Redes de telecomunicaciones y 5G**

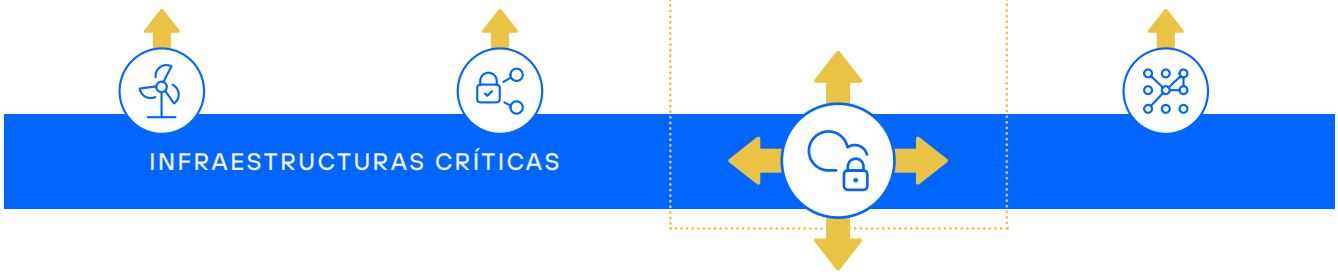
2.1 Operadores de infraestructuras cibersoberanas

El concepto de operador de infraestructuras cibersoberanas aborda la capacidad de una organización para mantener la soberanía sobre sus operaciones digitales y salvaguardar sus infraestructuras críticas de las amenazas cibernéticas.

Esto implica:

- Tener **control total sobre sus activos digitales**, sin dependencia de proveedores extranjeros o vulnerabilidades externas.
- Contar con medidas de **resiliencia cibernética** sólidas para responder y recuperarse de las amenazas cibernéticas de manera eficaz.
- Garantizar la **integridad y confidencialidad de los datos críticos** y la información sensible.
- Capacidad de **detectar y responder rápidamente a intrusiones cibernéticas**, minimizando el impacto en sus operaciones.

ENERGÍA	DEFENSA	CIBERSEGURIDAD	CADENA DE SUMINISTRO
• Independencia de fuentes externas. • Combinación energética equilibrada.	• Defensa fiable y robusta. • Industria autónoma.	• Capacidades Integrales. • Inteligencia independiente.	• Chipsets. • Combinación de producción confiable y equilibrada.



Producción OT	Energía OT	Defensa OT	5G & IoT	...

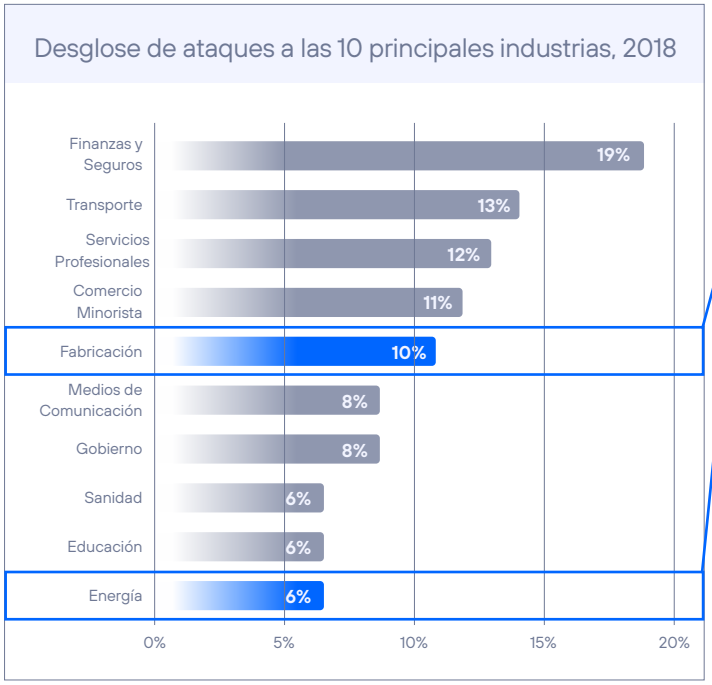
2.2 Importancia de la ciberseguridad en infraestructuras críticas

En sectores en los que la interacción con el cliente final tiene un peso menor, como la industria, la minería, la agricultura o las empresas del sector energético, la **digitalización ha avanzado de manera más lenta**, permitiéndoles mantener una distancia relativa de la transformación digital.

Este menor grado de adopción tecnológica ha estado estrechamente relacionado con las necesidades de ciberseguridad experimentadas por estas organizaciones. No obstante, en los últimos años, una serie de acontecimientos han actuado como catalizadores para acelerar la transformación digital en las áreas operativas de estos sectores económicos. El objetivo detrás de esta aceleración **es automatizar procesos, mejorar la eficiencia y la agilidad, y adaptarse a los cambios en los hábitos y necesidades de la sociedad**.

Este proceso de aceleración en la transformación ha venido acompañado de un aumento de los incidentes de ciberseguridad sufridos por estos sectores industriales.

En este sentido, la *Figura 1* ilustra este hecho mostrando el **aumento de posiciones en el ranking de sectores más atacados durante los últimos 5 años**. Se puede ver claramente que el **sector manufacturero y el sector industrial han escalado posiciones**, pasando a liderar el ranking desde 2021, por delante incluso del sector financiero y asegurador, que tradicionalmente ha sido el adalid de la inversión en ciberseguridad.



Porcentaje de ataques por industria 2019-2023

INDUSTRIA	2023	2022	2021	2020	2019
Fabricación	25.7%	24.8%	23.2	17.7	8
Finanzas y Seguros	18.2%	18.9%	22.4	23	17
Servicios Profesionales	15.4%	14.6%	12.7	8.7	10
Energía	11.1%	10.7%	8.2	11.1	6
Venta (por menor y mayor)	10.7%	8.7%	7.3	10.2	16
Educación	6.3%	7.3%	2.8	4	8
Sanidad	4.3%	5.8%	5.1	6.6	3
Gobierno	4.3%	4.8%	2.8	7.9	8
Transporte	2.8%	3.9%	4	5.1	13
Medios de comunic. y Telecomunicaciones	1.2%	0.5%	2.5	5.7	10

Figura 1. *Evolución del porcentaje de ataques por sector. Fuente: X-Force Threat Intelligence.*

También el sector sanitario merece una mención especial. Si bien su posición en el ranking anterior no ha cambiado en los últimos años, **el sector lidera el ranking de las industrias con un coste por incidente más alto.**

Sin duda, **la naturaleza de los datos que maneja lo hacen especialmente sensible**, cuestión que se hace más patente a medida que su superficie de ataque crece de forma imparable por la digitalización de los canales de atención y, especialmente, por el creciente número de dispositivos de electromedicina conectados.

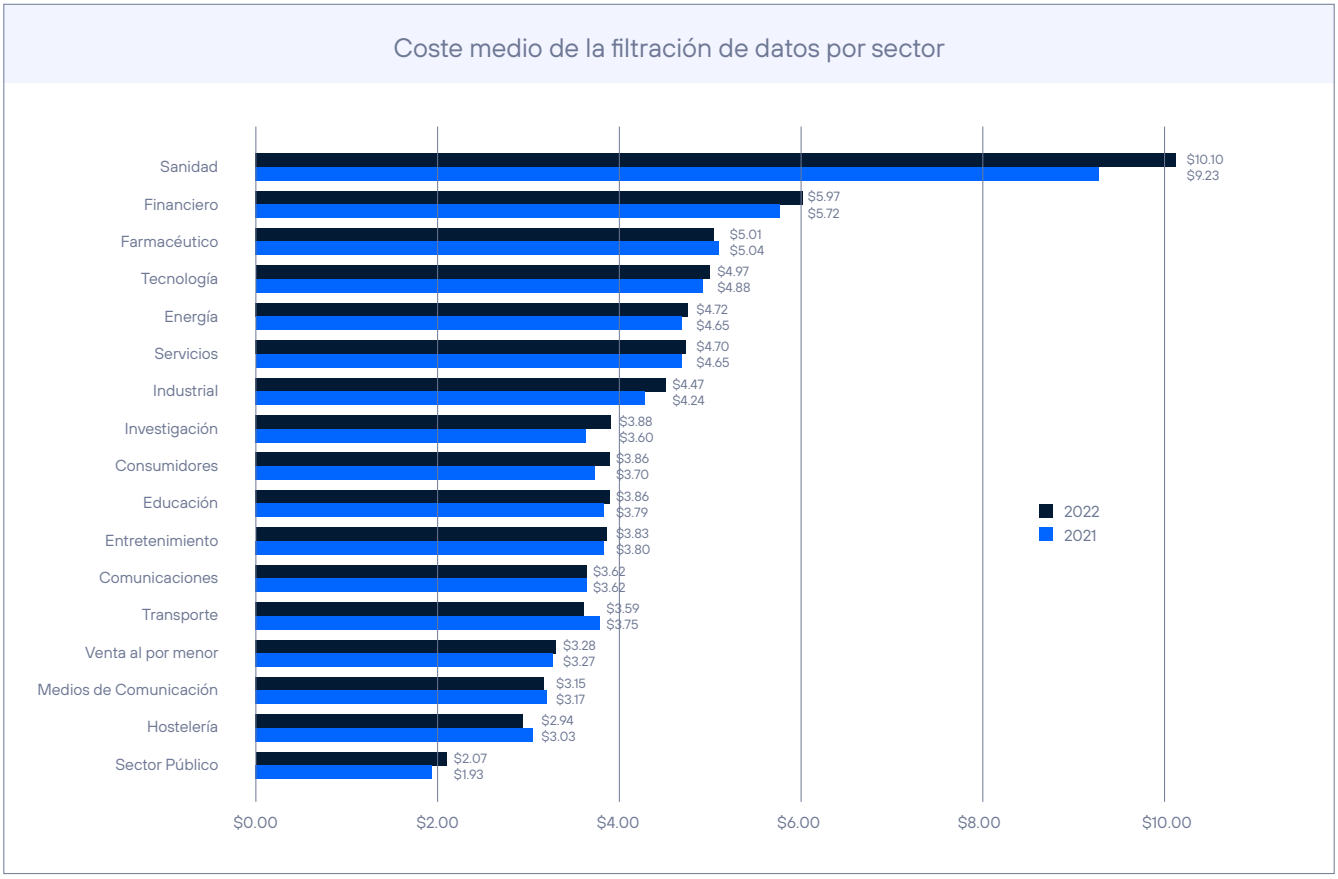


Figura 2. *Coste medio de los incidentes por industria. Fuente: Informe IBM 2022.*

Un tercer sector en auge a causa de los últimos conflictos geopolíticos es el de Defensa. La ciberseguridad siempre ha sido un área de interés para el sector militar, pero desde hace unos años, se le considera ya un dominio de combate de pleno derecho, junto a los cuatro tradicionales (tierra, mar, aire y espacio), pasando a considerarse ese 'quinto dominio' mencionado anteriormente.

Desde una perspectiva más técnica, al analizar el armamento, los vehículos y las naves de nueva generación, se comprende mejor la relevancia que cobra la ciberseguridad, pues se trata de dispositivos conectados que en muchos casos pueden manejarse en remoto y, por lo tanto, están **expuestos a que una vulnerabilidad pueda facilitar la toma de control por parte del enemigo.**

Por ello, no es de extrañar que se espera que este mercado crezca al 10% durante los próximos años. Cabe además comentar que es un mercado en el que se da preferencia a los proveedores nacionales y de países aliados por razones geopolíticas.

Figura 3. *Evolución del mercado de la ciberseguridad mililtar.*

2.3 Ciberseguridad en infraestructuras críticas: particularidades

Las infraestructuras críticas se distinguen de otros sistemas en varios aspectos fundamentales que impactan directamente en su ciberseguridad.

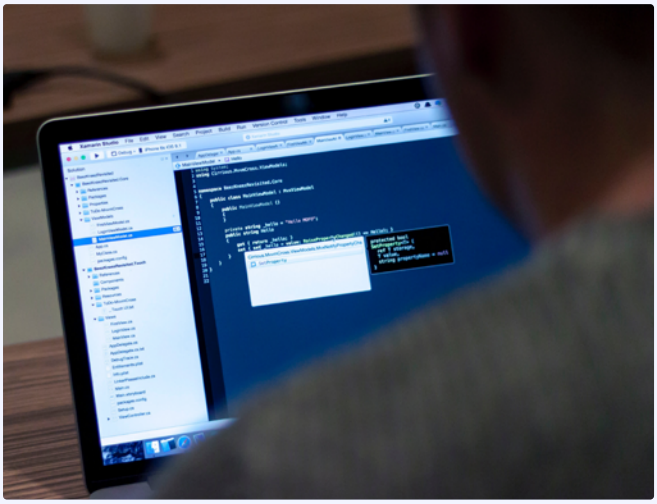
- **ORIGEN ANTIGUO:** sistemas de hardware y software empleados para supervisar y controlar procesos físicos no concebidos para conectarse a Internet. Los entornos OT suelen estar formados por sistemas antiguos que pueden haber estado en funcionamiento durante muchos años, lo que los hace más susceptibles a las vulnerabilidades y carecen de funciones de seguridad integradas.
- **FINALIDAD:** los sistemas OT están diseñados para garantizar la seguridad, fiabilidad y eficiencia de los procesos industriales, mientras que los sistemas IT tradicionales se centran en el procesamiento de datos y la comunicación.
- **PRIORIDAD:** a diferencia de las redes de TI, las redes OT dan prioridad a la comunicación en tiempo real y tienen estrictos requisitos de tiempo de actividad, lo que deja poco margen para interrupciones o tiempos de inactividad causados por medidas de seguridad.
- **DIVERSIDAD TECNOLÓGICA:** los sistemas OT abarcan una amplia gama de dispositivos y tecnologías, como sistemas de control industrial (ICS), sistemas de supervisión, control y adquisición de datos (SCADA), controladores lógicos programables (PLC) y maquinaria especializada. Esta diversidad tecnológica agrega una capa adicional de complejidad a la ciberseguridad de las infraestructuras críticas.
- **PRIMERO LO FÍSICO:** la ciberseguridad de los sistemas OT se centra en proteger las infraestructuras críticas, garantizar la disponibilidad, integridad y seguridad de los procesos industriales, y prevenir los posibles daños o perjuicios físicos causados por los ciberataques.

Estas diferencias subrayan la necesidad de abordar la ciberseguridad en las infraestructuras críticas de manera específica y adaptada a sus características únicas. La protección de estos sistemas desempeña un papel crucial en la preservación de la seguridad, la continuidad de las operaciones y la integridad de la sociedad moderna.

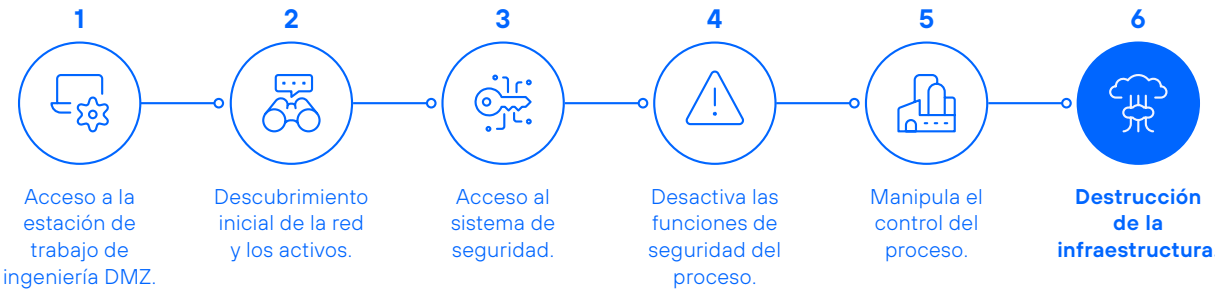
3. Ciberataques a sistemas industriales OT: el caso Tritón

Podemos ilustrar un ciberataque a una infraestructura crítica mediante el incidente conocido como escenario Tritón, que tuvo lugar en una instalación petroquímica en Arabia Saudí a mediados de 2017.

El caso Tritón representa el **primer incidente del que se ha informado públicamente que demuestra un ataque dirigido con un efecto conocido a un SIS** (Sistema Instrumentado de Seguridad) operativo. Las actividades de los piratas informáticos provocaron la parada del proceso del controlador SIS, lo que permitió descubrir el ataque.



Escenario de ataque OT (basado en Tritón)



1. El ataque se inicia con el **compromiso de una máquina en la red corporativa** mediante técnicas de phishing, la distribución de un pendrive infectado o un actor malicioso interno. Dado que esta máquina del entorno IT se usa para acceder a estaciones de ingeniería del entorno OT, el atacante procede a extraer las credenciales para conectarse a alguna de ellas utilizando herramientas como Mimikatz, capaces de extraer contraseñas almacenadas en memoria.

2. Una vez en el entorno OT, el atacante empieza a **explorar los diferentes activos** que allí se encuentran.

3. El objetivo final del atacante consiste en deshabilitar los controladores de seguridad diseñados para detener los procesos industriales cuando se detectan condiciones de operación peligrosas, por lo que en este punto trata de **localizar estos sistemas.**

4. Tras localizar el sistema de control, el atacante carga un malware específicamente diseñado para **tomar el control del sistema de forma remota y desactivar las funciones de seguridad** capaces de detener el proceso en cuanto a empieza a presentar un riesgo para la integridad física.

5. Con el sistema de seguridad fuera de juego, el atacante procede a **manipular los sistemas que controlan el proceso industrial.**

6. Los cambios que realiza el atacante sobre el sistema de control industrial tienen **efectos devastadores sin que los sistemas de control de seguridad puedan hacer nada para evitarlo.**

3.1 Operadores de infraestructuras cibersoberanas

¿Cuáles son las amenazas a las que se enfrentan hoy en día las infraestructuras críticas? El panorama mundial es dinámico y está en constante evolución. Compartimos aquí algunos de los retos más recientes y significativos a los que se enfrentan:

IMPULSADO POR EL FACTOR HUMANO

Ingeniería social: Los ataques de ingeniería social representan una amenaza importante, ya que los actores malintencionados intentan engañar a los empleados para obtener acceso no autorizado a los sistemas o información confidencial.

Errores y descuidos: Los errores y descuidos de los empleados pueden conducir a incidentes de seguridad, como la apertura de correos electrónicos o archivos adjuntos maliciosos, la pérdida de dispositivos o la configuración incorrecta de sistemas.

Falta de capacitación en ciberseguridad: La falta de conciencia y formación entre los empleados puede hacer que sean más susceptibles a las tácticas de ingeniería social y menos propensos a tomar medidas de seguridad adecuadas.

Acceso privilegiado: Los empleados con acceso privilegiado a los sistemas y datos confidenciales representan un riesgo, ya que pueden abusar de sus privilegios o ser víctimas de ataques dirigidos para obtener acceso no autorizado.

Colaboración involuntaria: Los empleados pueden colaborar involuntariamente en ciberataques al ser víctimas de malware o al permitir que los atacantes accedan a los sistemas a través de sus credenciales comprometidas.

IMPULSADO POR EL ADVERSARIO

Ciberataques sofisticados: Los sistemas de infraestructuras críticas son cada vez más el blanco de ciberataques sofisticados, incluidas las amenazas persistentes avanzadas (APT), los ataques de ransomware y los compromisos de la cadena de suministro. Estos ataques aprovechan las vulnerabilidades de los sistemas de IT y OT para interrumpir las operaciones, comprometer la integridad de los datos y potencialmente causar daños físicos o interrupciones generalizadas.

Amenazas de estado-nación: Los ciberataques patrocinados por estados suponen un reto importante para las infraestructuras críticas. Los países participan en campañas de ciberespionaje, sabotaje o interrupción dirigidas a sectores críticos, como la energía, la sanidad, el transporte y la defensa. Estas amenazas suelen implicar a adversarios bien dotados de recursos y altamente cualificados, con motivaciones estratégicas.

Amenazas internas: Las amenazas internas, ya sean intencionadas o no, siguen siendo un reto. Las personas malintencionadas con acceso privilegiado pueden aprovecharse de su posición para causar daños o robar información confidencial. Las acciones involuntarias de los empleados, como ser víctimas de ataques de ingeniería social o introducir inadvertidamente programas maliciosos, también pueden provocar incidentes de seguridad.

IMPULSADO POR LA TECNOLOGÍA

Creciente interconectividad: El aumento de la interconectividad entre los sistemas de IT y OT, junto con la proliferación de dispositivos IoT y servicios basados en cloud, amplía la superficie de ataque para las ciberamenazas. Las infraestructuras críticas se vuelven más vulnerables a los ciberataques a medida ya que más dispositivos y sistemas están conectados, creando posibles puntos de entrada para los atacantes.

Tecnologías emergentes: La adopción de tecnologías emergentes, como las redes 5G, la computación en cloud, la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT), introduce tanto oportunidades como desafíos para la ciberseguridad de las infraestructuras críticas. Si bien estas tecnologías mejoran la eficiencia y la conectividad, también introducen nuevas vulnerabilidades y complejidades que deben abordarse.

Vulnerabilidades de los sistemas heredados: Muchos sectores de infraestructuras críticas siguen dependiendo de sistemas antiguos que pueden carecer de actualizaciones periódicas de seguridad o tener protocolos de seguridad obsoletos. Estos sistemas no fueron diseñados originalmente teniendo en cuenta la ciberseguridad y pueden tener vulnerabilidades inherentes que pueden ser explotadas por los atacantes.

Riesgos de la cadena de suministro: La naturaleza global de las cadenas de suministro introduce riesgos de ciberseguridad. Los agresores pueden atacar a los proveedores, comprometer componentes de hardware o software, o inyectar código malicioso durante el proceso de fabricación. Los sistemas de infraestructuras críticas pueden utilizar componentes comprometidos. Esto supone una amenaza significativa a la integridad y seguridad.

IMPULSADO POR LA ORGANIZACIÓN

Limitación de recursos: Los ejecutivos a menudo se enfrentan a la falta de recursos, como presupuestos limitados, escasez de profesionales cualificados en ciberseguridad y dificultades para obtener las tecnologías y herramientas necesarias. Asignar recursos de forma eficaz para abordar las necesidades de ciberseguridad dentro de la organización puede ser una tarea desalentadora.

Respuesta y recuperación de incidentes complejos: Los ejecutivos deben desarrollar y mantener planes eficaces de respuesta y recuperación de incidentes para mitigar el impacto de los incidentes cibernéticos en las infraestructuras críticas. Esto incluye la detección oportuna, la contención y las medidas de recuperación para minimizar las interrupciones y restaurar las operaciones rápidamente.

Limitación del ciberseguro: Definir un ciberataque como un acto de guerra puede tener consecuencias de gran alcance para el ciberseguro. A menudo conduce a la exclusión de la cobertura de los daños causados por dichos ataques, dejando a las organizaciones vulnerables a pérdidas sustanciales. Además, las aseguradoras pueden dudar en ofrecer cobertura para los ciberataques relacionados con la guerra debido a su naturaleza significativa e impredecible, lo que resulta en una disponibilidad limitada de pólizas adecuadas. Si se ofrece cobertura, las primas pueden aumentar significativamente para reflejar el mayor riesgo, por lo que es menos asequible para las organizaciones que buscan protección.

Para hacer frente a estos retos cibernéticos mundiales se requiere un enfoque holístico que incluya marcos sólidos de ciberseguridad, evaluaciones continuas de los riesgos, actualizaciones periódicas de la seguridad, programas de concienciación y formación de los empleados, una estrecha colaboración entre los sectores público y privado e inversión en capacidades avanzadas de detección y respuesta a las amenazas.

3.2 Amenazas de los estados-nación: limitación del ciberseguro

La combinación de algunas de estas amenazas nos pone un gran reto por delante al tratar de proteger nuestras infraestructuras críticas.

¿Crees que el ciberseguro cubre a vuestra organización de una ciberguerra o de operaciones cibernéticas patrocinadas por el estado?

Las **ciberaseguradoras quieren excluir de sus pólizas los ciberataques patrocinados por estados.** Esto es especialmente relevante para los operadores de infraestructuras críticas. El riesgo de guerra cibernética es de naturaleza sistémica; en otras palabras, el riesgo planteado es para todo un sistema, incluidas todas sus partes componentes, no simplemente para organizaciones individuales. Dada nuestra dependencia de las infraestructuras digitales, no cabe duda de que un pequeño número de estados tienen en sus capacidades ofensivas cibernéticas el poder de causar daños económicos incalculables, que el mercado de seguros simplemente no podría soportar. Es contra estos riesgos que las exclusiones de guerra cibernética están siendo diseñadas para actuar.

En el caso de Merk & Co contra Ace American Insurance Company, esta última ya intentó excluir de su cobertura los daños del ciberataque de 2017 denominado "NotPetya", que cambió las reglas del juego. NotPetya era un malware vinculado al gobierno ruso que causó daños en todo el mundo y dio lugar a 3.000 millones de dólares en reclamaciones de seguros, algunas de las cuales aseguradoras como Ace sostenían que estaban excluidas. Ahora, Lloyds, el mercado de seguros y reaseguros con sede en Londres ha publicado una exclusión explícita que se incluirá por defecto en cualquier futura póliza de ciberseguro.

¿Y por qué es importante para las empresas que gestionan infraestructuras críticas?

La respuesta radica en los acuerdos de nivel de servicio (SLA) que con frecuencia estas empresas mantienen con su regulador y clientes. En caso de que la aseguradora no proporcione cobertura y, simultáneamente, el estado no asuma la responsabilidad como último recurso, existe el **riesgo de que estos SLAs le dejen fuera del negocio.**

4. Fórmula para ciberresiliencia de infraestructuras críticas

Como Guardianes de la Frontera Digital que somos en Telefónica Tech, tenemos una fórmula para la ciber-resiliencia en infraestructuras críticas. Consiste en los elementos que cualquier organización debería tener en mente a la hora de proteger sus infraestructuras críticas.

Lo predicamos de esta manera: **El riesgo es igual a la probabilidad de que un ciberataque tenga éxito multiplicada por el impacto de los daños que dicho incidente genera.**

RIESGO = PROBABILIDAD X IMPACTO

Así que, si nos lo tomamos como una fórmula de llamada a la acción,

- Primero, debemos conocer el **riesgo cibernético al que está expuesta nuestra infraestructura.**
- Luego, **proteger nuestra infraestructura crítica.**
- Por último, estar preparados para **detectar, responder y recuperarnos de cualquier incidente de ciberseguridad.**
- Todo ello, debe ser **gestionado y optimizado por un Centro de Operaciones de Seguridad OT especializado.**

1. Conoce tu postura	2. Infraestructura	3. Monitor & React	4. Gestión
• Seguridad física. • Plan maestro de seguridad. • Inventario activo. • Gestión de vulnerabilidades. • Inteligencia de amenazas cibernéticas de OT.	• Segregación TI-OT. • Segmentación OT. • Lista blanca de aplicaciones-EDR. • Cortafuegos de zona. • Control de acceso remoto.	• Monitoreo de seguridad. • OT: Integración de quipos, procesos y herramientas de ciberseguridad para detección y respuesta. • Administración de incidentes.	• + Gestión y optimización de seguridad OT de extremo a extremo.
Identificar y preparar	**Proteger**	**Detectar, responder y recuperar**	

En Telefónica Tech estamos utilizando esta fórmula internamente y con nuestros clientes más sofisticados para **contribuir a la resiliencia de nuestras infraestructuras críticas.** A continuación, os mostramos algunos ejemplos de lo que todo esto significa.

4.1 Entender la postura de ciberseguridad de la organización

Para el primer elemento de nuestra fórmula, en infraestructuras críticas tenemos que:

1. **Priorizar la seguridad física:** es un componente esencial para garantizar la protección de activos, instalaciones y sistemas vitales para el funcionamiento de la infraestructura. Se refiere a las medidas y prácticas destinadas a prevenir, detectar y responder a amenazas o intrusiones físicas que puedan comprometer la integridad, disponibilidad y confidencialidad de estas infraestructuras.

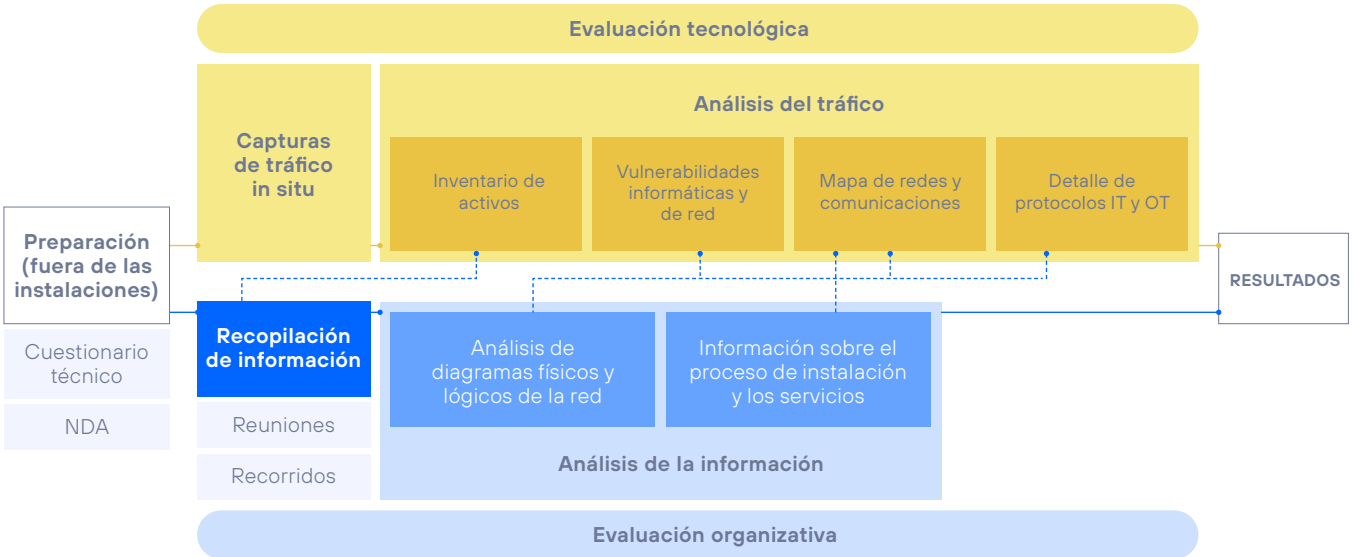
2. **Disponer de un Plan Director de Seguridad:** que les permita identificar y fasear las medidas y controles de ciberseguridad que deben desplegar teniendo en cuenta las necesidades y prioridades de su negocio y las regulaciones que les apliquen.

3. **Disponer de un inventario de activos real, basado en hechos:** un levantamiento de los activos de la planta o plantas objeto de análisis mediante la captura de tráfico y su análisis mediante herramientas capaces de interpretarlo, identificando los activos, sus relaciones de comunicación, vulnerabilidades en la configuración de los activos y la red y posible actividad maliciosa.

4. **Gestionar las vulnerabilidades:** resulta primordial identificar y gestionar las vulnerabilidades de los activos que componen la infraestructura, pues son el punto débil que pueden aprovechar los atacantes.

5. **Recopilar Inteligencia de ciber-amenazas:** una vez conocemos nuestra infraestructura y sus vulnerabilidades, conocer quién está interesado en explotarlas y cómo lo hace aporta información útil para mejorar las capacidades de detección y respuesta.

Ejemplo de una evaluación de ciberseguridad de energía OT:



4.2 Defender la infraestructura: creando una protección de 360° en torno a los activos

Para el segundo elemento de nuestra fórmula, en infraestructuras críticas tenemos que:

1. Aplicar una segregación IT-OT y una segmentación OT adecuadas: se centra en dar respuesta a la que suele ser la primera de las recomendaciones de ciberseguridad que se proponen. El alcance de estos proyectos puede dividirse en dos o más fases, empezando siempre por la segregación para establecer una clara barrera de protección perimetral entre las redes IT y las redes OT de naturaleza industrial. En la práctica, un servicio completo debe constar de las siguientes fases:

- Diseño de arquitectura de red industrial segura.
- Suministro del hardware y software necesario.
- Implantación y configuración de los NGFW (Next-Generation Firewall) y resto de equipos de comunicación que implementen la arquitectura de red definida.
- Explotación del equipamiento tecnológico implantado a fin de proporcionar un servicio similar en alcance al de cualquier tecnología incluida en el servicio Secure Device Management.

2. Aplicar listas blancas de aplicaciones y políticas de endpoints: esto nos permite limitar las aplicaciones que se pueden ejecutar en los sistemas que controlan y supervisan la producción, evitando que un atacante pueda instalar software malicioso que le permita tomar el control de los sistemas.

3. Implementar los cortafuegos de zona: como medida para microsegmentar las redes hasta el punto de controlar las comunicaciones entre cualquier par de dispositivos del entorno industrial, siempre que los requisitos en cuanto a latencia del entorno operativo lo permitan.

4. Desplegar un control de acceso remoto seguro: los entornos operacionales deben permitir el acceso remoto a operarios que tengan que proporcionar funciones de supervisión y mantenimiento, pero es fundamental que esto se haga de forma controlada mediante soluciones que permiten garantizar que los accesos se realizan de forma segura.

En la siguiente ilustración se puede ver un diseño de alto nivel de la protección propuesta para una implementación de red privada 5G de otro cliente de infraestructuras críticas en el que se ve:

- Cada zona de gestión protegida por políticas de confianza cero en el perímetro y los *endpoints*.
- Seguridad especial para la nube y el entorno 5G.
- Sistemas específicos OT para la supervisión de la red y la telemetría de los endpoints OT e IoT.

4.3 Importancia de la detección y respuesta para infraestructuras críticas

Para el tercer elemento de la fórmula, tenemos que pensar en lo que hace que la **detección y la respuesta en infraestructuras críticas** sean tan especiales.

A diferencia de la ciberseguridad IT, la ciberseguridad OT **requiere un profundo conocimiento de los procesos operativos, las tecnologías industriales específicas implicadas y el impacto potencial de un incidente de seguridad en los sistemas físicos.**

La colaboración entre los equipos de IT y OT es crucial para una ciberseguridad eficaz en entornos OT, ya que la experiencia y las perspectivas de ambos dominios son necesarias para abordar los distintos retos y requisitos de los sistemas OT.

En este caso, sugerimos diseñar y preparar teniendo en cuenta 5 cosas:

1	2	3	4	5
Visibilidad específica OT/IoT	Telemetría de endpoints específica de OT	Integración de sistemas OT	Guías específicas de OT para la detección	Acciones de respuestas seguras en OT

1. Visibilidad específica OT / IoT: Comienza con un enfoque diferente para recopilar datos de endpoint que confiar solo en el tráfico de red. Esto implica adaptar los mecanismos tradicionales de IT sin agente para que sean seguros y eficaces en OT. Un agente específico de OT, seguro y de eficacia probada, independiente del proveedor, y una arquitectura sin agentes que reúna una visibilidad profunda de cada endpoint. Esta combinación reúne cientos de datos de los endpoints, como todas las aplicaciones instaladas, todos los usuarios y cuentas y sus ajustes de seguridad, información completa sobre el estado de la configuración, etc. Esta visibilidad de los activos endpoints es similar a la que esperan los responsables de seguridad en sus sistemas de IT, sin causar ningún riesgo a los activos de OT.

2. Telemetría de endpoints específica de OT: A continuación, adapta la recopilación de información en tiempo real directamente de estos activos: registros, syslog, flujos de red, comportamiento de dispositivos y usuarios, estadísticas de rendimiento, etc. Todo esto se recopila de una manera sensible a la red OT para que funcione sin interrupción de las redes de ancho de banda limitado.

3. Integración de sistemas OT: En lugar de limitarnos a enviar datos salientes a un recopilador, necesitamos integrar una amplia gama de información de terceros disponible en los sistemas de control: Alteraciones AV y registros de las distintas soluciones OEM (Original Equipment Manufacturer) aprobadas, alertas de listas blancas, alertas y detecciones de cortafuegos, datos de estado de copias de seguridad, incluso alarmas de control de procesos. Por lo tanto, los motores de aprendizaje automático necesitan agregar telemetría de un conjunto de fuentes mucho más amplio para realizar detecciones precisas.

4. Guías específicas de OT para la detección: La detección y respuesta solo es eficaz si las detecciones se vinculan específicamente al entorno y proporcionan acciones de respuesta recomendadas relevantes para ese sistema. El enfoque identifica amenazas específicas de OT con cientos de detecciones preconstruidas. Las detecciones y las acciones de respuesta deben ser precisas y permitir la "respuesta menos disruptiva" posible dada la amenaza y el propio endpoint sistema.

5. Acciones de respuesta seguras en OT: en OT esas respuestas deben seguir procesos de ingeniería de controles industriales adecuados. Tenemos que "pensar en seguridad, pero actuar en OT". Para que la detección sea precisa y la respuesta rápida, debe permitir la "automatización" de las acciones de respuesta. Pero esas acciones deben pasar por ingenieros "locales" que conozcan los detalles del proceso antes de que se inicie la acción automatizada. La adaptación "Act OT" de la DR acelera la respuesta, pero incluye salvaguardas OT críticas.

4.4 Gestión del centro operativo de seguridad OT

Como paraguas de nuestra fórmula, recomendamos la **especialización en OT** cuando se trata de gestionar la seguridad de infraestructuras críticas, OT o IoT en nombre de nuestros clientes o socios. Esto es lo que hemos hecho, por ejemplo, en Telefónica Tech.

Junto con la fórmula de los 3 elementos para infraestructura crítica sugerimos centrarse en:

Gestión de dispositivos de seguridad OT: para garantizar que los dispositivos están activos y operando con normalidad, a la vez que actualizados con la última versión de software disponible.

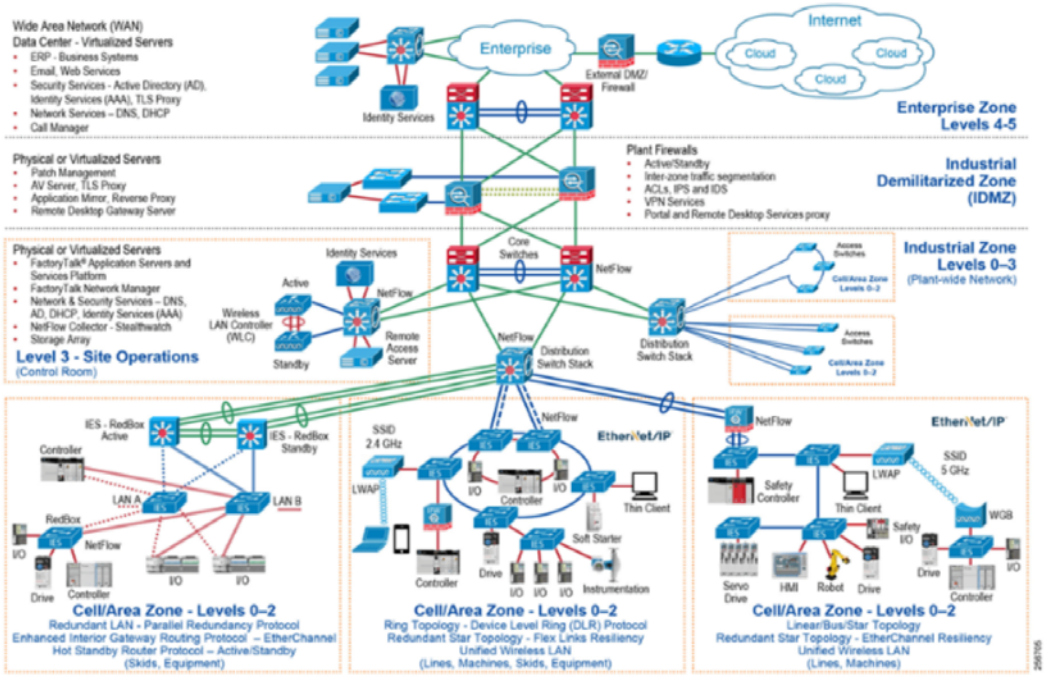
Gestión de alertas: consistente en la gestión de alertas generadas por la detección de actividad maliciosa en el entorno industrial, supervisión de salud de los equipos de monitorización y elaboración de informes sobre la actividad de generación y tratamiento de alertas y sobre cambios en activos y mapa de vulnerabilidades del entorno.

Respuesta a los incidentes: aquellas situaciones en las que se descubre que se ha producido un incidente con un impacto ya materializado, resulta fundamental responder con agilidad para contener el daño y remediar la situación mediante un equipo específicamente preparado para estas situaciones.

Elaboración de informes: con los que actualizar la información sobre el entorno operativo (i.e. cambios en activos y en vulnerabilidades) y sobre la actividad de detección y respuesta a incidentes.

Integración con herramientas de los Digital Operations Center (DOC) como plataformas de orquestación y automatización, plataformas de inteligencia sobre amenazas, portales de clientes y gestión de tiquets y supervisión de la seguridad.

Entorno del Operador de Infraestructuras Críticas



Equipo de seguridad interna

Socio de servicios de seguridad administrada especializado en OT

Gestión de dispositivos de seguridad OT	Monitorización de salud proactivo, ajuste mensual, actualizaciones y soporte.
Gestión de alertas	Monitorización de alertas, N1 24x7, N2 8x5, reomendaciones y notificación de incidentes de seguridad.
Respuesta ante incidentes	Threat Hunting y respuesta a incidentes en coordinación con el equipo de Infra Operator.
Gestión de informes	Informes semanales de dispositivos, alertas e información relevante, informes mensuales de riesgos del equipo de seguridad de OT.

Plataforma de orquestación y automatización

Portal de cliente

Plataforma de inteligencia de amenazas

Gestión de tickets y control de seguridad

5. Conclusión

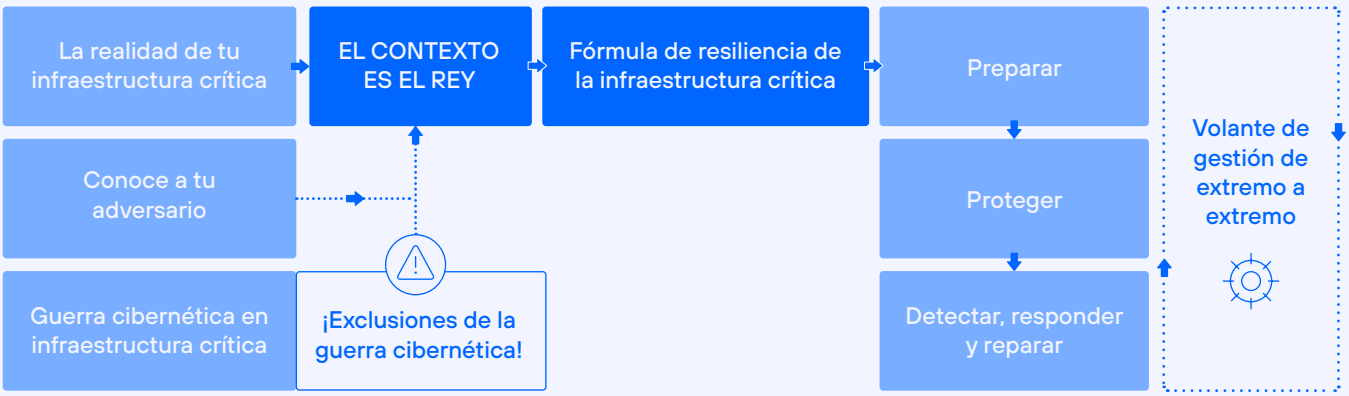
La protección de las infraestructuras críticas en un entorno digital cada vez más interconectado y expuesto a amenazas cibernéticas globales se ha convertido en una prioridad. En este sentido, es imprescindible comprender que la ciberseguridad en las infraestructuras críticas va más allá de las medidas tradicionales centradas en las tecnologías de la información IT. En este sentido, requiere un enfoque específico para los sistemas operativos OT, la protección de activos físicos y la colaboración estrecha entre los equipos de sistemas IT y OT.

La implementación de medidas como la segregación de redes, la aplicación de listas blancas de aplicaciones y la detección y respuesta precisas son elementos clave para garantizar la protección integral de las infraestructuras críticas.

Además, la gestión del centro operativo de seguridad OT y la integración de tecnologías emergentes como Inteligencia Artificial e Internet de las Cosas (IoT) son aspectos clave para fortalecer la ciberresiliencia de las infraestructuras, y robustece la capacidad de respuesta de empresas y organizaciones para hacer frente a posibles incidentes.

Telefónica Tech cuenta con la experiencia y conocimientos necesarios para ofrecer una propuesta integral (end-to-end) de productos y servicios especializados en ciberseguridad para infraestructuras críticas, adaptados a las necesidades específicas de cada cliente. Estos servicios incluyen desde evaluaciones para identificar y analizar los riesgos, monitorizar activos, detectar y dar respuesta a posibles incidentes, hasta la elaboración de planes directores para identificar, priorizar e implementar las soluciones necesarias.

Solo a través de un enfoque holístico y una colaboración efectiva entre los diferentes actores involucrados es posible enfrentar los nuevos desafíos cibernéticos y proteger las infraestructuras críticas de manera efectiva, esencial para garantizar la seguridad, la continuidad de las operaciones y la integridad de nuestras sociedades en un mundo cada vez más digitalizado y expuesto a amenazas cibernéticas globales.



Telefónica Tech