Eleven Paths

Ciberseguridad para la digitalización industrial

Claves para abordarla con éxito

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

Resumen ejecutivo

Las tecnologías digitales y en particular, lo que se ha convenido en llamar IoT (internet de las cosas), traen consigo un mundo de posibilidades que las organizaciones de cualquier sector no pueden dejar de aprovechar para aumentar su flexibilidad y capacidad de adaptación a los gustos y hábitos de sus clientes, mejorar los servicios que prestan mediante la monitorización continua o ser más eficientes.

Todas estas tecnologías tienen en común la necesidad de una mayor conectividad en el entorno de las organizaciones, tanto con el exterior, es decir, con sus clientes y proveedores, como internamente, consiguiendo una mayor coordinación e integración entre las diferentes organizaciones y departamentos.

Esta mayor interconexión entre áreas que recientemente estaban aisladas (e.g. sistemas de información y sistemas de operación) así como entre organizaciones que hasta ahora utilizaban procesos de interoperación menos digitales y automatizados hace que, paralelamente al proceso de transformación digital, haya un incremento de su superficie de ataque y, en consecuencia, de los riesgos de ciberseguridad a los que se expone.

A diferencia de las olas de transformación digital anteriores (explosión de los sistemas TI, dispositivos personales, cloud), en esta ocasión, los cambios se están produciendo en el núcleo de las organizaciones industriales, en sus sistemas operacionales, que son los encargados de supervisar y controlar los procesos productivos, que tradicionalmente habían estado más aislados.

Telefónica viene acompañando a sus clientes en este proceso de transformación digital desde sus mismos orígenes, ofreciéndoles soluciones y servicios especializados para afrontar los riesgos de ciberseguridad y de igual forma, continuamos adaptando y mejorando nuestra oferta para mantenernos a la vanguardia.

Este documento arranca explicando las fuerzas que empujan a la industria hacia la transformación digital y los riesgos de ciberseguridad asociados, para después presentar la metodología que sigue ElevenPaths para ayudar a nuestros clientes a abordar este reto, resaltando los aspectos diferenciales de la propuesta. Por último, se presentan dos escenarios tipo que ejemplifican dos tipos de proyectos de ciberseguridad distintos: organizaciones con fábricas tradicionales que han de adaptarse al nuevo entorno y organizaciones que están construyendo fábricas nuevas en los que la conectividad celular es un elemento clave.

01 Contexto

01.1. Factores que motivan la transformación digital de la industria

La competencia a la que están expuestas las empresas industriales las obliga a plantear constantemente iniciativas con las que adaptarse y mejorar, las cuales persiguen uno o varios de los principios que caracterizan el concepto de "Fábrica del Futuro" (Factory of the Future, s.f.):

Mayor flexibilidad para adaptarse a los gustos y hábitos cambiantes de los consumidores

Las organizaciones deben estar atentas a lo que ocurre a su alrededor, siguiendo los cambios en los gustos e intereses de sus clientes y poniendo a su disposición la posibilidad de personalizar el producto a su gusto. Uno de los ejemplos que mejor refleja esta tendencia es "Nike by you". Una iniciativa lanzada por Nike que permite al consumidor final personalizar sus zapatillas online con un diseño propio que después se le hará llegar a casa.

Digitalización del diseño, la producción y del propio producto

El principal exponente de este concepto es el "gemelo digital". Por un lado, facilita la concepción y simulación de las propiedades del producto sin recurrir a modelos físicos, así como digitalizar la producción, aumentando ahorros y eficiencia. Por otro, permite crear réplicas virtuales de los productos a fin de realizar una monitorización durante su vida útil para anticiparnos a problemas que puedan surgir. Esto tiene grandes aplicaciones en campos como el automóvil, la aviación o cualquier otro entorno en el que el desgaste de las piezas pueda tener un impacto en las vidas humanas.

Fabricación sostenible o de cero residuos

En el mundo de hoy es más importante que nunca gestionar apropiadamente las limitadas materias primas, para lo cual se necesitan soluciones digitales que permitan su seguimiento al completo, desde su extracción hasta el reciclado. Un ejemplo de esto es el de las baterías eléctricas de los automóviles. Los metales con las que se construyen podrían escasear en el futuro próximo y eso ha provocado que algunos fabricantes del sector del automóvil realicen movimientos para asegurarse su suministro. Además, la gestión de las baterías una vez construidas y a lo largo de su ciclo de vida contribuye a optimizar su uso y posterior reciclado.

Todas estas iniciativas comparten la necesidad de una mayor conectividad e integración entre las distintas áreas que componen una organización, pero también con sus clientes y proveedores con el fin de facilitar el flujo de información necesario para que los procesos de negocio fluyan con la máxima agilidad.

01.2. Ningún sector industrial escapa a esta dinámica transformadora

Como hemos visto, la necesidad de conectividad e integración con terceros empuja a una continua transformación, pero ésta no es exclusiva de un sector o vertical en particular.

En mayor o menor medida, cualquier sector de la economía cuyas operaciones son susceptibles de ser automatizadas se ve inmerso en este proceso de transformación. Algunos de esos sectores son los siguientes:

Sector sanitario
Pudiera parecer uno de los menos afectados por la digitalización, sin embargo, en cualquier hospital se pueden encontrar grandes redes de PCs, servidores y dispositivos IoT, pero también sistemas médicos especiales, como sensores, monitores, máquinas de rayos o escáneres. El correcto funcionamiento de todos los sistemas es fundamental para una operación segura que tiene un impacto directo sobre la salud de las personas.

Sector del transporte
Hoy en día depende en gran manera del uso de redes de comunicaciones y compartición de información en tiempo real. Podríamos hablar de las redes en aeropuertos o de las que hay en el interior y exterior de los trenes, que controlan sistemas tan comunes para los pasajeros como las pantallas y megafonía, pero también automatismos críticos como el frenado o el control de puertas.

Sector retail
También está plenamente embarcado en una transformación digital que ha llenado sus centros y plantas de distribución de dispositivos IoT inalámbricos que habilitan la operación a máxima velocidad de toda la logística.

01.3. Riesgos de ciberseguridad en entornos operacionales

Esa misma transformación que afecta a todos los sectores industriales y que los ayuda a mejorar su competitividad requiere afrontar un importante reto: la ciberseguridad.

La mayor parte de estos riesgos son causados por el incremento de conectividad de los sistemas industriales y la integración de unas tecnologías con otras. Esto se traduce en una mayor superficie de ataque, tanto en sistemas tradicionales como en entornos de nueva creación. En ese mismo sentido distinguimos dos tipos de escenarios.

INDUSTRIA TRADICIONAL

Ha evolucionado manteniendo los sistemas y redes, que denominaremos legados, los cuales pueden llegar a tener hasta varias décadas de antigüedad.
Esos sistemas conviven en mayor o menor medida con redes planas y ampliaciones ad hoc que se han ido añadiendo con los años. Todo esto resulta en un desconocimiento de qué hay realmente conectado a la red. Además, en general, suele regir el principio de "si funciona no lo toques", por lo que los sistemas acostumbran a estar desactualizados.

INDUSTRIA MODERNA

Tales como las de automoción, que han sido concebidas desde su diseño para implementar las últimas tecnologías de automatización y gran conectividad entre sus sistemas. Sin embargo, el time to market, las limitaciones en el presupuesto y los requerimientos de disponibilidad no siempre permiten mantener un estado de seguridad adecuado. Algunos de sus puntos débiles son los accesos remotos inseguros sin un control y trazabilidad adecuados, el uso de USBs potencialmente infectados y la gran cantidad de dispositivos IoT a gestionar.

¿Qué problemas podemos encontrar?

Falta de visibilidad: No sabemos exactamente qué hay conectado en nuestra red y cómo se está comunicando. Es imposible defender algo que no sabes que existe.

Redes planas: Una red plana significa que cualquier dispositivo se puede comunicar con cualquier otro sin restricciones.
Un atacante o virus se puede mover por toda la red sin problemas

Protocolos inseguros: El uso de protocolos antiguos, propietarios, sin cifrar ni autenticar presenta un riesgo enorme. Por ejemplo, se pueden suplantar variables, leer información privilegiada y actuar sobre los autómatas.

Software antiguo y desactualizado: Debido a la naturaleza de la operación de estos entornos es común encontrarnos con software antiguo y sin actualizar lo cual implica la acumulación de vulnerabilidades que pueden ser explotadas por un atacante para tomar control de los sistemas.

Malware (USB o email): La mayoría de los ataques se producen por infecciones de malware a través de correo electrónico o USBs infectados que también se pueden propagar por una red industrial.

Accesos remotos inseguros: Los accesos remotos por medios inseguros y sin controlar abren brechas de seguridad en las redes industriales, ya que no podemos estar seguros de quien está accediendo y qué está haciendo.

Activos físicos desprotegidos: Armarios de control sin vigilancia, salas de ordenadores abiertas, switches con bocas activadas... Todo esto también puede ser aprovechado por un atacante para causar daño.

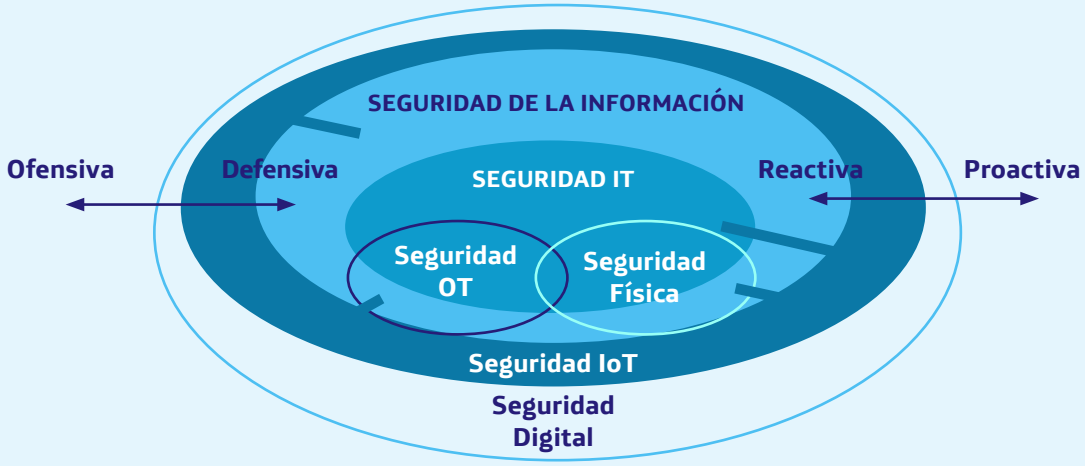
Ingeniería social: Las personas somos el eslabón más débil, la falta de concienciación hace que caigamos en la trampa de los ciberdelincuentes.

Falta de respuesta a ciber incidentes: El impacto de un ciberataque es mucho mayor si no contamos con un plan de respuesta adecuado que permita recuperarse y resolver la emergencia lo antes posible. Es probable que muchas organizaciones se vean desbordadas al contemplar el tamaño del problema y que perciban que cualquier pequeño cambio puede desbaratar el precario equilibrio de la organización que, aunque con sus ineficiencias, más o menos sobrevive al día a día.

01.4. Importancia de una ciberseguridad holística

Al considerar la transformación digital y sus riesgos es evidente que ya no podemos hablar de organizaciones aisladas con pocos puntos de conexión con el mundo exterior y que pueden defenderse fácilmente. Ahora tenemos organizaciones hiperconectadas con todos los agentes con los que se relacionan y que deben aprender a gestionar sus riesgos y protegerse en este nuevo contexto.

Una de las consecuencias derivadas es la necesidad de integrar áreas de la seguridad que tradicionalmente eran independientes, por ejemplo, la seguridad física y la seguridad IT, que ahora pueden verse conectadas por elementos como las cámaras IP o los sistemas de control de acceso digitales. Para gestionar estos riesgos es útil considerar el modelo de seguridad creado por Gartner. En él se representa los diferentes dominios de seguridad que deben tenerse en cuenta para realizar una gestión integral de los riesgos de ciberseguridad.



Modern IT security model by Gartner

Bajo este esquema, no sólo deben tratarse los riesgos de cada dominio independientemente sino también los riesgos derivados de las nuevas conexiones entre ellos. En este sentido, al conectar el dominio IT con el dominio físico, podríamos estar abriendo la puerta a que un atacante, desde la red corporativa o internet, pudiera manipular sistemas de control de acceso físico o de video vigilancia.

Ahora bien, conectar distintos dominios también trae nuevas posibilidades para la ciberseguridad. Permite la integración de diferentes tecnologías, para orquestar y automatizar acciones más complejas y efectivas en todos los dominios.

Un caso de ejemplo en el que se aprovecha esta integración entre tecnologías es el siguiente:

1. DETECCIÓN

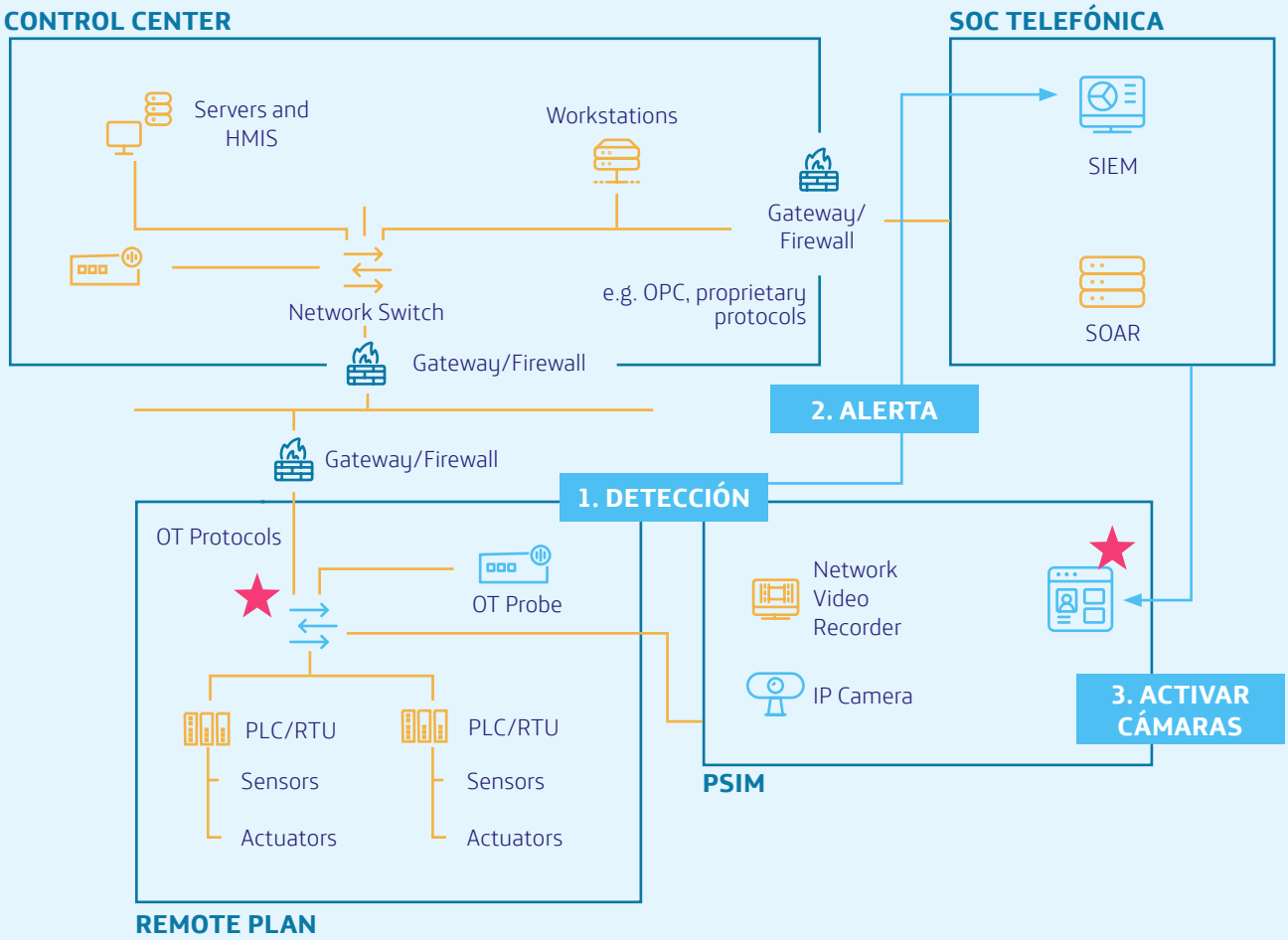
Un sistema de detección de anomalías de red instalado en una planta detecta que ha habido una nueva conexión no autorizada a un Switch de la red de control del entorno OT.

2. ALERTA

Este sistema genera una alerta que es enviada a un SIEM central que recibe y procesa eventos IT y OT, el cual comprueba si existe una orden activa de trabajo.

3. ACTIVAR CÁMARAS

Si no existía una orden de trabajo se envía una orden al centro de control de cámaras de videovigilancia para enfocar la sala donde está el switch.



02 Propuesta ElevenPaths para la ciberseguridad OT

Ante la evidente dificultad para abordar los problemas y la gestión de la ciberseguridad de este tipo de entornos industriales y en plena transformación digital ElevenPaths ha creado una propuesta para ayudar a sus clientes en esta complicada tarea.

02.1. ¿Por qué ElevenPaths?

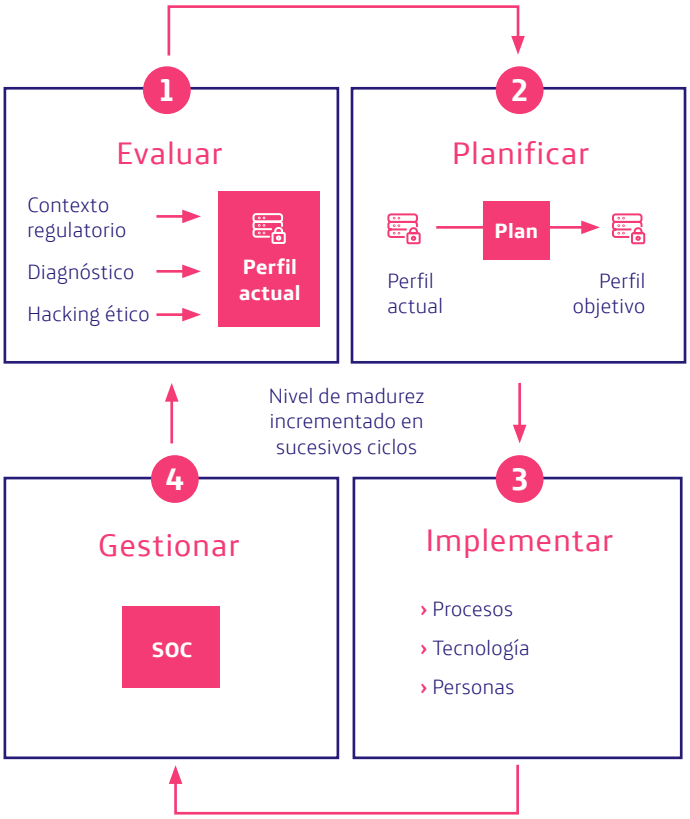
ElevenPaths, como parte del grupo Telefónica, y ahora integrado en la nueva Telefónica Cybersecurity Tech, tiene experiencia en la operación y la seguridad de entornos complejos e infraestructuras críticas como son las redes de telecomunicaciones. El compromiso con la disponibilidad, los SLAs, el cuidado en la implantación de actualizaciones y la protección de la infraestructura ante ataques de cualquier naturaleza forman parte del ADN de Telefónica desde hace más de cien años. Por ello, nuestro equipo comprende las preocupaciones y necesidades de sus clientes industriales.

De hecho, Telefónica no solo se dedica a la protección de las redes de manera lógica, si no también física. Desde hace más de 30 años Telefónica Ingeniería de Seguridad ha operado proyectos de seguridad física para infraestructuras críticas, tales como pozos petrolíferos, aeropuertos, túneles para trenes de alta velocidad, entre otros muchos. Telefónica también es proveedor de servicios de Cloud, conectividad y gestión para redes de dispositivos IoT y por supuesto de seguridad para todos ellos.

Por ello, en ElevenPaths tenemos un equipo multidisciplinar con una amplia experiencia en la Ciberseguridad aplicada a multitud de sectores como la banca, redes IoT, los comercios online o las redes industriales. De esta manera podemos crear una propuesta completa para la seguridad actual y futura de las organizaciones industriales.

02.2. Metodología METEO

Para abordar el reto de la ciberseguridad industrial ElevenPaths ha creado METEO (Metodología ElevenPaths para Tecnologías y Entornos Operacionales), una metodología propia basada en un proceso cíclico con el que incrementar el nivel de seguridad con cada iteración. El proceso consta de cuatro pasos:



› **Evaluar:** Se evalúa el estado de seguridad actual usando como referencia los estándares aplicables como IEC 62443 o NIST 800 82 para generar un informe del estado de la seguridad y recomendaciones de mejora.

› **Planificar:** En la fase de planificación se establece un nivel objetivo de madurez que se quiere alcanzar en la iteración y se decide qué medidas se van a usar para alcanzarlo, tanto tecnológicas como organizativas.

› **Implementar:** Durante la implementación se ejecutan los cambios y soluciones de ciberseguridad planificadas, con un seguimiento detallado de los objetivos y pruebas de verificación.

› **Gestionar:** Por último, queda gestionar las medidas que se han adoptado, para ello se da toda la documentación y formación necesaria y se ofrece la gestión por parte de Telefónica desde su SOC.

Para cada uno de estos pasos, ElevenPaths dispone de una serie de tecnologías y procedimientos que ha ido mejorando y adaptando en el tiempo, asimilando la experiencia adquirida en distintos proyectos y clientes.
En los siguientes apartados se resaltarán esos valores diferenciales de la propuesta de ElevenPaths.

02.3. Evaluar y planificar

En ElevenPaths creemos que el proceso de evaluación de una infraestructura industrial debe incluir dos aspectos principales.

El primero es el trabajo de **consultoría clásica**, basada en la comprensión de los procesos industriales, los riesgos, las prácticas de ciberseguridad y, en definitiva, toda información que se recoge a partir de entrevistas.

El segundo es el **análisis técnico**, utilizando herramientas de última generación para inspeccionar los activos y redes OT, siempre de una forma eminentemente pasiva, controlando concienzudamente cualquier impacto sobre la producción.

Para ello hemos creado una herramienta a la que hemos denominado ASPI_™ (Analizador de Seguridad de Plantas Industriales). Esta herramienta incorpora diversas tecnologías para evaluar la ciberseguridad de las redes y activos, tales como analizadores de protocolos OT, IT o de IoT médico, capturadoras de tráfico y conectividad remota. ASPI_™ nos permite hacer un diagnóstico técnico de manera ágil y, si es necesario, de forma remota, minimizando al máximo los costes. Este diagnóstico permite tener una primera idea de los puntos de mejora más notables en la ciberseguridad de la organización a partir de los cuales priorizar y planificar los siguientes pasos a seguir, que enriquecerán esos trabajos de consultoría clásica, tales como:

› **Evaluación de madurez:** La evaluación de madurez permite conocer en qué medida se aplican las mejores prácticas de ciberseguridad industrial en la organización, para lo que utilizamos algunas de las referencias y normativas más reconocidas y usadas en la materia. El resultado es un "análisis GAP" que permite trazar la hoja de ruta para mejorar la postura de ciberseguridad de la organización, tanto a nivel técnico como organizacional y cultural.

› **Análisis de riesgos:** Mientras la evaluación de madurez evalúa las actividades y procesos de la organización frente a las buenas prácticas, el análisis de riesgo permite identificar los riesgos específicos que afectan a la organización en sus activos industriales para tomar mejores decisiones, optimizando los recursos y dirigiendo las inversiones a los proyectos de mitigación de riesgos más relevantes.

› **Auditoría:** Una auditoría permite comparar de forma rigurosa el nivel de seguridad y cumplimiento frente a alguna norma, como pueden ser ISO 27000 e IEC 62443.

Una vez obtenidos los resultados de las actividades de evaluación se inicia la fase de planificación en la que nuestro equipo de expertos, junto al personal designado por el cliente, aborda esos resultados para obtener las claves de la situación actual.

A continuación, se establecen los objetivos a los cuales se quiere llegar en esa iteración basándose en múltiples criterios tales como la urgencia de algunos riesgos, las necesidades regulatorias, el tiempo de implementación y el presupuesto disponible de tal forma que se maximicen los beneficios obtenidos.

Finalmente, dados esos objetivos, se crea un plan de proyectos que sirve como camino a seguir para lograr los propósitos iniciales.

02.4. Implementar

La fase de implementación puede ser tremendamente compleja, empezando por la cuestión de qué tecnología instalar, de qué fabricante o cómo se integrará con el resto de los sistemas y procesos de la empresa.

En los últimos tiempos hemos visto como el panorama de soluciones de seguridad cambia casi de una semana para otra, con adquisiciones de empresas nuevas por parte de otras más grandes y establecidas, inclusión de nuevas funcionalidades, giros para abarcar nuevos entornos, anuncios de integraciones entre varias tecnologías, etc.

Por eso es muy importante mantenerse actualizado, conocer en profundidad todas las soluciones disponibles, sus diferencias y puntos fuertes y aplicar en cada caso la más conveniente aprovechando las sinergias entre unas y otras.

Para ello en ElevenPaths contamos con varios laboratorios en los que probar todas las tecnologías con las que después trabajamos. En ellos se verifican las funcionalidades anunciadas, se hacen comparativas de rendimiento entre unas y otras y se prueban las últimas novedades e integraciones, generando así un conocimiento de gran utilidad para nosotros y nuestros clientes.

Además, ElevenPaths tiene alianzas con los principales fabricantes y participa en múltiples alianzas para colaborar en la mejora de las tecnologías de ciberseguridad.

ElevenPaths ofrece un amplio abanico de soluciones, adaptables a todos los entornos y niveles de madurez, con los que ayudar a sus clientes a mejorar aspectos concretos de su ciberseguridad.

Segregación
Permite hacer que las **redes OT solo sean accesibles por las conexiones estrictamente necesarias**, mejorando así la seguridad perimetral.

Segmentación
La segmentación divide la red en zonas y conductos, agrupando activos para una **gestión más sencilla y un control total de las comunicaciones** entre ellos.

Monitorización
La monitorización p**ermite detectar ataques en las redes OT e IoT**, buscando tanto patrones malignos conocidos como anomalías sobre la operación normal de la red que indiquen un posible ataque.

Accesos remotos seguros
Para asegurar los accesos remotos con una plataforma unificada que además de dar seguridad a las conexiones permite también **monitorizarlas, controlar a los usuarios y dar acceso** únicamente a los activos necesarios.

Protección USB
Esta solución **defiende los activos de la infección de malware a través de USBs** y también de ataques eléctricos como los de los USBKiller.

Cyber Deception
Permite **adelantarse a los atacantes, creando campañas de engaño** a la medida de la organización para descubrir sus técnicas e intereses y llevar a cabo una defensa activa.

Formación y concienciación
La formación y concienciación de las personas es una medida fundamental para la seguridad de una organización. Pueden darse cursos generales o especialistas, por ejemplo, específicos sobre ciberseguridad industrial.

Cyber Range
Los ejercicios de cyber range sirven para **formar a las personas mediante juegos de ciberseguridad** con entornos, herramientas y ataques realistas.

02.5. Gestionar

La gestión de la ciberseguridad es un aspecto tan importante o más que el resto ya que, por mucha tecnología que se instale, si no se gestiona adecuadamente, su utilidad a la hora de defender a la organización será cada vez menor, provocando únicamente estorbos a los trabajadores y a los procesos.

Por ello se cuenta con SOCs o Centros de Operaciones de Seguridad. Estos centros gestionan tecnologías tales como los firewalls o las sondas de monitorización, manteniéndolos siempre actualizados y bien configurados para su uso diario, reduciendo así las molestias para el cliente y liberando a su área de sistemas o IT. Por otro lado, estos centros también trabajan en la integración de tecnologías, de manera que, por ejemplo, los firewalls, las sondas y los logs de otros dispositivos se coordinen y sean aprovechados conjuntamente en un SIEM.

Finalmente, los SOCs son los encargados de coordinar y dar respuesta cuando se produce un incidente de ciberseguridad, en cuyo caso se trabaja también en la automatización de la respuesta para que sea más rápida y efectiva.

ElevenPaths cuenta con un SOC inteligente a nivel global, distribuido en varias sedes alrededor del mundo, para la operación 24x7 todos los días del año. Estas son algunas de sus características:

Global Unified Costumer Portal: Se provee al cliente de un portal unificado que reúne paneles con información detalla e indicadores, visión completa de la postura de seguridad de la organización y con integraciones de todas las fuentes necesarias.

Threat Intelligence Platform: La plataforma de inteligencia de amenazas permite conocer el contexto de adversarios que aplica al perfil de riesgos y genera TTPs e IoCs enfocados en los casos de los clientes para mejorar sus defensas.

Orchestration and automation: La orquestación y automatización de la respuesta a casos de uso como phishing, escaneos de puertos o alertas del SIEM permite grandes mejoras en la operación, reduciendo el tiempo de exposición y estandarizando la respuesta.

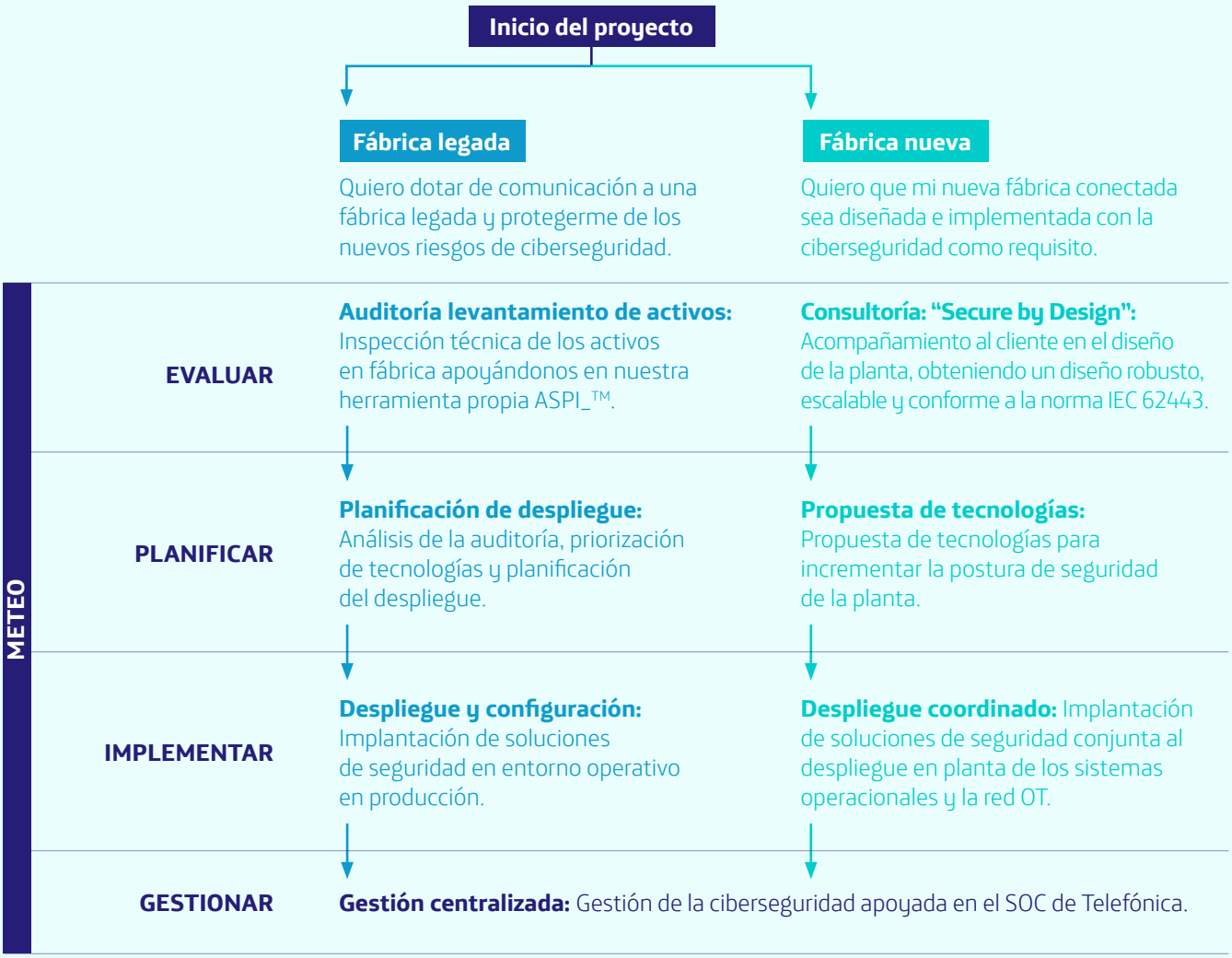
Managed Detection and Response: La gestión de detección y respuesta está en el núcleo de la oferta del iSOC, con capacidades de EDR y detección rápida por telemetría, contra inteligencia y campañas de engaño para aprender de los adversarios y servicios de DFIR llegado el caso.

03 Aplicación de METEO a entornos OT

La metodología de ElevenPaths es aplicable a todo tipo de sectores, niveles de madurez y clientes.
A la hora de planificar un proyecto de ciberseguridad industrial sobre un entorno productivo concreto, debemos diferenciar entre fábricas de nueva creación y fábricas que ya están en operación. En ambos casos se podrán identificar, planificar y ejecutar acciones para mejorar el nivel de resiliencia del entorno, pero en el primer caso, podrán realizarse desde la misma fase de diseño, lo cual resulta altamente recomendable.

En el siguiente esquema se describen resumidamente las distintas fases del proceso a seguir en cada caso.

METEO: Metodología ElevenPaths para Tecnologías y Entornos Operacionales



Si quieres conocer más sobre nuestra metodología y porfolio y cómo puede aplicarse a tu caso, no dudes en ponerte en contacto con nosotros a través de communications@11paths.com.

Sobre ElevenPaths

ElevenPaths es la compañía de ciberseguridad de Telefónica, integrada dentro del holding Telefónica Tech, que aglutina los negocios digitales con mayor potencial de crecimiento de la compañía.

En un mundo en el que las ciberamenazas son inevitables, como proveedores de servicios de seguridad gestionada inteligente, nos enfocamos en prevenir, detectar, dar respuesta y disminuir los posibles ataques a los que se enfrentan las empresas. Garantizamos la ciber-resiliencia de nuestros clientes a través de un soporte 24/7 gestionado desde once i-SOC alrededor del mundo con capacidad operativa global.

Creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y, de esta manera, logramos ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Trabajamos para garantizar un entorno digital más seguro a través de alianzas estratégicas que nos permitan mejorar la seguridad de nuestros clientes, así como a través de colaboraciones con organismos y entidades líderes como la Comisión Europea, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, EuroPol, Incibe, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Centro de Ciberseguridad Industrial (CCI) y APWG.

Más información:
elevenpaths.com | @ElevenPaths | blog.elevenpaths