Basque CyberSecurity Centre

PROYECTOS TIPO DE CIBERSEGURIDAD INDUSTRIAL

Los receptores de la información solo podrán compartirla con miembros de su propia organización y con cliente y proveedores que necesiten conocerla para protegerse a símismos o evitar daños mayores.
El emisor puede especificar restricciones adicionales para compartir esa información.

Basque CyberSecurity Centre

ÍNDICE

1. Esquema general

1.1 Contexto

1.2 Estructura

1.3 Detalle de proyectos desarrollados

1.4 Propuesta para la puesta en marcha de los proyectos de ciberseguridad

2. Detalle de los proyectos

2.1 Diseño e implantación de arquitecturas seguras en redes industriales

2.2 Securización de los accesos remotos OT

2.3 Evaluación de la seguridad de la información / datos industriales

2.4 Evaluación y mejora del software industrial en las plantas

2.5 Formación y Concienciación

2.6 Plan de ciberseguridad industrial

2.7 Adopción de buenas prácticas de estándares

2.8 Medidas de protección de información estratégica o sensible

2.9 Monitorización de seguridad industrial

Basque CyberSecurity Centre

.01

ESQUEMA GENERAL

1.1 Contexto

No cabe duda de que la ciberseguridad es uno de los grandes retos a los que se enfrentan actualmente las empresas, y especialmente las de entornos industriales. Y no es algo circunstancial. La enorme cantidad de ciberataques que se están constatando diariamente tienen una serie de características comunes:

- Por norma general son ataques indiscriminados que no tienen un objetivo fijo entre las posibles víctimas, y en mucha menor medida, ataques dirigidos.
- Son muy virulentos, lo que puede ocasionar un impacto muy elevado en las organizaciones que los sufren, incluso provocando cuantiosas pérdidas o el cierre de las mismas.
- Reportan grandes beneficios a los grupos cibercriminales que los ejecutan, por lo que estos grupos están destinando cada vez más medios y recursos para la comisión de este tipo de delitos.

A lo anterior se suma que hasta hace relativamente poco tiempo, la ocurrencia de un ciberataque en un entorno industrial era una anécdota que se publicaba exclusivamente en prensa especializada y generalmente ligada a incidentes en grandes empresas o infraestructuras críticas (red eléctrica en Ucrania, central nuclear en Irán, etc.), lo que ocasionaba cierta sensación de lejanía debido precisamente a la distancia y al tipo de empresa. Pero lo cierto es que actualmente los incidentes registrados en empresas locales han pasado a ser portada de medios generalistas, por lo que la alarma social en torno a la ciberseguridad es muy elevada.

En el ámbito de la ciberseguridad industrial, se podría afirmar incluso que la incidencia de un ciberataque tiene consecuencias más elevadas, debido a una serie de factores, como:

- Las medidas de ciberseguridad tradicionalmente se han aplicado buscando la protección exclusiva de la información que gestiona una empresa, pero no se ha considerado la protección en si misma de la disponibilidad, confidencialidad o integridad de los propios sistemas de control industrial.
- Lo cierto es que la conexión de los sistemas de control industrial a las redes corporativas es un hecho relativamente reciente, dado que se concibieron, en su momento, como sistemas aislados. Esto genera un problema adicional, ya que para su diseño original no se contempló la ciberseguridad como un requisito funcional adicional, lo que requiere de un mayor esfuerzo para la adecuada protección de los mismos.
- Las consecuencias de la materialización de un incidente de seguridad en un entorno industrial pueden tener consecuencias imprevisibles, directamente relacionadas con magnitud de los sistemas afectados, en diferentes órdenes: paradas no programadas de los sistemas de producción, imposibilidad de fabricación, incumplimiento en el suministro de pedidos, cancelación de contratos o penalizaciones como consecuencia de incumplimientos de niveles de servicio acordados en contratos, pérdida de imagen de confianza en el sector y en los clientes, etc.

Por lo tanto, y considerando que las empresas industriales se han convertido en un objetivo principal de los ciberdelincuentes, parece claro que la pervivencia de las empresas pasa necesariamente por disponer de un nivel de seguridad adecuado acorde al nivel de riesgo que presenta su actividad, lo que pasa, inevitablemente, por la puesta en marcha de proyectos de ciberseguridad como los que se presentan a continuación.

1.2 Estructura

Se pretende proporcionar, de una forma estructurada y con contenidos explicados de forma sencilla, el detalle de una serie de proyectos de ciberseguridad que deberían ser contemplados, en algún momento, por cualquier empresa de ámbito industrial.

Esta información proporciona una base para que las empresas industriales entiendan la necesidad de acometer proyectos de ciberseguridad, y puedan solicitar, con un mayor conocimiento de causa, enfoques de colaboración proporcionados por las empresas especialistas del sector, que además aparecen listadas en el "Libro blanco de la Ciberseguridad en Euskadi", publicado por el BCSC.

Cada proyecto se encuentra estructurado de la siguiente forma:

- Una **descripción** de la tipología del proyecto, que permite contextualizar el mismo dentro de las posibles necesidades de la empresa.
- Los **objetivos** que se persiguen con la puesta en marcha del proyecto.
- Los **beneficios** que se alcanzarían con la implantación plena del proyecto. El nivel global de beneficios se representa asimismo de forma gráfica en términos de reducción del nivel de riesgo.
- **Dimensiones de la ciberseguridad que mejora la ejecución del proyecto**, tomando como referencia las fases de la ciberseguridad definidas por el NIST (National Institute of Standards and Technology) y aceptadas como referencia por la comunidad internacional: Identificar, Proteger, Detectar, Responder y Recuperar. Se resaltan las dimensiones que mejora el proyecto.
- Una orientación en cuanto a los **tiempos estimados de ejecución del proyecto**. Lógicamente totalmente ligados a la dimensión del proyecto a llevar a cabo.
- **Requerimientos de dedicación de recursos de las empresas solicitantes**, que pretende señalar, de forma gráfica, la dedicación del personal interno de la organización al proyecto, considerando que el mismo se ejecuta de la mano de una empresa especializada externa.
- Una relación de algunas **buenas prácticas** que sería conveniente considerar a la hora de plantearse la ejecución del proyecto, y que en algún caso pueden ser limitantes para alcanzar los objetivos del mismo.
- Los **servicios relacionados** de forma habitual con la ejecución del proyecto, en relación a la tipología de actividades a llevar a cabo.
- **Otros proyectos relacionados** que mantienen una estrecha relación con el propio proyecto.
- **Área de proyecto subvencionable en el programa de ayudas de ciberseguridad industrial del Centro Vasco de Ciberseguridad (SPRI)** en la que se encuadra el proyecto, de acuerdo a lo establecido en las bases que regulan el mismo.
- **Perfil de empresa suministradora de servicios o productos**, que proporciona una indicación de acuerdo a las capacidades que debería presentar la empresa especializada encargada de la ejecución del proyecto, de acuerdo a la categorización registrada en el "Libro blanco de la Ciberseguridad en Euskadi".

Es importante considerar que todas las valoraciones indicadas se han realizado con carácter general, por lo que la situación, contexto y necesidad de una empresa industrial en concreto puede tener una valoración específica que puede diferir en las aquí representadas.

Basque CyberSecurity Centre

1.3 Detalle de proyectos desarrollados

A continuación, se muestra, a modo de resumen, una relación de los proyectos desarrollados.

DISEÑO E IMPLANTACIÓN DE ARQUITECTURAS SEGURAS EN REDES INDUSTRIALES

Beneficios	Tiempo estimado de ejecución	Requerimiento de dedicación de recursos internos
		

SECURIZACIÓN DE LOS ACCESOS REMOTOS OT

Beneficios	Tiempo estimado de ejecución	Requerimiento de dedicación de recursos internos
		

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN / DATOS INDUSTRIALES

Beneficios	Tiempo estimado de ejecución	Requerimiento de dedicación de recursos internos
		

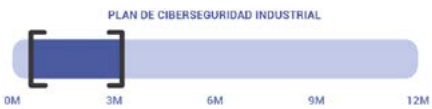
EVALUACIÓN Y MEJORA DEL SOFTWARE INDUSTRIAL EN LAS PLANTAS

Beneficios	Tiempo estimado de ejecución	Requerimiento de dedicación de recursos internos
		

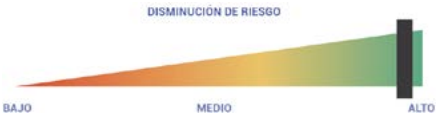
FORMACIÓN Y CONCIENCIACIÓN

Beneficios	Tiempo estimado de ejecución	Requerimiento de dedicación de recursos internos
		

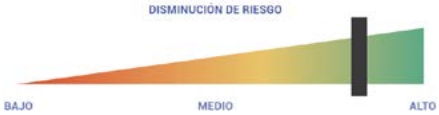
PLAN DE CIBERSEGURIDAD INDUSTRIAL

Beneficios	Tiempo estimado de ejecución	Requerimiento de dedicación de recursos internos
		

ADOPCIÓN DE BUENAS PRÁCTICAS DE ESTÁNDARES

Beneficios	Tiempo estimado de ejecución	Requerimiento de dedicación de recursos internos
		

MEDIDAS DE PROTECCIÓN DE INFORMACIÓN ESTRATÉGICA O SENSIBLE

Beneficios	Tiempo estimado de ejecución	Requerimiento de dedicación de recursos internos
		

MONITORIZACIÓN DE SEGURIDAD INDUSTRIAL

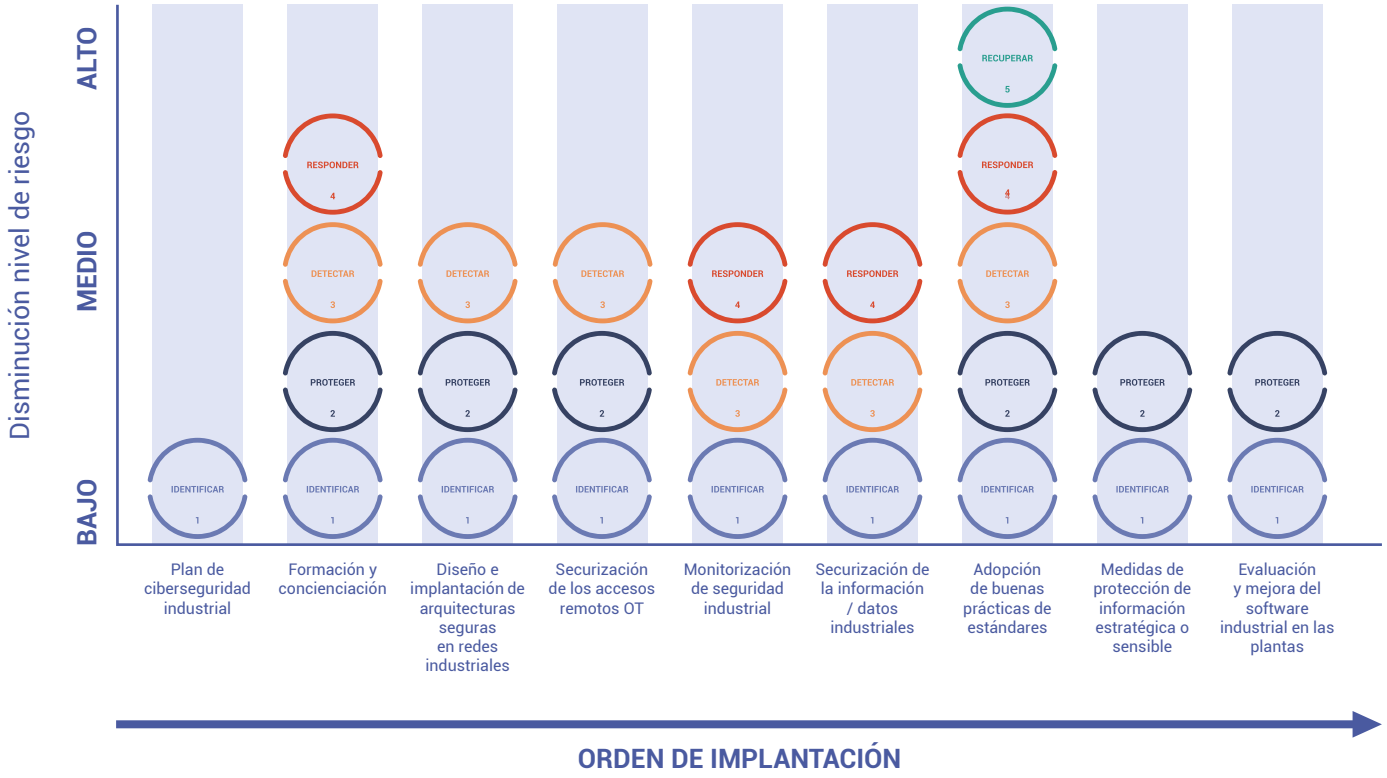
Beneficios	Tiempo estimado de ejecución	Requerimiento de dedicación de recursos internos
		

1.4 Propuesta para la puesta en marcha de los proyectos de ciberseguridad

La realización de proyectos de ciberseguridad puede venir dada por varios motivos:

- Por la necesidad motivada de dar respuesta a una situación de amenaza específica, que mitiga o disminuye el nivel de riesgo identificado.
- Dentro de un contexto en el que los proyectos de ciberseguridad se abordan desde una perspectiva de planificación priorizada y ordenada, con el objetivo de alcanzar un nivel de riesgo asumible por la organización.
- Por requisitos contractuales de clientes y proveedores.

Para ilustrar cual sería un recorrido lógico de puesta en marcha de los proyectos de ciberseguridad desarrollados, el punto de partida es una empresa que no ha llevado a cabo ninguna iniciativa en este ámbito, y que necesita ponerse en marcha de forma ordenada. La propuesta sería, por lo tanto:



No cabe duda, en cualquier caso, que el orden de implantación mostrado en la gráfica anterior puede no encajar con la singularidad y circunstancias concretas de cada empresa, por lo que simplemente debe tomarse a modo orientativo.

Basque CyberSecurity Centre

.02

DETALLE DE LOS PROYECTOS

2.1 Diseño e implantación de arquitecturas seguras en redes industriales

DESCRIPCIÓN DEL PROYECTO

Si bien hasta hace relativamente poco tiempo era frecuente que las redes IT y OT no estuvieran ni física ni lógicamente conectadas, lo cierto es que en la actualidad la interoperabilidad entre estos dos entornos se ha convertido, en muchos de los casos, en una necesidad requerida para la operativa habitual de los procesos industriales.

En este sentido, la coexistencia de elementos característicos de las redes IT y OT en una misma red lógica para dotarles de visibilidad y capacidad de interacción mutua, es una consecuencia de una implementación de red básica en el que no se han considerado premisas de ciberseguridad ni en su diseño y, desde luego, ni en su implementación. Este modelo se ha basado en una confianza plena de las redes internas considerando que el tráfico interno es confiable, muy lejos de la práctica actual más habitual del modelo "Zero trust", en las que las redes internas de las organizaciones, tanto en IT como en OT, tienen la misma consideración frente al riesgo que el que pudieran tener las redes externas o públicas (como, por ejemplo, Internet).

Asimismo, hay que considerar que los elementos de las redes OT suelen encontrarse en un alto grado de riesgo debido a la falta de medidas de seguridad desplegadas sobre los mismos, en muchos casos por carencias asociadas a su antigüedad, configuraciones relajadas, falta o imposibilidad de actualizaciones, Sistemas Operativos obsoletos, … así como el uso de protocolos de comunicaciones característicos de este entorno, en el que la ciberseguridad no se consideró en el diseño de los mismos, por lo que las comunicaciones sin autenticación entre extremos o la inexistencia de cifrado en las comunicaciones, por ejemplo, permiten su compromiso de forma relativamente sencilla.

Por último, y no menos importante, nos encontramos con los requerimientos de conectividad que requieren terceros (ingenierías, fabricantes, etc.) para dar soporte y/o mantenimiento a los sistemas industriales presentes, así como las necesidades de conectividad necesarias para proyectos relacionados con la captación de datos en planta con fines de explotación de los mismos para mejora de los procesos productivos, mantenimientos productivos, etc.

La base fundamental, por lo tanto, se centra en disponer de una arquitectura de red y seguridad que permita:

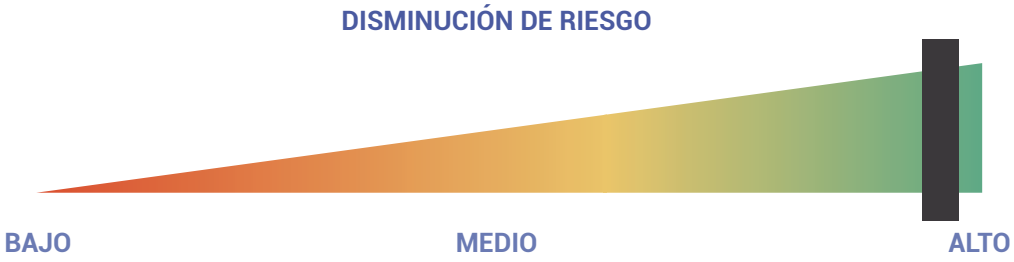
- Realizar una separación de los entornos IT/OT, mediante una adecuada configuración de la electrónica de red, así como con el uso de elementos de seguridad (cortafuegos) que permitan limitar y monitorizar las comunicaciones que se produzcan entre ambos entornos.
- Realizar una segmentación de las redes OT, mediante la definición de redes adicionales (o "zonas") dentro de cada uno de estos entornos que permitan: 1) incluir en estas zonas elementos que comparten una funcionalidad o una finalidad común, y 2) limitar las comunicaciones (o "conductos") a aquellos tráficos explícitamente autorizados.

OBJETIVOS

Los objetivos que persigue este proyecto son los siguientes:

- Realizar un diseño de una arquitectura de red IT/OT segura, contemplando todas las medidas necesarias que permitan la separación de los entornos IT y OT, así como la definición de zonas y conductos adecuados, a través de configuraciones en la electrónica de red, uso de cortafuegos, inspección de tráfico, etc.
- Partiendo de un diseño de red segura predefinido, llevar a cabo la implementación del mismo mediante la adquisición y puesta en marcha de los elementos de seguridad necesarios y adecuados a cada uno de los entornos.

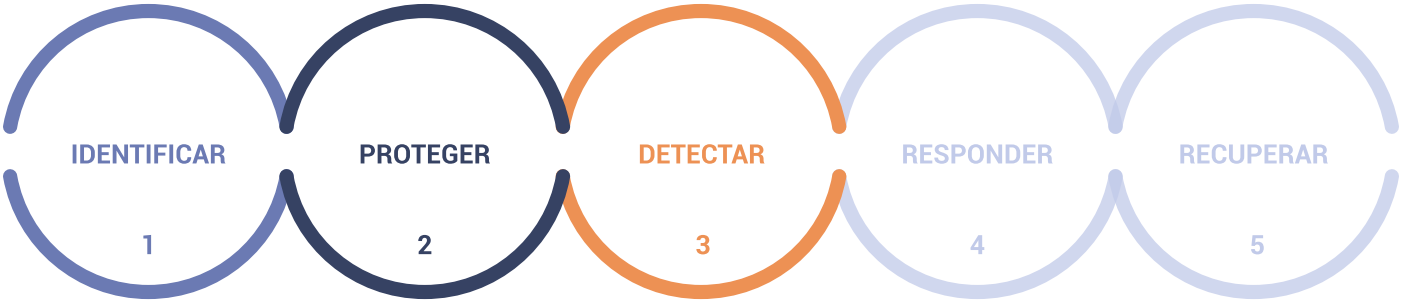
BENEFICIOS



Los beneficios que se alcanzarían con la puesta en marcha de este proyecto serían los siguientes:

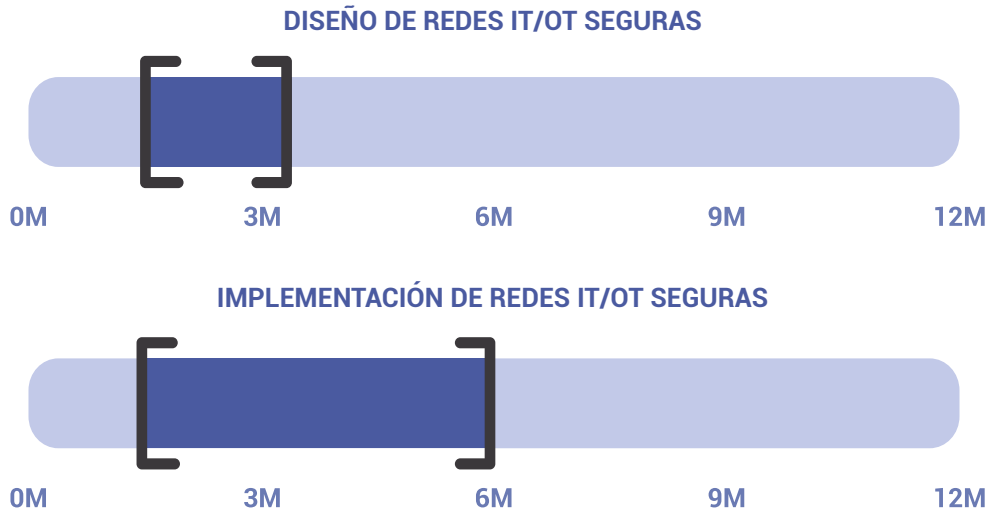
1. Contribuir a asegurar la continuidad del negocio.
2. Mejorar el nivel de resiliencia frente a las ciberamenazas.
3. Identificar las comunicaciones y los distintos elementos que las generan, permitiendo aquéllas que sean estrictamente necesarias.
4. Realizar un análisis del tráfico actual y detección de posibles anomalías ya existentes dentro de la organización.
5. Disponer de un diseño de red adecuado, escalable y gestionable desde la perspectiva de la gobernanza de seguridad.
6. Disminuir el impacto en la organización como consecuencia de la materialización de un incidente de seguridad, dado que un correcto establecimiento de zonas y conductos limitaría el mismo a la zona afectada.
7. Reducir el grado de exposición y visibilidad de los activos industriales dentro de la red.
8. Disponer de una monitorización del tráfico de red interzonas, permitiendo la identificación de tráfico no autorizado de forma que puedan analizarse las causas y naturaleza del mismo.
9. Posibilidad de detección de tráfico malicioso (IDS) que pudiera producirse interzonas y entornos, pudiendo llegar a implementar reglas de reacción o de protección automatizadas (IPS).
10. Posibilitar la implementación de una arquitectura de accesos seguros de terceros a las redes corporativas, mediante la creación de zonas específicas para conexiones externas y zonas de salto.

DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO



TIEMPOS ESTIMADOS DE EJECUCIÓN

Los tiempos estimados de ejecución de este tipo de proyectos se indican únicamente a modo orientativo ya que los mismos dependen fuertemente de factores como: tamaño y complejidad de la red, número de zonas y conductos a definir, conocimiento del estado actual del entorno, etc.



REQUERIMIENTOS DE DEDICACIÓN DE RECURSOS DE LAS EMPRESAS SOLICITANTES

BUENAS PRÁCTICAS DURANTE SU EJECUCIÓN

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar una serie de cuestiones importantes:

- Colaboración IT/OT: los proyectos de diseños de redes requieren generalmente de la participación activa tanto del personal de IT como del de OT, dado que en ocasiones los límites de la "propiedad" de la red en ambos entornos pueden encontrarse difuminados. Por lo tanto, es fundamental contar con la participación activa en el proyecto tanto con los técnicos de redes del Área de IT como del personal del Área de Producción/Mantenimiento/Operación/... que puedan aportar información y conocimiento de la infraestructura existente. Se recomienda el uso de equipos multidisciplinares.
- Contexto industrial: el diseño de la arquitectura de red de una planta requiere conocer exhaustivamente el modelo de funcionamiento de los sistemas de control industrial presentes en la misma, así como las necesidades de interconexión con otros elementos que, en función del grado de integración existente, pudieran encontrarse situados en el entorno OT o IT.
- Inventario de activos: resulta difícil analizar y diseñar un modelo de red sin saber qué es lo que se encuentra conectado a la misma, por lo que un inventario, al menos básico, es el punto de partida que permite establecer la relación entre el contexto industrial y el mundo físico. Resulta importante igualmente identificar las comunicaciones que estos establecen con otros equipos y sistemas corporativos tanto estos se encuentran desplegados en las instalaciones como en plataformas Cloud.

Criticidad de los activos: esta característica determina el nivel de protección que debe contemplarse en función de la criticidad de los activos dentro de un proceso industrial o en función del nivel de riesgo que representen, y podría materializarse en la necesidad de establecer zonas de red con mayor nivel de seguridad que otras.

Posibilidad de modificaciones en los sistemas de control industrial: es frecuente que un rediseño de una red de planta implique la realización de cambios en los direccionamientos de determinados elementos, pero hay que considerar que no siempre es posible llevarlos a cabo: impacto económico de los cambios, incertidumbre de funcionamiento, ventanas horarias para la realización de cambios, contratos con terceros que lo impiden expresamente, … hay que considerar estos factores como posibles limitantes y adaptar el diseño de la red a las posibilidades existentes.

SERVICIOS RELACIONADOS

Para el diseño de las arquitecturas de redes IT/OT seguras:

- Servicios de consultoría especializado en entornos industriales.

Para la implantación de arquitecturas de redes IT/OT seguras:

- Suministro, instalación, configuración y puesta en marcha de equipamiento de seguridad: cortafuegos, cortafuegos nueva generación (NGFW).
- Servicios para la instalación, configuración y puesta en marcha de infraestructura de red (switches, puntos de acceso, etc.)

OTROS PROYECTOS RELACIONADOS

- Diseño y/o implementación de arquitecturas de accesos remotos seguras.

ÁREA DE PROYECTO SUBVENCIONABLE EN EL PROGRAMA DE AYUDAS DE CIBERSEGURIDAD INDUSTRIAL

- Convergencia e integración de los sistemas de protección ante ciberataques para entornos IT / OT (Information Technology / Operational Technology). Diseño y ejecución de arquitecturas seguras y en su caso materialización de la segmentación de redes industriales.

PERFIL DE EMPRESA SUMINISTRADORA DE SERVICIOS O PRODUCTOS

Las empresas que cuentan con la capacidad de prestación de los servicios incluidos en este tipo de proyectos, y que se encuentran registradas en el "Libro blanco de la Ciberseguridad en Euskadi" son aquellas que se encuentran encuadradas en la siguiente categorización:

Capacidad	Categoría de la solución	Grupo de producto / servicio
PROTEGER	Tecnología de protección	Seguridad Wireless Acceso remoto/VPN Firewall /Firewall de próxima generación Gestión unificada de amenazas (UTM)

2.2 Securización de los accesos remotos OT

DESCRIPCIÓN DEL PROYECTO

La creciente conectividad de los sistemas de control industrial (SCI) a las redes corporativas de las empresas está permitiendo una nueva forma de prestación de servicios tanto por parte del personal interno de las empresas, así como por parte de los proveedores.

La posibilidad de establecer conexiones remotas a los SCI facilita aumentar la calidad del servicio prestado por terceros desde diferentes perspectivas:

- Mejora de los tiempos de respuesta frente a malfuncionamientos o incidencias.
- Optimización de los recursos para intervenciones que no requieren presencia física en la planta.
- Posibilitar la captura de datos de los SCI para tareas relacionadas con mantenimiento preventivo, optimización y mejora de procesos industriales, etc.
- Reducción de costes por desplazamiento de técnicos y operarios especializados.

Por otro lado, y considerando el aumento de los escenarios de teletrabajo, las conexiones remotas de personal propio han adquirido una importancia fundamental para el correcto desarrollo de las funciones habituales.

En este sentido, y si bien en relación a las conexiones de personal propio es habitual que las mismas se establezcan a través de los sistemas VPN corporativos, en el entorno OT es frecuente que cada ingeniería o fabricante, de los múltiples que podemos encontrarnos en una misma planta, disponga de medios de acceso remoto propios, y que:

- En el mejor de los casos, estos dispositivos o sistemas se encuentran en conocimiento de la empresa propietaria de la instalación, aunque no gestionados por ella.
- Pueden no utilizar necesariamente la red corporativa para establecer las conexiones remotas, sino redes de tipo móvil (4G, etc.).
- Se desconoce la configuración de seguridad de estos elementos, por lo que políticas relajadas podrían permitir una visibilidad excesiva ya no sólo de los elementos bajo la responsabilidad por parte del proveedor, sino del resto de elementos de las redes corporativas.
- Al no existir una gestión de las conexiones por parte de la empresa final, se desconoce la respuesta a tres preguntas básicas sobre el establecimiento de conexiones: quién, cuándo y para qué.
- La inexistencia de una regulación contractual de este tipo de accesos dificulta la asignación de responsabilidades en caso de ocurrencia y materialización de un incidente de seguridad a través de este medio, atribuible a un proveedor.

En definitiva, hay que considerar que la existencia de medios de acceso remoto al corazón de las plantas puede convertirse, si éstos no se encuentran correctamente diseñados, instalados y gestionados, en una amenaza a la seguridad de las redes corporativas. La falta de medidas de seguridad y control en las conexiones puede causar que:

- Una política de seguridad de accesos remotos relajada o poco restrictiva pueda ser utilizada por un tercero no autorizado para comprometer las redes internas de la empresa, lo que puede suponer, en caso de que se materialice, un impacto de consecuencias elevadas.
- Una incidencia de seguridad en nuestro proveedor se extienda a nuestra infraestructura. Es lo que se denomina ataque mediante la cadena de suministro.

OBJETIVOS

Los objetivos que persigue este proyecto son los siguientes:

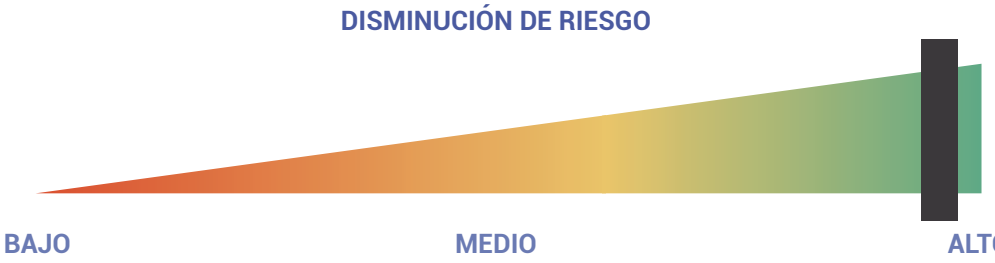
Establecer un modelo de accesos remotos al entorno OT que permita a la empresa disponer de los recursos necesarios

para mantener una gestión y visibilidad total sobre las conexiones que se establezcan bien desde personal interno como desde terceros.

Determinar la arquitectura tecnológica que permita mantener un equilibrio adecuado entre seguridad y operatividad, de forma que el acceso remoto por parte del personal propio, así como el de las empresas proveedoras de servicios de mantenimiento, no se encuentre penalizado por las medidas de seguridad que se consideren adecuadas.

Implantar un modelo de arquitectura de accesos remotos al entorno OT, tanto desde la perspectiva técnica como desde la organizativa, definiendo las políticas, protocolos y procedimientos necesarios y adecuados para una correcta gestión de los mismos.

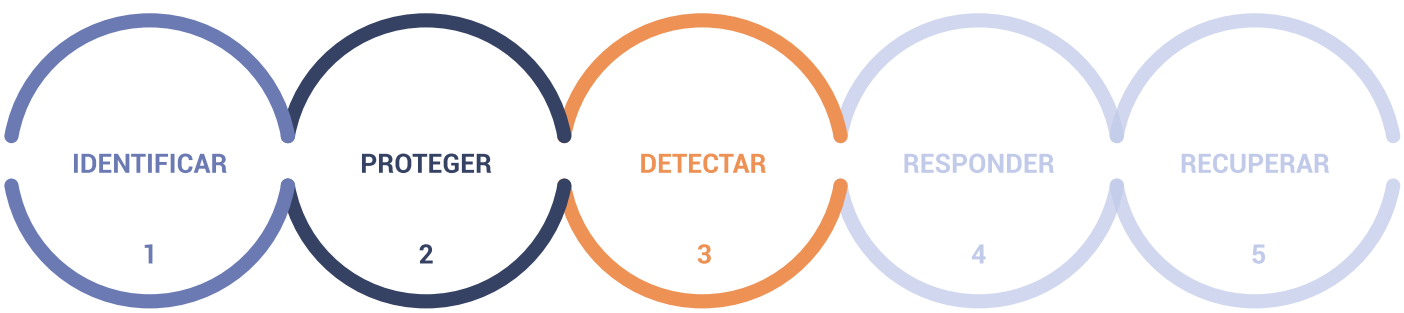
BENEFICIOS



Los beneficios que se alcanzarían con la puesta en marcha de este proyecto serían los siguientes:

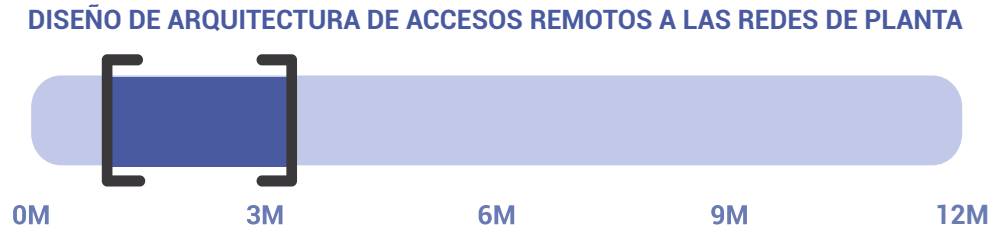
1. Contribuir a asegurar la continuidad del negocio.
2. Mejorar el nivel de resiliencia frente a las ciberamenazas.
3. Disminución del nivel de riesgo ocasionado por las conexiones a las redes del entorno OT que se producen desde el exterior de las redes corporativas, tanto por personal interno como externo.
4. Disminuir la probabilidad de un ataque a través de la cadena de suministro.
5. Mantener un control y gestión de todas las vías de acceso a las redes de planta, facilitando la identificación de eventos de seguridad que pudieran estar produciéndose a través de las mismas.
6. Permitir el establecimiento de medidas técnicas orientadas a un aumento de la seguridad de las conexiones.
7. Regular el marco contractual y procedimental para el establecimiento de las conexiones remotas por parte de nuestros proveedores, estableciendo claramente las responsabilidades en caso de materialización de un incidente de seguridad.
8. Garantizar la confidencialidad en el flujo de comunicaciones.

DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO

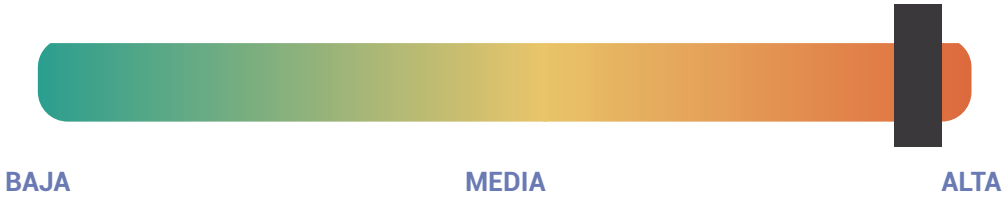


TIEMPOS ESTIMADOS DE EJECUCIÓN

Los tiempos estimados de ejecución de este tipo de proyectos se indican únicamente a modo orientativo y los mismos dependen fuertemente de factores como: tamaño y complejidad de la red, número de zonas y conductos a definir, etc.



REQUERIMIENTOS DE DEDICACIÓN DE RECURSOS DE LAS EMPRESAS SOLICITANTES



BUENAS PRÁCTICAS DURANTE SU EJECUCIÓN

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar una serie de cuestiones importantes:

- Inventario de proveedores: hay que contar con la ayuda del personal del Área de Producción/Mantenimiento/Operación/… para poder identificar qué proveedores requieren acceso remoto, bajo qué circunstancias, cuáles son los medios que están empleando en la actualidad (si se conocen) y vigencia de accesos remotos (soporte anual, bianual, 24x7x365; 8x5; etc.) debiéndose renovar de forma periódica.
- Inventario de dispositivos de acceso remoto: analizar la red a la búsqueda de dispositivos no inventariados que pudieran emplearse para el establecimiento de accesos remotos.
- Modelo de arquitectura de red existente: una red OT no segmentada impide el establecimiento de zonas y conductos orientados a limitar los accesos remotos a aquellos elementos a los que únicamente se requiera el acceso.
- Infraestructura de seguridad adecuada: la inexistencia de elementos de seguridad adecuados o una deficiente configuración de los mismos puede dificultar enormemente la implementación de modelos de acceso remoto adecuados a las circunstancias concretas de cada empresa.

SERVICIOS RELACIONADOS

Para el diseño de un modelo de arquitectura de accesos remotos a las redes OT:

- Servicios de consultoría.

Para la implantación de los modelos de arquitecturas de accesos remotos:

- Suministro, instalación, configuración y puesta en marcha de equipamiento de seguridad que disponga de funcionalidades adecuadas para el establecimiento de conexiones remotas seguras: cortafuegos, cortafuegos de nueva generación (NGFW).
- Servicios para la instalación, configuración y puesta en marcha de elementos específicos para el establecimiento de conexiones remotas (si fuera necesario).

OTROS PROYECTOS RELACIONADOS

- Diseño y/o implementación de arquitecturas de redes IT/OT seguras.
- Inventario de los diferentes elementos en un sistema crítico industrial.

ÁREA DE PROYECTO SUBVENCIONABLE EN EL PROGRAMA DE AYUDAS DE CIBERSEGURIDAD INDUSTRIAL

Securización de los accesos remotos OT a los equipos industriales de la planta productiva requeridos para el mantenimiento de equipo, control y operación de los mismos, tareas realizadas cada vez con más frecuencia de manera remota.

PERFIL DE EMPRESA SUMINISTRADORA DE SERVICIOS O PRODUCTOS

Las empresas que cuentan con la capacidad de prestación de los servicios incluidos en este tipo de proyectos, y que se encuentran registradas en el "Libro blanco de la Ciberseguridad en Euskadi" son aquellas que se encuentran encuadradas en la siguiente categorización:

Capacidad	Categoría de la solución	Grupo de producto / servicio
PROTEGER	Tecnología de protección	Seguridad Wireless Acceso remoto/VPN Firewall /Firewall de próxima generación Gestión unificada de amenazas (UTM)

2.3 Evaluación de la seguridad de la información / datos industriales

DESCRIPCIÓN DEL PROYECTO

Es indudable que la información es el principal activo sobre el que reside la actividad de las empresas. Sin datos relativos a clientes, pedidos, personal, … sería imposible gestionar los diversos procesos de negocio que pudieran encontrarse establecido en la organización.

Desde la perspectiva puramente industrial, puede concluirse sin duda que existe también información que podría catalogarse como crítica para el negocio, considerando, entre otras:

- La necesidad de salvaguardar la confidencialidad de la información proporcionada por un tercero como, por ejemplo, los planos proporcionados por uno de nuestros clientes para la fabricación de una pieza.
- La propiedad intelectual en referencia a patentes industriales, diseños, … propios y que constituyen el factor diferencial de nuestro negocio y que podrían tener un alto valor para la competencia.
- El código, programas, … que se encuentran en ejecución en los diferentes componentes que constituyen los sistemas de control industrial en producción en la planta y cuya alteración puede desembocar en interrupciones de las operaciones.
- El dato operacional extraído de la propia actividad industrial, y que a través de su análisis permite la optimización de los propios procesos productivos.

La información de ámbito industrial, por lo tanto, y al igual que otro tipo de información confidencial que pueda existir en la empresa, es susceptible de ser protegida en la medida que aporta un valor innegable al negocio. Sin embargo, no es frecuente encontrase con medidas de protección adecuadas para los anteriores escenarios planteados.

En este sentido, la información existente puede verse comprometida desde dos vertientes:

- Exfiltraciones de datos no autorizadas llevadas a cabo por personal interno de las organizaciones.
- Robo de información por terceros que bien, de forma dirigida o no, pudieran tener acceso en un momento dado a la misma.

Una de las vías a través de la cual se puede poner a prueba la fortaleza de la organización en este ámbito, es a través de la realización de auditorías de seguridad que permitan identificar carencias en materia de protección de la información industrial y que evalúen la efectividad de las medidas que pudieran encontrarse ya desplegadas o proponer aquellas que se determinen como pertinentes.

Las fórmulas más habituales de ejecución de este tipo de auditorías de seguridad o pruebas de intrusión (también denominado “Hacking Ético”), pasan por:

- Simular la actividad que sería llevada a cabo por parte de un atacante que no disponga de más información y accesibilidad a la empresa que la que pueda obtener por sus propios medios, a través de fuentes públicas, con el objetivo de alcanzar las redes internas corporativas y acceder a información confidencial.
- Simular un escenario que parte de la existencia de un puesto de la red comprometido o de un robo de credenciales de un usuario que permitan una conexión remota a las redes corporativas, para a partir de ahí, llevar a cabo las acciones que llevaría a cabo un tercero atacante.

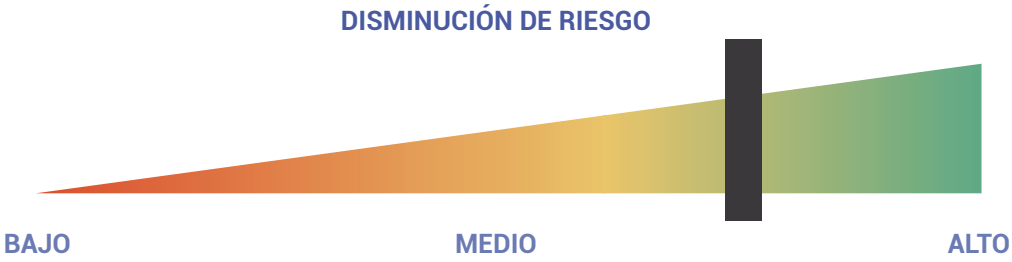
Las técnicas que pueden emplearse para llegar a comprometer un puesto de la red corporativa incluyen, además de medidas de explotación de vulnerabilidades o fallos de seguridad de índole puramente técnico, técnicas de ingeniería social que traten de conseguir el acceso a través de la propia persona usuaria.

OBJETIVOS

Los objetivos que persigue este proyecto son los siguientes:

- Determinar el nivel de exposición, protección y resiliencia al que se encuentra expuesta la organización desde la perspectiva de un atacante externo.
- Identificar el grado de accesibilidad de la información industrial crítica para el negocio, tanto por parte de usuarios internos como por parte de terceros no autorizados.
- Evaluar el grado de concienciación en materia de ciberseguridad de las personas usuarias de la organización frente a ataques que empleen técnicas de ingeniería social.
- Determinar las medidas de protección adecuadas para salvaguardar la confidencialidad de la información.

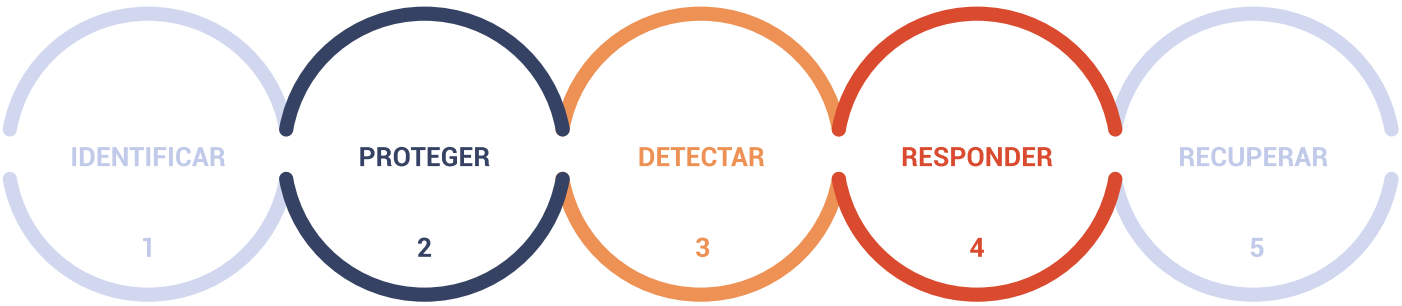
BENEFICIOS



Los beneficios que se alcanzarían con la puesta en marcha de este proyecto serían los siguientes:

1. Contribuir a asegurar la continuidad del negocio.
2. Mejorar el nivel de resiliencia frente a las ciberamenazas.
3. Identificar medidas que deberían ser implementadas como parte de una gobernanza responsable de la ciberseguridad.
4. Contrastar la eficacia de las medidas que se hubieran podido llevar a cabo en torno a la formación y concienciación en materia de ciberseguridad de las personas usuarias.
5. Evaluar la capacidad de detección y respuesta frente a amenazas por parte del personal técnico, al estar simulando realmente un escenario de ataque.
6. Permitir la definición u optimización de medidas técnicas orientadas a un aumento de la protección de la información confidencial existente.

DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO



TIEMPOS ESTIMADOS DE EJECUCIÓN

Los tiempos estimados de ejecución de este tipo de proyectos se indican únicamente a modo orientativo.

REQUERIMIENTOS DE DEDICACIÓN DE RECURSOS DE LAS EMPRESAS SOLICITANTES

BUENAS PRÁCTICAS DURANTE SU EJECUCIÓN

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar las siguientes cuestiones:

- Establecer ventanas horarias: si se considera oportuno por parte de la organización, se deben definir las ventanas horarias para la ejecución de los tests, aunque en este sentido hay que considerar que un atacante real no tiene limitaciones horarias para perpetrar un ataque.
- Notificación de los test a proveedores externos: únicamente en la medida que se deba permitir o autorizar expresamente este tipo de ejercicios, sobre todo en el caso de aquellos proveedores de comunicaciones o que proporcionen servicios de acceso remoto a la organización.
- No notificar los tests al personal técnico: de esta forma también es posible evaluar de forma práctica los procedimientos establecidos de detección, notificación y respuesta ante incidentes.
- Establecer acuerdos contractuales: con el objetivo de realizar un tratamiento adecuado de la información que pudiera obtenerse como resultado de las pruebas, y que garantice especialmente la destrucción de la misma de acuerdo a los términos que se establezcan.

SERVICIOS RELACIONADOS

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar las siguientes cuestiones:

- Servicios de consultoría por parte de un equipo especializado en Hacking Ético con conocimiento en entornos y tecnología industrial.

OTROS PROYECTOS RELACIONADOS

- Medidas de protección de información estratégica o sensible.

ÁREA DE PROYECTO SUBVENCIONABLE EN EL PROGRAMA DE AYUDAS DE CIBERSEGURIDAD INDUSTRIAL

- Securización de la información/datos industriales. Auditorías y simulaciones de ataques por personas externas a la organización y auditorias sobre perfiles internos con diferentes niveles de accesos a datos de la compañía.

PERFIL DE EMPRESA SUMINISTRADORA DE SERVICIOS O PRODUCTOS

- Las empresas que cuentan con la capacidad de prestación de los servicios incluidos en este tipo de proyectos, y que se encuentran registradas en el "Libro blanco de la Ciberseguridad en Euskadi" son aquellas que se encuentran encuadradas en la siguiente categorización:

Capacidad	Categoría de la solución	Grupo de producto / servicio
PROTEGER	Mantenimiento	Test de penetración / Red Teaming

2.4 Evaluación y mejora del software industrial en las plantas

DESCRIPCIÓN DEL PROYECTO

El software que gestiona sistemas de control industrial, el control de la producción, etc. generalmente no se ha desarrollado aplicando medidas de seguridad desde su diseño, por lo que es muy frecuente que presente una serie importante de carencias que lo hacen muy vulnerable frente a un tercero atacante.

En ocasiones por la antigüedad del software existente, o simplemente por una falta de adecuación a sistemas de desarrollo seguro por parte de las empresas proveedoras, lo cierto es que no es habitual el empleo de frameworks de desarrollo seguros que implementen de forma nativa medidas frente a vulnerabilidades clásicas como SQL Injection, Cross Site Scripting, etc. así como la implementación de medidas frente a ataques basados en fuzzing, DoS, etc.

Las actividades que se pueden llevar a cabo en el ámbito de este tipo de proyectos serían las siguientes:

- Realización de un análisis de vulnerabilidades contra el software/sistemas del ámbito industrial.
- Realización de pruebas de evaluación de la disponibilidad e integridad de los sistemas en el ámbito de la propia red.
- Revisión y auditoría del código fuente de los programas, identificando las carencias existentes de base en el propio software.

No cabe duda que el compromiso por parte de un tercero no autorizado de los sistemas que gobiernan y operan los procesos industriales, puede suponer un impacto muy elevado en la empresa, por lo que asegurar la ciberseguridad del software, aunque en ocasiones pueda resultar complejo, es una medida de mejora importante en materia de ciberseguridad.

Es importante señalar que la mejora de la ciberseguridad del software estará muy probablemente ligada intrínsecamente a las capacidades del propio proveedor del software. En este sentido, y ante la imposibilidad de desarrollar y/o aplicar parches o actualizaciones, será necesario plantearse otro tipo de medidas compensatorias (o virtual-patching).

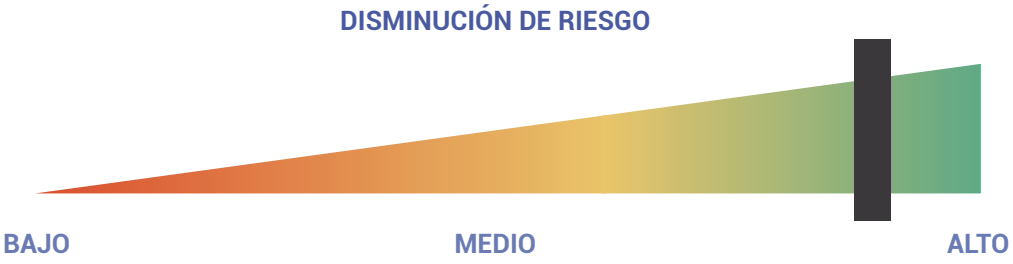
OBJETIVOS

Los objetivos que persigue este proyecto son los siguientes:

Analizar la seguridad de las aplicaciones de carácter industrial y determinar el nivel de riesgo que presentan frente a accesos no autorizados.

Evaluar y establecer el conjunto de medidas que es necesario desplegar para disponer de un nivel de protección adecuado a la criticidad del proceso industrial que se encuentra ligado al software.

BENEFICIOS



Los beneficios que se alcanzarían con la puesta en marcha de este proyecto serían los siguientes:

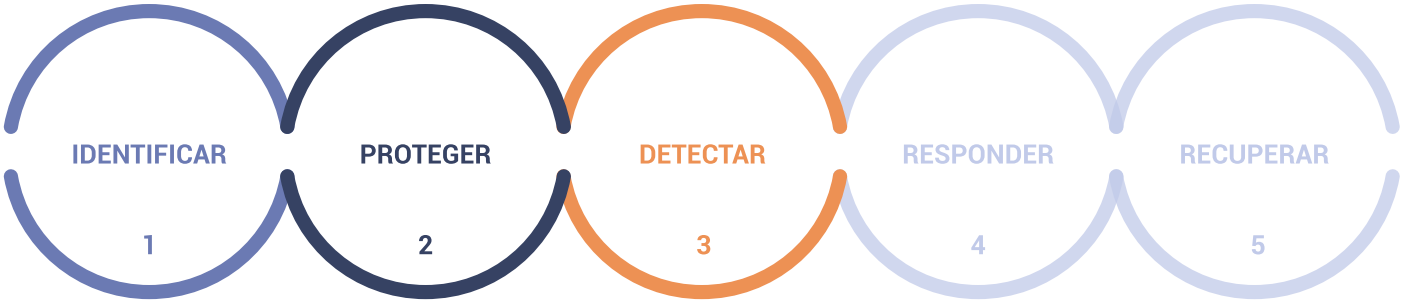
Contribuir a asegurar la continuidad de los procesos industriales mediante la securización del software que los opera.

Mejorar el nivel de resiliencia frente a las ciberamenazas.

Identificar el nivel de exposición y vulnerabilidades del software existente en el entorno industrial.

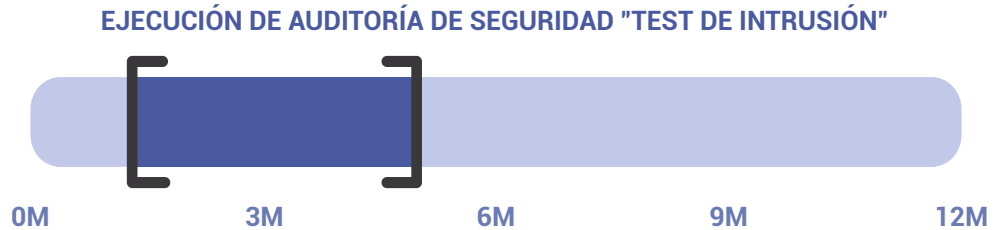
Determinar las medidas que sería necesario desplegar en el ámbito del software para asegurar la continuidad de los procesos industriales.

DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO



TIEMPOS ESTIMADOS DE EJECUCIÓN

Los tiempos estimados de ejecución de este tipo de proyectos se indican únicamente a modo orientativo.



REQUERIMIENTOS DE DEDICACIÓN DE RECURSOS DE LAS EMPRESAS SOLICITANTES

BUENAS PRÁCTICAS DURANTE SU EJECUCIÓN

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar las siguientes cuestiones:

- Establecer ventanas horarias para la realización de los tests: si se considera oportuno por parte de la organización, se deben definir las ventanas horarias para la ejecución de los tests, aunque en este sentido hay que considerar que un atacante real no tiene limitaciones horarias para perpetrar un ataque.
- Accesibilidad a código fuente: en ocasiones no será posible acceder al código fuente de las aplicaciones, por lo que no será posible la realización de este tipo de auditorías.
- Notificar fallos de seguridad a los proveedores del software: en la medida que se identifiquen brechas de seguridad deberían ser comunicadas al proveedor para que proceda a su subsanación urgente, tanto para la remediación del entorno de nuestra empresa, así como para el resto de instalaciones en terceros. En este sentido, es importante evaluar la respuesta del proveedor ante este tipo de hechos considerando la criticidad de las medidas a desplegar.

SERVICIOS RELACIONADOS

- Servicios de consultoría por parte de un equipo especializado en Hacking Ético con conocimiento en entornos y tecnología industrial.
- Servicios de consultoría por parte de personal especializado con conocimientos avanzados de ciberseguridad aplicada al desarrollo del software.

OTROS PROYECTOS RELACIONADOS

- Diseño e implantación de arquitecturas seguras en redes industriales.
- Adopción de buenas prácticas de estándares.

ÁREA DE PROYECTO SUBVENCIONABLE EN EL PROGRAMA DE AYUDAS DE CIBERSEGURIDAD INDUSTRIAL

- Evaluación de la ciberseguridad del software industrial en las plantas productivas y mejora del mismo.

PERFIL DE EMPRESA SUMINISTRADORA DE SERVICIOS O PRODUCTOS

Las empresas que cuentan con la capacidad de prestación de los servicios incluidos en este tipo de proyectos, y que se encuentran registradas en el "Libro blanco de la Ciberseguridad en Euskadi" son aquellas que se encuentran encuadradas en la siguiente categorización:

Capacidad	Categoría de la solución	Grupo de producto / servicio
PROTEGER	Mantenimiento	Test de penetración / Red Teaming
	Procesos y procedimientos de protección de la información	Static Application Security Testing (SAST) Seguridad de las aplicaciones

2.5 Formación y Concienciación

DESCRIPCIÓN DEL PROYECTO

No cabe duda de que a medida que la efectividad de las medidas técnicas para la protección que se despliegan en las empresas aumenta, las posibilidades de éxito de un atacante disminuyen en la misma proporción. Por ello, el panorama actual de amenazas se encuentra muy focalizado al uso de las personas como medio para lograr el compromiso de un sistema.

Es en este escenario cuando las vulnerabilidades intrínsecas asociadas a la naturaleza humana adquieren un mayor protagonismo, por lo que hay que proporcionar conocimientos y entrenamiento adecuados para poder reaccionar de manera adecuada frente a amenazas que intenten explotarlas.

La formación y concienciación de usuarios en materia de ciberseguridad debería considerarse como una actividad permanente, desarrollando un programa formativo que abarque:

Formación específica dirigida a perfiles concretos. Abarca desde sesiones formativas específicas para la Alta Dirección como cursos que desarrollan con mayor profundidad aspectos normativos, técnicos o legales adecuados para perfiles con diferentes responsabilidades en materia de ciberseguridad en la organización.

Formaciones de concienciación general en materia de ciberseguridad orientadas a las personas empleadas de la organización.

Avisos, consejos, píldoras informativas, … relacionados con aspectos concretos de la ciberseguridad o con noticias de actualidad que de forma periódica mantengan en alerta a las personas usuarias de la organización.

Para poder evaluar y medir el grado de capacitación de las personas usuarias, resulta muy recomendable llevar a cabo ejercicios prácticos que, simulando ataques dirigidos a las personas, permitan obtener conclusiones y aspectos de mejora sobre los objetivos alcanzados con el desarrollo del plan formativo. Este tipo de ejercicios se desarrollan mediante técnicas de ingeniería social que no deben circunscribirse únicamente al ámbito tecnológico (phishing, suplantación de identidad, …), sino que deben poner en práctica otro tipo de técnicas basadas en el mundo físico (intrusión física a instalaciones, ingeniería social, suplantación de identidad telefónica o presencial, etc.).

OBJETIVOS

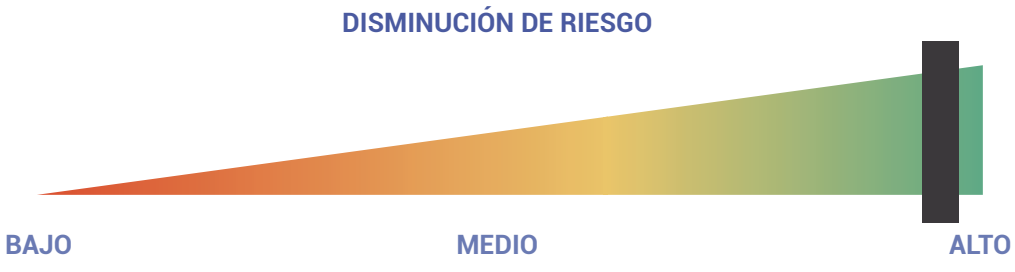
Los objetivos que persigue este proyecto son los siguientes:

Contribuir a la seguridad global de la organización a través de la formación y capacitación del personal en materia de ciberseguridad y, específicamente, de ciberseguridad industrial.

Proporcionar medios que permiten que las personas usuarias dispongan de conocimientos de ciberseguridad contextualizados a su puesto de trabajo, de forma que pueda ser consciente de los riesgos que entraña con respecto al resto de la organización.

Mantener en alerta y "tensión" constante a las personas usuarias en relación al panorama de amenazas e incidentes que pudieran estar ocurriendo no solo a nivel internacional, sino en empresas similares del entorno más cercano.

BENEFICIOS



DESCRIPCIÓN DEL PROYECTO

Los beneficios que se alcanzarían con la puesta en marcha de este proyecto serían los siguientes:

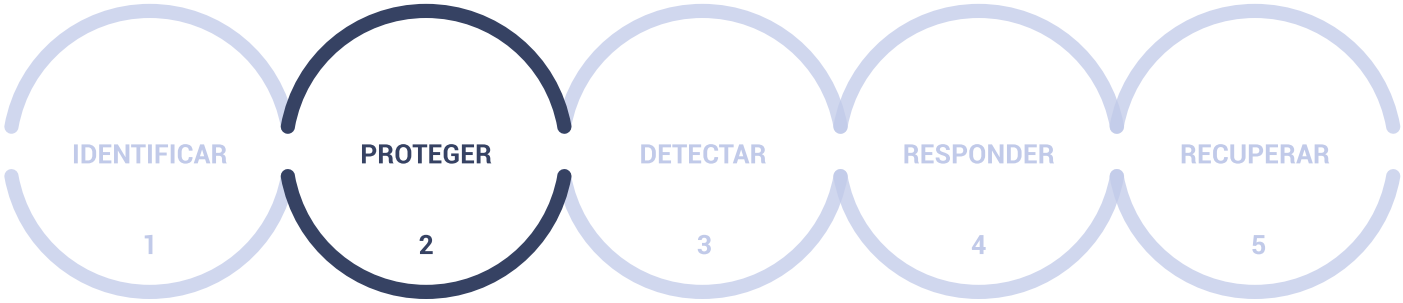
Desarrollar capacidades y habilidades en el personal de la empresa que permitan adquirir conocimientos y destrezas relacionados con la ciberseguridad aplicada a su entorno de trabajo de modo que sirvan como una capa adicional de defensa para la organización.

Mantener en permanente alerta al personal para evitar situaciones de materialización de incidentes de seguridad en la empresa.

Al igual que se produce en procesos relacionados con la seguridad física (por ejemplo, simulacros de incendio), experimentar de forma controlada las reacciones del personal frente a una amenaza simulada.

Verificar que los medios de notificación de incidencias de seguridad funcionan de forma adecuada.

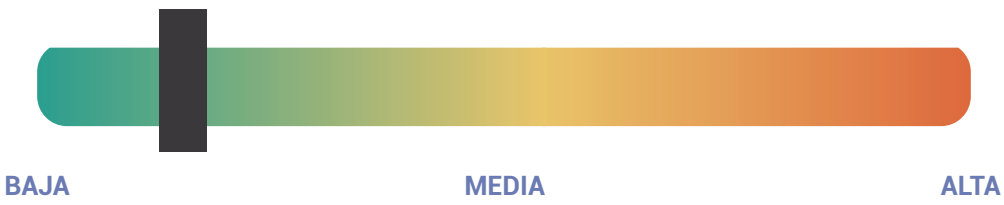
DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO



TIEMPOS ESTIMADOS DE EJECUCIÓN

Los tiempos estimados de ejecución de este tipo de proyectos se indican únicamente a modo orientativo.

REQUERIMIENTOS DE DEDICACIÓN DE RECURSOS DE LAS EMPRESAS SOLICITANTES



BUENAS PRÁCTICAS DURANTE SU EJECUCIÓN

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar las siguientes cuestiones:

- Formación personalizada: para que una formación sea realmente efectiva, debe ser diseñada de acuerdo a las especificidades de la empresa, de forma que el personal de la misma se vea reflejado, especialmente, en los casos de uso y ejemplos que pudieran ser expuestos a lo largo de la misma.
- Factor sorpresa: los test de ingeniería social no deben ser comunicados más que al personal implicado en la gestión de los mismos, de forma que pueda aprovecharse el factor sorpresa para evaluar las reacciones del personal. Esto incluye asimismo y especialmente, a los componentes de la Alta Dirección, sobre los que deberían intensificarse las acciones.
- Anonimización de los resultados: los resultados de los tests o de las evaluaciones que puedan realizarse sobre los conocimientos adquiridos durante el desarrollo del plan formativo, no deben ser expuestos de forma pública señalando a personas concretas. Las conclusiones deben tener carácter general, así como las actividades de refuerzo o mejora que se identifiquen tras el análisis de las mismas.

SERVICIOS RELACIONADOS

- Servicios de formación y capacitación específica.

OTROS PROYECTOS RELACIONADOS

- Realización de tests de intrusión empleando técnicas de ingeniería social.

ÁREA DE PROYECTO SUBVENCIONABLE EN EL PROGRAMA DE AYUDAS DE CIBERSEGURIDAD INDUSTRIAL

- Iniciativas para la concienciación de la plantilla de la empresa industrial en el ámbito de ciberseguridad.

PERFIL DE EMPRESA SUMINISTRADORA DE SERVICIOS O PRODUCTOS

Las empresas que cuentan con la capacidad de prestación de los servicios incluidos en este tipo de proyectos, y que se encuentran registradas en el "Libro blanco de la Ciberseguridad en Euskadi" son aquellas que se encuentran encuadradas en la siguiente categorización:

Capacidad	Categoría de la solución	Grupo de producto / servicio
PROTEGER	Concienciación y formación	Sesiones de formación Cyber Ranges
	Mantenimiento	Test de penetración / Red Teaming

2.6 Plan de ciberseguridad industrial

DESCRIPCIÓN DEL PROYECTO

La ciberseguridad en entornos industriales es un aspecto que, lamentablemente y hasta el momento, no se ha tomado en consideración de forma habitual en gran parte de las empresas.

Esta situación no es casual, y se encuentra condicionada por una serie de aspectos comunes a toda la industria:

- La no consideración de la ciberseguridad desde el diseño, lo que implica la inexistencia de controles y medidas de seguridad.
- La falta de conocimiento detallado de la arquitectura y componentes de los sistemas de control industrial existentes, que en muchas ocasiones reside exclusivamente en empresas proveedoras.
- La antigüedad del parque de elementos conectados a las redes industriales, en muchas ocasiones fuera del periodo de soporte de los fabricantes y con numerosas vulnerabilidades de seguridad conocidas, lo que supone un riesgo directamente proporcional a su exposición al resto de elementos de la red.
- La inexistencia de arquitecturas de red adecuadas conforme a criterios de seguridad aceptables.
- La imposibilidad de disponer de ventanas de intervención adecuadas para la puesta en marcha de determinadas medidas de seguridad, condicionadas por producciones 24x7 o periodos de mantenimientos programados.

Por lo tanto, y antes de comenzar con la puesta en marcha de medidas concretas, y que puede que no sean ni las más prioritarias ni las más adecuadas, las actividades lógicas para definir esta "hoja de ruta" de la ciberseguridad industrial son:

- Conocer el estado actual de la empresa en materia de ciberseguridad industrial, mediante un diagnóstico que permita identificar los puntos débiles y fuertes, valorando el riesgo en relación a escenarios de posibles amenazas y determinando las actividades que es necesario llevar a cabo para que la organización alcance un nivel de riesgo aceptable (y conocido).
- Establecer un plan, en el marco de un periodo temporal y de asignación de recursos (personas, económico) asumible por la organización, que permita acometer, de forma estructurada y priorizada, los proyectos de ciberseguridad que se hayan definido.

La determinación del nivel de riesgo se lleva a cabo a través de la realización de un análisis de riesgos. Esta actividad se puede llevar a cabo mediante diversas metodologías, basadas tanto en estándares de mercado (Magerit, etc.) como aquellas de factura propia que permitan alcanzar resultados similares. Las fuentes u orígenes de información que se pueden emplear para que el análisis abarque el máximo de ámbitos a me posible, pueden ser las siguientes:

- Contraste con marcos normativos o estándares de seguridad como la ISA/IEC 62443, ISO27002, NIST, etc.
- Ejecución de tests de intrusión en sus diferentes modalidades, incluyendo el análisis de comunicaciones inalámbricas en planta.
- Realización de análisis para la identificación de vulnerabilidades.

La relación de actividades que se identifiquen como consecuencia de la realización del análisis de riesgos permitirá establecer el correspondiente plan de acción.

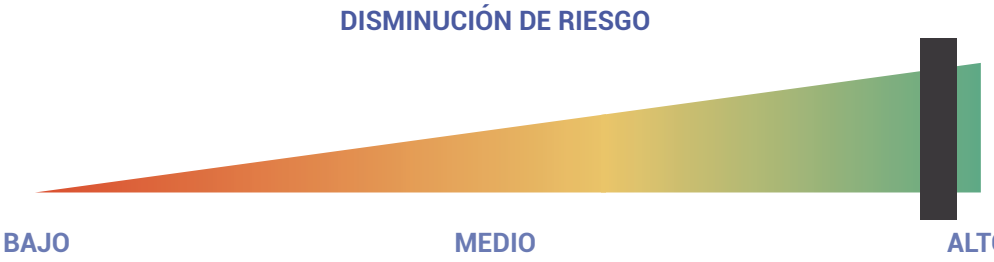
OBJETIVOS

Los objetivos que persigue este proyecto son los siguientes:

- Identificar, cuantificar y poner de manifiesto el nivel de riesgo que presenta la organización en materia de ciberseguridad industrial.

- Determinar las actividades que mitigan, transfieren o eliminan los riesgos identificados.
- Establecer un calendario de ejecución de proyectos que recoja las actividades del punto anterior que la organización ha decidido llevar a cabo, en base a su apetito de riesgo.
- Hacer partícipe a la Alta Dirección de la empresa mediante la presentación, validación, respaldo y seguimiento del plan de proyectos.

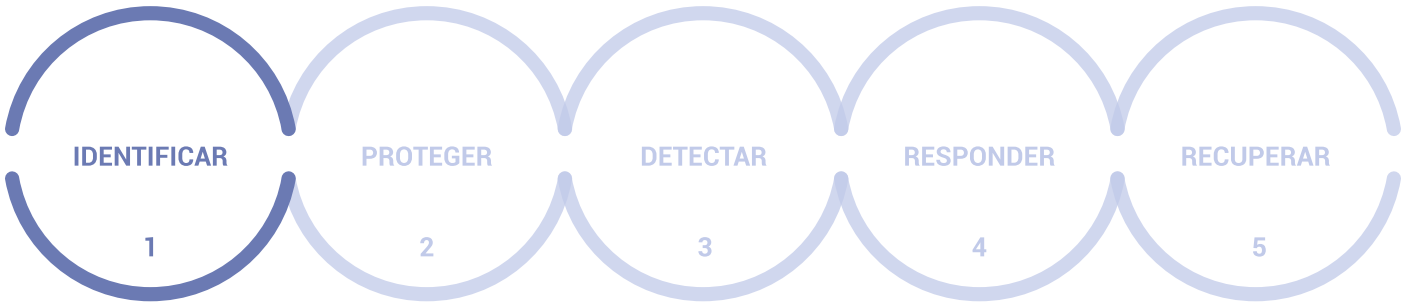
BENEFICIOS



Los beneficios que se alcanzarían con la puesta en marcha de este proyecto serían los siguientes:

1. Conocer el nivel de riesgo y las actividades que son necesarias para llevarlo a límites aceptables por la organización, con el objetivo de contribuir a asegurar la continuidad del negocio.
2. Disponer de un calendario de costes e inversiones que permita planificar la función financiera en relación a los proyectos de seguridad a acometer en un periodo de tiempo acordado y abordable.
3. Hacer partícipe a la Alta Dirección de la empresa de la necesidad de actuar frente a escenarios de riesgo que pueden causar interrupciones no esperados que produzcan impactos no asumibles por el negocio.

DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO



TIEMPOS ESTIMADOS DE EJECUCIÓN

Los tiempos estimados de ejecución de este tipo de proyectos se indican únicamente a modo orientativo.

REQUERIMIENTOS DE DEDICACIÓN DE RECURSOS DE LAS EMPRESAS SOLICITANTES

BAJA MEDIA ALTA

BUENAS PRÁCTICAS DURANTE SU EJECUCIÓN

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar las siguientes cuestiones:

- Apoyo de la Alta Dirección: si la Alta Dirección no participa en esta iniciativa, existe la posibilidad de que el proyecto no avance más allá de la fase del diseño del plan. Es importante asegurar este apoyo y, sobre todo, buscar la validación formal del Plan.
- Confianza y transparencia: en ocasiones, y en función de quien sea el promotor del proyecto, es posible que se produzcan reticencias en el momento de proporcionar cierta información o que no se transmita de forma fehaciente y ajustada a la realidad. Hay que considerar que poner de relevancia los aspectos menos consolidados de la ciberseguridad en la organización supone una oportunidad de mejora de los mismos a través de este plan.

SERVICIOS RELACIONADOS

- Servicios de consultoría.

OTROS PROYECTOS RELACIONADOS

- Inventario de los diferentes elementos en un sistema crítico industrial.
- Realización de un test de intrusión industrial.
- Auditorias de las comunicaciones inalámbricas industriales.

ÁREA DE PROYECTO SUBVENCIONABLE EN EL PROGRAMA DE AYUDAS DE CIBERSEGURIDAD INDUSTRIAL

- Diagnóstico de situación actual de la industria en materia de ciberseguridad industrial y elaboración de su plan de acción para la mejora de la Ciberseguridad. Análisis de riesgo industrial y de vulnerabilidad industrial. Inventario de los diferentes elementos en un sistema crítico industrial. Realización de un test de intrusión industrial. Análisis de vulnerabilidades en aplicaciones web. Auditorias de las comunicaciones inalámbricas industriales.

PERFIL DE EMPRESA SUMINISTRADORA DE SERVICIOS O PRODUCTOS

- Las empresas que cuentan con la capacidad de prestación de los servicios incluidos en este tipo de proyectos, y que se encuentran registradas en el "Libro blanco de la Ciberseguridad en Euskadi" son aquellas que se encuentran encuadradas en la siguiente categorización:

Capacidad	Categoría de la solución	Grupo de producto / servicio
IDENTIFICAR	Entorno del negocio	Análisis de impacto en el negocio
	Gobernanza y gestión del riesgo	Cumplimiento, riesgo y gobernanza
	Análisis del riesgo	-
	Estrategia de gestión del riego	-
	Gestión del riesgo en la cadena de suministro	-

2.7 Adopción de buenas prácticas de estándares

DESCRIPCIÓN DEL PROYECTO

Tradicionalmente se han establecido sistemas de gestión que han permitido la gobernanza de la seguridad de la información, fundamentalmente basados en ISO27001, y de un tiempo a esta parte, han surgido estándares y marcos de referencia que permiten implementar la función análoga en el ámbito puramente industrial como, por ejemplo: ISA/IEC 62443, NIST CSF, etc.

La gestión conjunta de la seguridad de la información y la de los procesos operacionales supone la integración, en un único sistema, de la gestión de la ciberseguridad de toda la organización. Lo cierto, sin embargo, es que la industria se encuentra actualmente sumida en la necesidad de identificar un marco único de gestión de la ciberseguridad IT y OT que sea aplicable a una amplia mayoría de sectores industriales, dado que, y ante esta carencia, se han desarrollado normativas sectoriales (o incluso de marcos exclusivos de una única empresa) que no dejan de ser generalmente una reformulación de las normativas y estándares anteriormente citados.

En este sentido, y si bien en muchos casos las empresas advierten la puesta en marcha de las buenas prácticas detalladas en estos estándares como una vía de mejora interna de la gestión de la ciberseguridad sin otro fin adicional, en otras ocasiones la necesidad viene forzada por requerimientos de terceros (generalmente clientes), que exigen demostrar que la empresa gestiona diligentemente la ciberseguridad, incluyendo la obligación de alcanzar determinadas certificaciones.

Estos marcos o estándares de referencia establecen un conjunto de controles de seguridad que la organización debería implementar, en función lógicamente de si son o no de aplicación en base a las características concretas de la misma, y abarcan todos los aspectos relacionados con la ciberseguridad: personas, procesos y tecnología.

En relación al alcance o aplicabilidad de la ciberseguridad industrial, la ISA/IEC 62443 ofrece un completo conjunto de controles de seguridad desde diferentes roles o perspectivas: propietario de instalaciones, integrador de sistemas o fabricante de componentes. En el caso del rol de fabricante de componentes, este estándar establece un marco de referencia para el desarrollo seguro de componentes (ISA/IEC 63442-4-1), así como los controles de seguridad (ISA/IEC 62443-4-2) que es necesario implementar, en función de un determinado nivel de seguridad objetivo a conseguir.

Por lo tanto, el futuro cercano pasa por asumir, implementar y, en algunas ocasiones, demostrar mediante la certificación emitida por una entidad certificadora independiente:

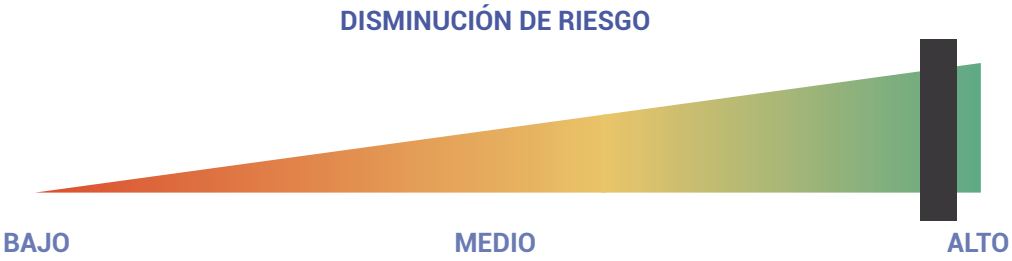
- La gestión de la ciberseguridad en entornos industriales (incluyendo de forma integrada los entornos IT y OT) como un proceso corporativo más en la organización.
- La seguridad en el diseño, desarrollo y funcionalidades de ciberseguridad implementadas en un componente.

OBJETIVOS

Los objetivos que persigue este proyecto son los siguientes:

- Asegurar la continuidad del negocio en base a la gestión de la ciberseguridad del mismo.
- Disminuir la probabilidad de materialización de un incidente de seguridad como consecuencia de no conocer el riesgo al que la organización se encuentra expuesta.
- Disponer de una visión permanente del nivel de riesgo de la organización en materia de ciberseguridad.
- Contribuir a establecer una sistemática estructural y continua en la adopción de la ciberseguridad como un proceso corporativo más.
- Asignar los medios y recursos adecuados para mantener el nivel de riesgo en los límites que la organización considere como asumibles.

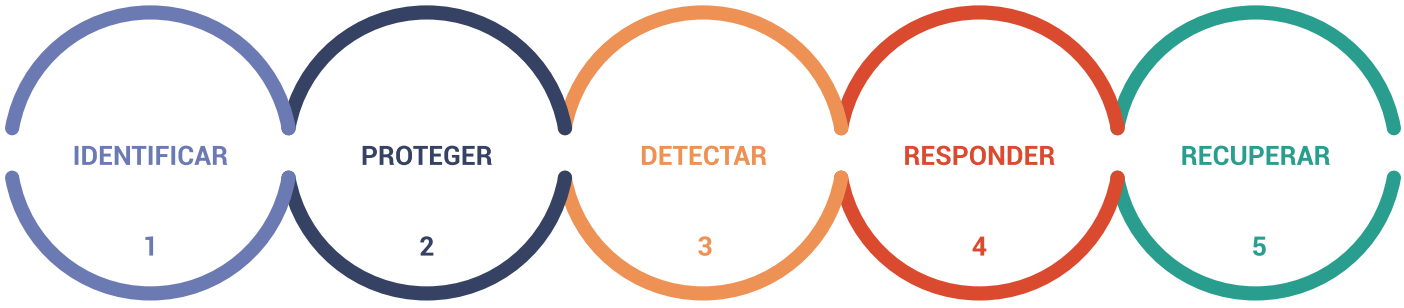
BENEFICIOS



Los beneficios que se alcanzarían con la puesta en marcha de este proyecto serían los siguientes:

1. Imbuir la cultura de la necesidad de la ciberseguridad como base fundamental para garantizar la continuidad del negocio.
2. El establecimiento de procesos formales corporativos para la gestión de la ciberseguridad, permitiendo establecer medidas de control y seguimiento de la efectividad de los mismos.
3. La determinación y asignación de roles y responsabilidades en materia de ciberseguridad, especialmente cuando en muchas ocasiones los límites entre los entornos IT y OT son ciertamente difusos.
4. Incorporar la ciberseguridad desde el diseño en la puesta en marcha de sistemas de control industrial en las propias instalaciones de las empresas.
5. Permitir desarrollar componentes desde la perspectiva de ciberseguridad.
6. Obtener un reconocimiento acreditado por entidades de certificación autorizadas e independientes sobre la ciberseguridad aplicada a la propia organización o en los productos que se comercializan.
7. Cumplimiento de nuevos requisitos por parte de clientes y proveedores en materia de reducción de riesgos tecnológicos, manejo de información, garantizar suministros, entre otros.

DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO



TIEMPOS ESTIMADOS DE EJECUCIÓN

Los tiempos estimados de ejecución de este tipo de proyectos se indican únicamente a modo orientativo.

REQUERIMIENTOS DE DEDICACIÓN DE RECURSOS DE LAS EMPRESAS SOLICITANTES

BAJA MEDIA ALTA

BUENAS PRÁCTICAS DURANTE SU EJECUCIÓN

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar las siguientes cuestiones:

- La Alta Dirección como promotora del proyecto: dado que la implantación de un sistema de gestión de la seguridad IT y OT implica necesariamente la participación, y, por tanto, destinar recursos de la práctica totalidad de las Áreas de la empresa, el proyecto debe nacer como un requerimiento del mismo por parte de la Alta Dirección, de forma que no pueda cuestionarse el fin perseguido por el mismo, ni los recursos que haya que destinar para su ejecución.
- Gestión del cambio: la implantación de nuevos procesos o los cambios en las formas de llevar a cabo condicionadas por los requerimientos de ciberseguridad requieren de una buena gestión del cambio que permita ser asumidos por la organización, de forma positiva y natural, en un corto espacio de tiempo.

SERVICIOS RELACIONADOS

- Servicios de consultoría.

OTROS PROYECTOS RELACIONADOS

- Adaptación a normativas o exigencias sectoriales/empresariales en materia de ciberseguridad industrial.
- Adaptación al cumplimiento del Esquema Nacional de Seguridad –ENS- (Real Decreto 3/2010).
- Adecuación al Reglamento PIC (Real Decreto 704/2011).

ÁREA DE PROYECTO SUBVENCIONABLE EN EL PROGRAMA DE AYUDAS DE CIBERSEGURIDAD INDUSTRIAL

- Adopción de buenas prácticas recogidas en estándares de Ciberseguridad industrial (por ejemplo, ISA/IEC 62443 o equivalentes) u otros de gestión de la Ciberseguridad (por ejemplo, ISO 27001 o equivalentes) ampliamente reconocidos. Adaptación al cumplimiento del Esquema Nacional de Seguridad (Real Decreto 3/2010), Reglamento PIC (Real Decreto 704/2011). Mejora continua del proceso de gestión de ciberseguridad mediante el despliegue de medidas específicas o evolución de las mismas a niveles de madurez superiores a los preexistentes.

PERFIL DE EMPRESA SUMINISTRADORA DE SERVICIOS O PRODUCTOS

Las empresas que cuentan con la capacidad de prestación de los servicios incluidos en este tipo de proyectos, y que se encuentran registradas en el "Libro blanco de la Ciberseguridad en Euskadi" son aquellas que se encuentran encuadradas en la siguiente categorización:

Capacidad	Categoría de la solución	Grupo de producto / servicio
IDENTIFICAR	Entorno del negocio	Análisis de impacto en el negocio
	Gobernanza y gestión del riesgo	Certificación de seguridad Cumplimiento, riesgo y gobernanza
	Análisis del riesgo	-
	Estrategia de gestión del riego	-
	Gestión del riesgo en la cadena de suministro	-

Grupo de producto / servicio

2.8 Medidas de protección de información estratégica o sensible

DESCRIPCIÓN DEL PROYECTO

La información es un activo vital para las empresas. Permite desarrollar todos los procesos de negocio, y su pérdida o inaccesibilidad puede tener consecuencias importantes en la propia continuidad del negocio.

La información se puede encontrar en diferentes lugares y formas: en papel o digital, en bases de datos, en servidores de ficheros ofimáticos, en sistemas de almacenamiento en la nube, etc. pero lo cierto es que, en la actualidad, la cantidad de información en formato papel que se utiliza como base de un proceso concreto en un entorno industrial es cada vez menor (y en muchos casos, residual).

Por lo tanto, el aseguramiento de la información existente en medios digitales supone, en sí mismo, asegurar el funcionamiento de la empresa. Sin embargo, llegar a alcanzar una protección adecuada de la información digital supone plantearse una serie de cuestiones que, a su vez, pueden convertirse en grandes retos:

- ¿La empresa conoce dónde se encuentran los repositorios donde reside la información corporativa?
- ¿Somos capaces de determinar la criticidad de la información que poseemos?
- ¿Tenemos la capacidad de determinar el valor de la información y lo que supondría su pérdida, inaccesibilidad, transmisión no autorizada a terceros, etc.?
- ¿Sabemos las medidas de seguridad que se están aplicando en la actualidad para prevenir tratamientos no autorizados de la información? ¿Y conocemos verdaderamente su efectividad?

En definitiva, plantearse medidas de protección de la información sin considerar aspectos de gestión documental más generales como los anteriormente citados, puede llegar a ser una medida eficaz, pero en muchos casos, poco eficiente.

Por lo tanto, y partiendo de la base de que la empresa tiene identificada, al menos, la información más crítica o confidencial para el negocio, será necesario establecer un conjunto de medidas organizativas, procedimentales y técnicas destinadas a un nivel de protección acorde. Entre las medidas técnicas, podemos destacar, entre otras, las siguientes:

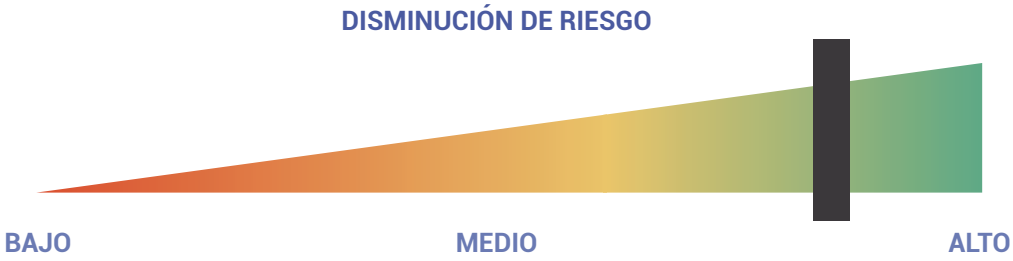
- Control de acceso mediante permisos de seguridad en carpetas de los servidores de ficheros corporativos.
- Despliegue de soluciones IRM (Information Rights Management) para mantener un control de la información con independencia de donde se encuentre almacenada.
- Puesta en marcha de sistemas DLP (Data Loss Prevention) que permiten implementar medidas orientadas a prevenir las fugas no autorizadas de la información desde las redes corporativas a través de los medios de transmisión de datos más frecuentes.
- Gestionar la seguridad de la información que se encuentra en los sistemas en la nube, mediante soluciones CASB (Cloud Access Security Broker), que permiten aplicar políticas de seguridad en los recursos existentes en este tipo de entornos.

OBJETIVOS

Los objetivos que persigue este proyecto son los siguientes:

- Asegurar la confidencialidad de la información crítica para la empresa, tanto frente a terceros como personal interno no autorizado.
- Ayudar a la empresa en el cumplimiento de la Ley de Propiedad Industrial mediante la protección de la información encuadrada dentro de la misma.

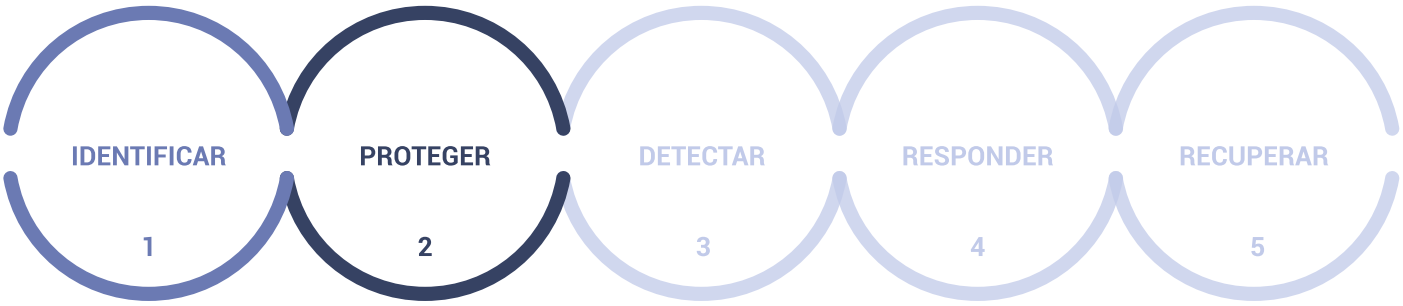
BENEFICIOS



Los beneficios que se alcanzarían con la puesta en marcha de este proyecto serían los siguientes:

1. Favorecer la continuidad del negocio a través del aseguramiento de la información.
2. Identificar los repositorios de información corporativos y el nivel de confidencialidad de la información contenida en los mismos.
3. Disponer de un control exhaustivo sobre la documentación confidencial que permita conocer quién, cuándo y cómo ha realizado un determinado tratamiento de la misma.
4. Dificultar el acceso a la información confidencial a personas no autorizadas.

DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO



TIEMPOS ESTIMADOS DE EJECUCIÓN

Los tiempos estimados de ejecución de este tipo de proyectos se indican únicamente a modo orientativo.

REQUERIMIENTOS DE DEDICACIÓN DE RECURSOS DE LAS EMPRESAS SOLICITANTES

BUENAS PRÁCTICAS DURANTE SU EJECUCIÓN

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar las siguientes cuestiones:

- Identificación de repositorios de información: será necesario la aplicación de técnicas basadas en la recopilación de información a través de entrevistas con las personas usuarias de las diferentes áreas de la organización, así como la posibilidad de emplear herramientas automatizadas para las tareas de descubrimiento. Como ya se ha comentado con anterioridad, este es generalmente el primero de los retos a los que se debe enfrentar una organización.

- Establecimiento del nivel de confidencialidad de la información: para ello se recomienda establecer un valor económico a la información o, al menos, el impacto en la organización, en términos cualitativos, de la pérdida, inaccesibilidad o robo de la misma, con el objetivo de poder justificar posteriormente la aplicación de las medidas de protección que se consideren para cada nivel de confidencialidad determinado.

- Determinar el grado de protección de la información: y que determinará las medidas a aplicar sobre la misma.

SERVICIOS RELACIONADOS

- Servicios de consultoría.

- Suministro, instalación, configuración y puesta en marcha de software para la protección de información confidencial o sensible.

OTROS PROYECTOS RELACIONADOS

- Adecuación de los sistemas de copias de seguridad.

ÁREA DE PROYECTO SUBVENCIONABLE EN EL PROGRAMA DE AYUDAS DE CIBERSEGURIDAD INDUSTRIAL

- Medidas de protección de información estratégica o sensible como puedan ser la propiedad intelectual, estrategias de I+D+i, planos de edificios o de diseño de productos, información afectada por el RGPD o cualquiera otra directamente relacionada con la competitividad y sostenibilidad del negocio (ejemplo de medidas: cifrado del almacenamiento, control de acceso, control de distribución de copias, borrado seguro, etc.).

PERFIL DE EMPRESA SUMINISTRADORA DE SERVICIOS O PRODUCTOS

Las empresas que cuentan con la capacidad de prestación de los servicios incluidos en este tipo de proyectos, y que se encuentran registradas en el "Libro blanco de la Ciberseguridad en Euskadi" son aquellas que se encuentran encuadradas en la siguiente categorización:

Capacidad	Categoría de la solución	Grupo de producto / servicio
IDENTIFICAR	Gobernanza y gestión del riesgo	Cumplimiento, riesgo y gobernanza
PROTEGER	Seguridad del dato	Prevención de fuga de información Cifrado Seguridad de acceso a la nube Firma digital
	Tecnología de protección	Seguridad de copia de seguridad y almacenamiento

2.9 Monitorización de seguridad industrial

DESCRIPCIÓN DEL PROYECTO

Disponer de una visión completa, detallada y permanentemente de lo que ocurre en las redes industriales, es el factor clave que permite identificar eventos de seguridad y anticipar una respuesta adecuada a los mismos, antes de que se produzcan impactos con consecuencias no tolerables para las empresas.

Una monitorización de las redes industriales debería permitir obtener información relacionada con:

- La identificación de patrones de ataque que pudieran estar produciéndose en las redes industriales, tanto característicos del entorno IT (y por desgracia muy habituales en entornos de planta) como específicos del entorno OT.
- El análisis de la información obtenida de la interpretación del tráfico de red, desde un punto de vista exclusivamente operacional (datos de variables de procesos), asociado a los protocolos industriales presentes, tras una aplicación de contexto que permita establecer una relación entre los datos obtenidos con la realidad de los sistemas de control industrial.
- Asimismo, y dado que la monitorización de la red permite disponer de una visibilidad muy elevada del tráfico circulante, obtener una instantánea de los activos industriales existentes en la red.

Sin embargo, un buen sistema de monitorización por sí mismo no resuelve la totalidad de los aspectos relacionados con la gestión de incidentes de seguridad, considerando que la información que proporcionan estos sistemas hay que analizarla y, si fuera necesario en función de la criticidad del evento identificado, proceder con las acciones de respuesta adecuadas.

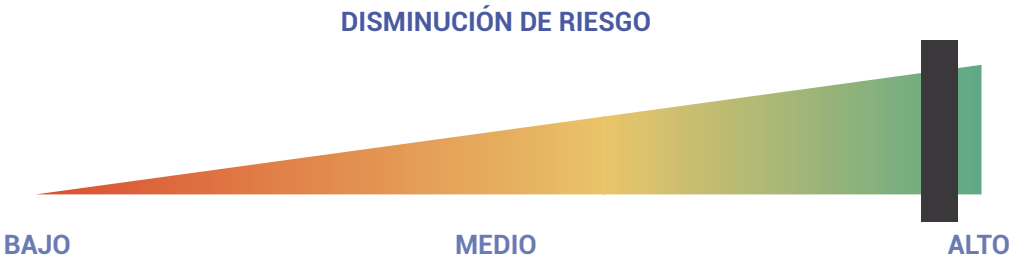
En este sentido, es muy interesante incorporar la información obtenida desde los sistemas de monitorización industriales a una solución SIEM (Security Incident and Event Management), de forma que puedan formar parte de una correlación de eventos mayor, permitiendo una mayor efectividad en la detección de incidentes a los equipos de seguridad.

OBJETIVOS

Los objetivos que persigue este proyecto son los siguientes:

- Disponer de la capacidad de identificar eventos de seguridad en las redes corporativas industriales.
- Proporcionar medios y recursos para mejorar los tiempos de respuesta y, por lo tanto, el impacto sufrido en los sistemas de producción, en caso de materialización de un incidente de seguridad.
- Establecer un modelo de gestión de la monitorización de seguridad que permita ser medido y mejorado.

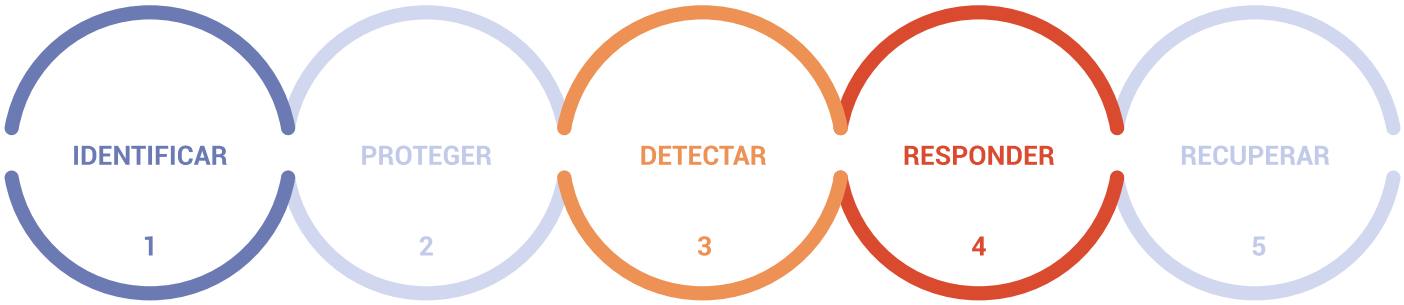
BENEFICIOS



Los beneficios que se alcanzarían con la puesta en marcha de este proyecto serían los siguientes:

1. Identificación e inventario de activos en redes industriales.
2. Identificación de vulnerabilidades asociadas a los activos identificados.
3. Visualización del tráfico existente en las redes industriales.
4. Asegurar la continuidad del negocio gracias a la identificación proactiva de incidentes de seguridad basados en patrones ataques de ataque tradicionales IT/OT.
5. Identificación de anomalías operacionales que pueden ser significativas o estar relacionadas con un evento de seguridad.
6. Mejora de los tiempos de activación de las capacidades de respuesta en caso de materialización de un incidente de seguridad.

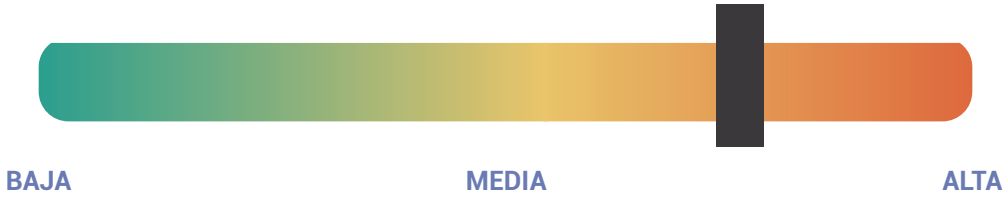
DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO



TIEMPOS ESTIMADOS DE EJECUCIÓN

Los tiempos estimados de ejecución de este tipo de proyectos se indican únicamente a modo orientativo.

REQUERIMIENTOS DE DEDICACIÓN DE RECURSOS DE LAS EMPRESAS SOLICITANTES



BUENAS PRÁCTICAS DURANTE SU EJECUCIÓN

Para llevar a cabo de forma correcta este tipo de proyectos, hay que considerar las siguientes cuestiones:

- Niveles de captación de datos: hay que determinar claramente hasta qué nivel se va a proceder con la captura de tráfico de red, considerando que en muchas ocasiones una máquina que presenta una única interfaz en la red corporativa puede, a su vez, disponer de una red interna muy extensa. Esta circunstancia condiciona el desarrollo del siguiente punto.

- Arquitectura del sistema de monitorización: la principal dificultad en el despliegue de un sistema de monitorización de entornos industriales supone el dimensionamiento y arquitectura del sistema de captación de datos del tráfico de la red, en muchas ocasiones ocasionado por la existencia de elementos de comunicaciones no gestionables que impiden un despliegue adecuado de las sondas.

- ¿Identificación de activos activa o pasiva?: si además de la propia monitorización del tráfico empleamos este tipo de soluciones para abastecer nuestro inventario de activos OT, hay que considerar la posibilidad de emplear técnicas de identificación pasivas (el nivel de detalle de la información a obtener es muy dependiente del tipo de tráfico observado por el sistema de monitorización, dado que no se interactúa de ninguna de las maneras con los equipos finales) y/o activas (interacción con los elementos finales para la obtención de información detallada). Con respecto a las técnicas activas, se recomienda que las soluciones empleen protocolos de conexión que no perjudiquen ni interfieran en el correcto funcionamiento de los elementos interrogados.

- Recursos para la gestión y supervisión del sistema de monitorización: es importante considerar la carga adicional de trabajo que supone el tratamiento de la información que se recibirá desde un sistema de monitorización, por lo que es necesario plantearse la necesidad de reforzar, bien de forma interna o bien con servicios de terceros, esta actividad..

SERVICIOS RELACIONADOS

- Servicios de seguridad gestionada y de monitorización de amenazas de seguridad.

- Suministro, instalación, configuración y puesta en marcha de software para la monitorización de la seguridad en entornos industriales.

OTROS PROYECTOS RELACIONADOS

- Despliegue de sistemas de gestión y monitorización de la red (NMS – Network Management System).

- Sistemas de monitorización y control de cambios en componentes de automatización industrial.

ÁREA DE PROYECTO SUBVENCIONABLE EN EL PROGRAMA DE AYUDAS DE CIBERSEGURIDAD INDUSTRIAL

- Monitorización de dispositivos de seguridad perimetral y de otros dispositivos industriales (switches, sondas, appliances, firewalls industriales, PLCs, etc.).

PERFIL DE EMPRESA SUMINISTRADORA DE SERVICIOS O PRODUCTOS

Las empresas que cuentan con la capacidad de prestación de los servicios incluidos en este tipo de proyectos, y que se encuentran registradas en el "Libro blanco de la Ciberseguridad en Euskadi" son aquellas que se encuentran encuadradas en la siguiente categorización:

Capacidad	Categoría de la solución	Grupo de producto / servicio
DETECCIÓN	Anomalías y eventos	Detección de intrusiones
	Monitorización continua de seguridad	SIEM / Solución de correlación de eventos Cyber Threat Intelligence Centro de Operaciones de Seguridad (SOC)
RESPONDER	Plan de respuesta	Gestión de incidentes
	Mitigación	Servicios de respuesta ante incidentes (CSIRTaaS)

Basque CyberSecurity Centre

BASQUE CYBERSECURITY CENTRE:

El punto de encuentro de la ciberseguridad en Euskadi

info@bcsc.eus

Albert Einstein 46, 3ª planta Edificio E7
Arabako Teknologi Parkea
01510 Vitoria-Gasteiz

945 236 636