Ciberseguridad industrial

Normalizada y con seguridad para el futuro

PHOENIX CONTACT
INSPIRING INNOVATIONS

Ciberseguridad industrial: la confianza es la base

Vivimos en una época en la que el desarrollo de las tecnologías de comunicación permite que millones de equipos intercambien información en todo el mundo. Por eso, es necesaria una estrategia para garantizar la seguridad de red y la disponibilidad de la planta. En este contexto, Phoenix Contact desarrolla soluciones para proteger en su empresa los sistemas, los conocimientos técnicos y todos los datos confidenciales que dan forma a los procesos comerciales y de producción.

Más información sobre el tema

Hay muchas razones por las que abordar el tema de la ciberseguridad.
En este folleto le ofrecemos una visión general sobre este tema y le mostramos las posibles soluciones.

Encontrará información actualizada sobre la ciberseguridad en:
https://phoe.co/cyber-security
Además, encontrará muchos vídeos útiles en nuestro canal de Youtube:
https://phoe.co/youtube

Escanee el código QR para obtener más información sobre la ciberseguridad industrial

Deje atrás sus preocupaciones

Le ofreceremos todas las herramientas para la seguridad de sus máquinas e instalaciones. Cree sin complicaciones su paquete completo y personalizado de productos, servicios y soluciones.

Contenido

Relevancia de la ciberseguridad en todas las industrias

El tema de la ciberseguridad incumbe a todos, tanto fabricantes como empresas explotadoras, la industria o la infraestructura crítica. La creciente interconexión y conexión de sistemas de control y automatización industriales (ICS) a Internet también hace que estos cada vez estén más expuestos a ataques cibernéticos y cambios no deseados.

Por este motivo, la ICS Security cada vez adquiere más relevancia.

Fabricantes de maquinaria

La seguridad aumenta la fiabilidad y disponibilidad de sus máquinas. Para el mantenimiento remoto de cara al cliente se precisa además una conexión remota segura.

Explotador de la instalación

La seguridad no solo garantiza la disponibilidad y el desarrollo fiable de sus instalaciones y procesos, sino que protege además sus conocimientos técnicos sobre producción.

Industria automovilística

La disponibilidad de sus instalaciones es su activo más preciado. Los mecanismos de seguridad garantizan la disponibilidad de las líneas de producción y pueden incluso aumentarla.

Sector energía

Las empresas del sector energía juegan un papel importante en el suministro básico a las personas. Por este motivo, los legisladores de muchos países obligaron a los explotadores a proteger la infraestructuras de importancia crítica de sus instalaciones para evitar un acceso no autorizado.

Agua/aguas residuales

Su tarea más importante es garantizar el suministro continuo de agua potable y la limpieza de las aguas residuales. Con la seguridad, garantizará el acceso remoto a las estaciones remotas de bombeo y elevación y protegerá los sistemas de automatización frente al creciente número de ciberataques por Internet.

Petróleo y gas

La seguridad debe considerarse un requisito en el ámbito de Safety, en particular en entornos explosivos o ligeramente inflamables. No en vano, una instalación hackeada no solo puede suponer un riesgo financiero, sino también un riesgo para la seguridad de sus empleados.

¿Qué podría pasar? Posibles consecuencias de un incidente de seguridad

Las empresas solo tienen éxito si sus plantas de producción funcionan de forma segura y sin fallos. Los fallos, los sabotajes o las pérdidas de datos pueden causar un alto daño económico. Y es que las paradas no solo implican pérdidas financieras, sino que también ponen en peligro los plazos de entrega y, como consecuencia, la imagen y la reputación de la empresa. En un análisis de sitios y procesos, puede evaluar los riesgos relativos de su sistema industrial y su interacción con el sistema de información de la instalación.

Pérdida de conocimientos técnicos

La competencia también puede acceder a datos de producción confidenciales. ¿Puede cuantificar el daño económicamente?

Pérdida de datos

De repente, se pierden datos vitales para la empresa. ¿Cuánto es el esfuerzo y el coste de reconstruir estos datos?

Paros de las instalaciones

Los problemas de seguridad provocan la parada de la producción durante algunas horas o incluso días. ¿Cuál es el coste de dicha pérdida de producción?

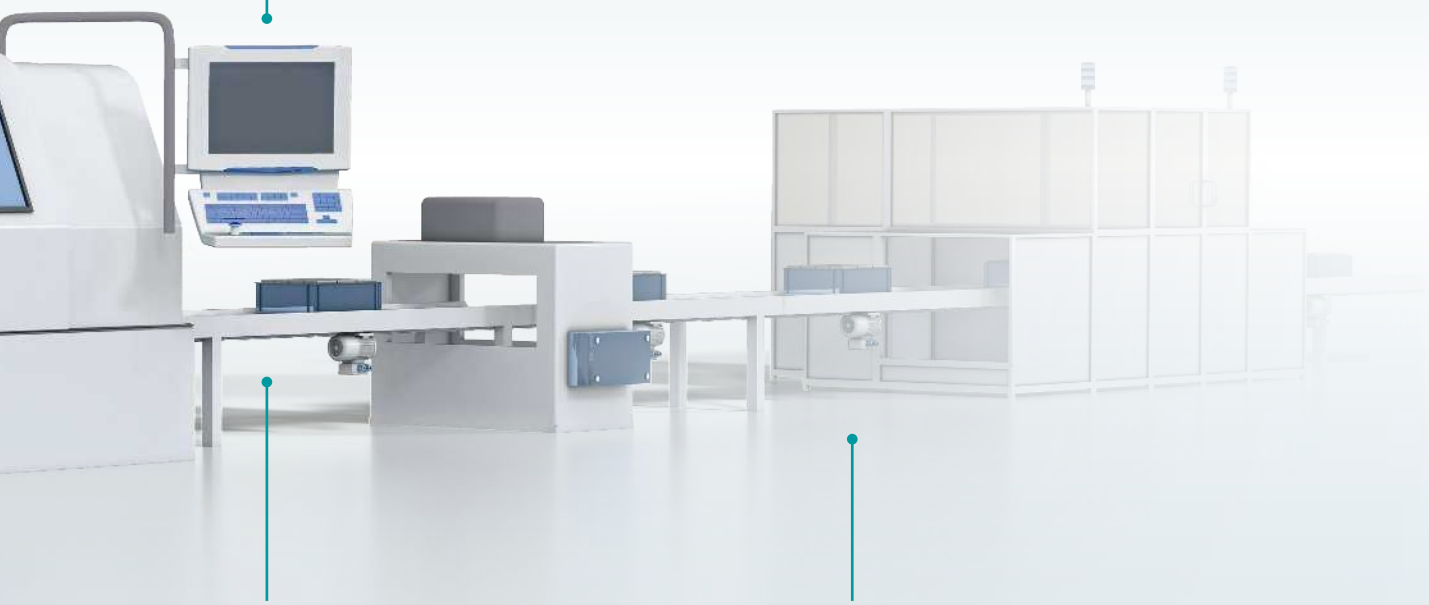
Lo que ya ha pasado

La lista de incidentes de seguridad en la industria es cada vez más larga: “Stuxnet”, un programa dañino especial para sistemas SCADA, los virus “Industroyer” (2016) y “TRITON” (2017), un ataque selectivo a los controles de seguridad y el software de extorsión “WannaCry” (2017), que ha atacado a más de 230.000 sistemas en todo el mundo.

Puede obtener información actualizada sobre temas de seguridad en cualquier momento a través de nuestros canales de redes sociales y boletines informativos.

Lectura

¿Qué sucede si los socios y clientes cuestionan su reputación por la fiabilidad y seguridad de los datos de su empresa?



Chantaje con ransomware

Bloqueo total de la producción y los archivos. ¿Cuál es el coste del rescate exigido para reactivar el proceso de producción?

Costes de personal

¿Cuántas horas de trabajo se necesitan para reparar los daños provocados por medidas de seguridad inadecuadas?

360° Security: nuestro estándar de calidad

Phoenix Contact ofrece seguridad normalizada en productos, soluciones industriales y servicios para lograr un funcionamiento seguro en el futuro de máquinas, instalaciones e infraestructuras. La seguridad está anclada en todo el ciclo de vida de nuestros productos y soluciones. Nuestro objetivo es hacer que la seguridad moderna sea intuitiva, por ejemplo, mediante una configuración sencilla, con funciones de seguridad integradas, con soluciones completas maduras y con servicios de consultoría de soporte. La disponibilidad de las actualizaciones necesarias durante muchos años aporta además una larga vida útil de nuestros componentes.

Oferta completa de seguridad sin complicaciones

Sus datos están seguros con nosotros

Conocemos lo que rodea a la seguridad y, por lo tanto, podemos asegurarle que siempre trataremos sus datos confidencialmente. Phoenix Contact mantiene un sistema de gestión de la seguridad de la información ("SGSI") que define, entre otras cosas, el tratamiento de datos e información confidenciales de acuerdo con los requisitos de la norma ISO/IEC 27001.

Productos seguros

Phoenix Contact introduce un proceso de desarrollo seguro. En él, las medidas de seguridad se implementan, verifican y documentan basándose en un análisis de amenazas. Además, los productos disponen de diferentes funciones de seguridad y de una comunicación codificada o de funciones de cortafuegos. Además, las vulnerabilidades de la seguridad se comprueban constantemente y se proporcionan actualizaciones de seguridad.

Servicios seguros

La seguridad no se puede implementar sin la correcta integración de los mecanismos de seguridad y la atención de cada uno de los empleados. Por ello, Phoenix Contact le ofrece diferentes servicios de asistencia: desde la evaluación de su nivel de seguridad individual y el asesoramiento para mejorar su seguridad hasta la formación de los empleados. Todos los servicios se prestan manteniendo los estándares de seguridad más elevados. Sus inquietudes están a salvo con nosotros.

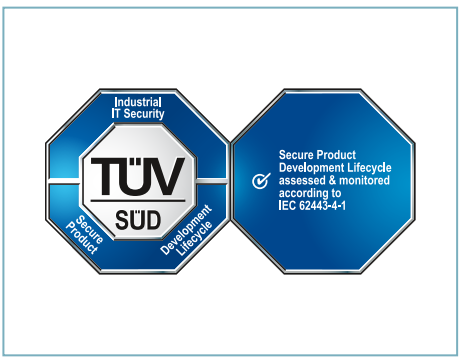
Soluciones seguras

Phoenix Contact combina servicios y productos seguros para lograr soluciones y arquitecturas de seguridad integrales. Además de productos seguros, también podemos ofrecerle soluciones de automatización seguras para una amplia variedad de requisitos e industrias.

Mejora continua

Nuestro Product Security Incidente Response Team (PSIRT) recopila y analiza permanentemente las posibles lagunas de seguridad en los productos y procesos. En caso de que se detecte una laguna de seguridad, se resuelve rápidamente para garantizar la máxima seguridad.

Encontrará todos los mensajes en: https://phoe.co/PSIRT



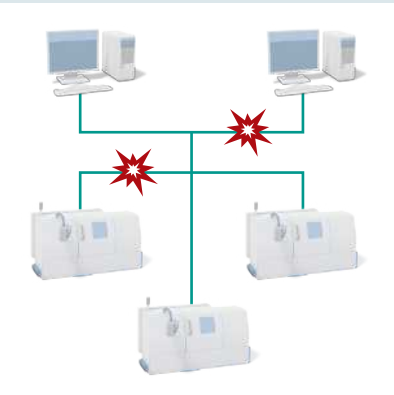
Seguridad certificada

Phoenix Contact ha sido certificada por TÜV SÜD como una de las primeras empresas en Alemania según IEC 62443, parte 4-1:2018, edición 1.0. Esto confirma que el desarrollo de productos de Security by Design se basa en un proceso de desarrollo seguro. También estamos certificados como proveedores de servicios para el diseño de soluciones de automatización seguras según la norma, parte 2-4. Además, trabajamos continuamente en la obtención de otros certificados para nuestra oferta de seguridad.

Riesgos de seguridad habituales y soluciones

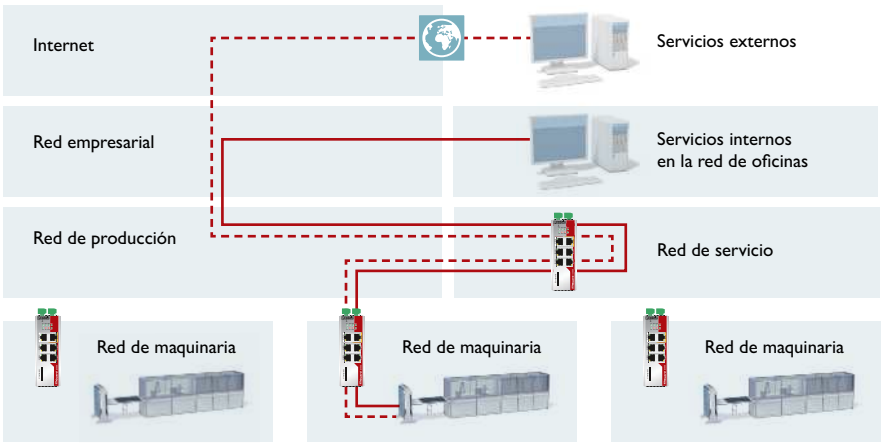
Riesgo: fallos provenientes de Office

Los fallos y virus, p. ej. del entorno Office, se pueden contagiar directamente al entorno de producción.



Solución: segmentación de la red

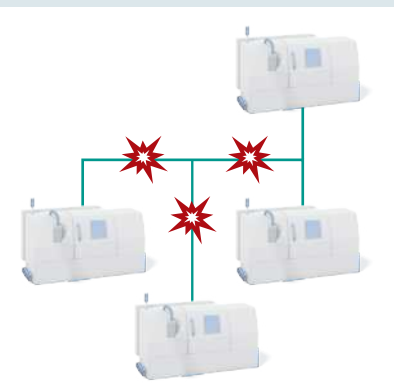
Mediante la división de grandes redes en pequeños segmentos, se puede controlar el intercambio de datos entre las diferentes zonas, p. ej. entre la producción y Office o entre diferentes partes de la instalación. Los segmentos individuales se pueden separar con ayuda de VLAN o cortafuegos. Para la comunicación entre los segmentos de red individuales deben emplearse routers o switches de capa 3. Estos equipos captan los errores de red, de manera que no se puedan expandir al resto de la red.



Segmentación de la red con routers de seguridad mGuard

Riesgo: infección por software dañino

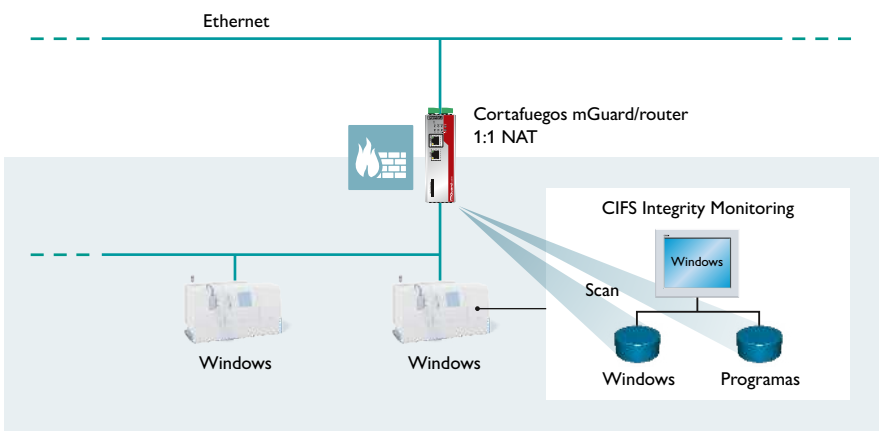
Con frecuencia, el software dañino está concebido de forma que intenta expandirse a los sistemas vecinos para dañarlos. Un ejemplo es el software dañino WannaCry, que infecta los sistemas Windows no actualizados.



Solución: limitación de la comunicación

El uso de cortafuegos puede limitar o impedir la propagación del software dañino. Si se bloquean todas las posibilidades de comunicación que no son técnicamente necesarias, se pueden evitar muchos ataques.

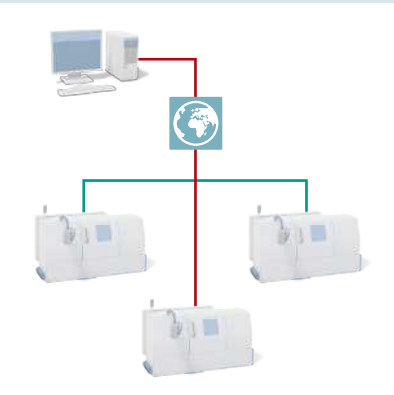
Además, la Integrity Monitoring apta para la industria (p. ej. CIM) ayuda a detectar y contener en una fase temprana cambios y manipulaciones en sistemas basados en Windows, como sistemas de control, unidades de operación o PC.



CIFS Integrity Monitoring

Riesgo: ataques de hackers

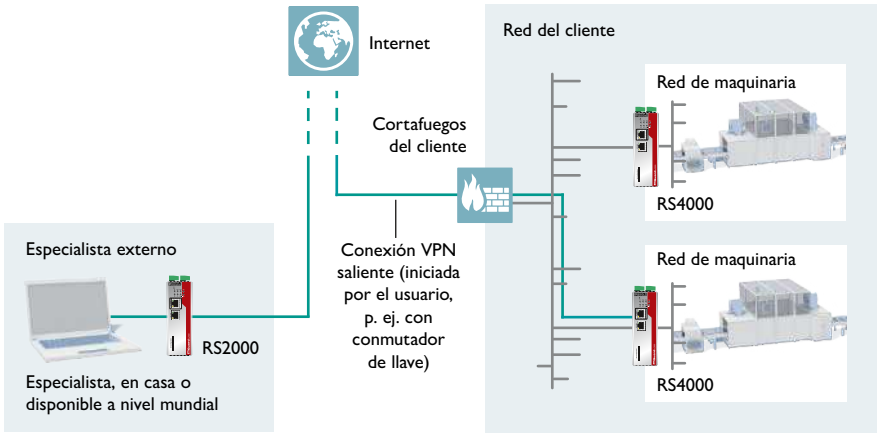
Los delincuentes pueden utilizar una conexión abierta a Internet para copiar datos o realizar cambios en el sistema.



Solución: transmisión de datos codificada

Se debe impedir el acceso a los sistemas de automatización a través de Internet. Esto se puede lograr mediante un cortafuegos en el acceso a Internet, que limita todo el tráfico entrante y saliente a las conexiones necesarias y permitidas.

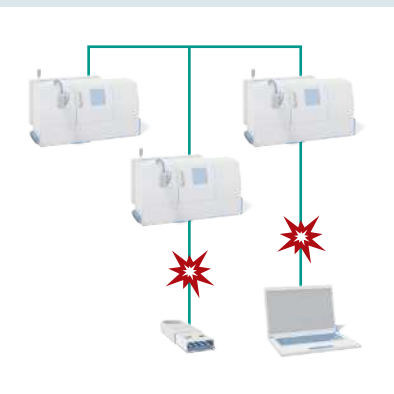
Todas las conexiones de amplio alcance deben estar cifradas, p. ej. a través de VPN con IPsec.



Mantenimiento remoto seguro con transmisión de datos codificada

Riesgo: hardware infectado

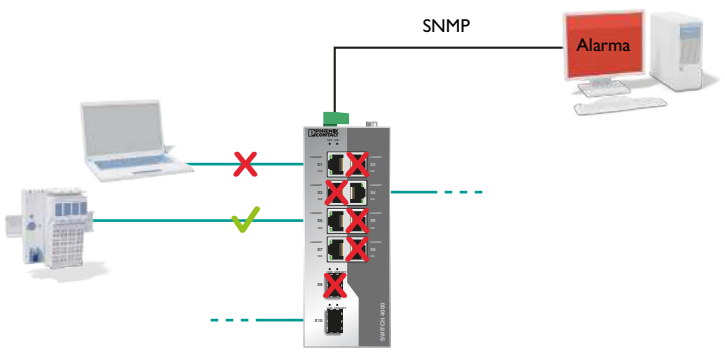
El hardware infectado, como una memoria USB o un portátil, puede contagiar el software dañino a la red.



Solución: protección de los puertos

Mediante la función Port Security, puede configurar directamente en los componentes de la red que los participantes no deseados no puedan intercambiar datos con la red. Además, deben desconectarse los puertos libres si no se necesitan.

Algunos componentes también ofrecen la opción de avisarle a través de SNMP y un contacto de aviso si se registra un acceso no autorizado a la red.

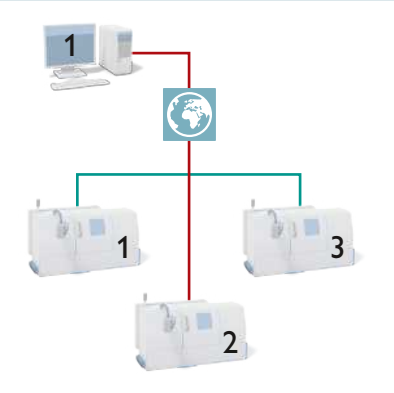


Desconexión de puertos y aviso mediante alarma a través de SNMP

Riesgos de seguridad habituales y soluciones

Riesgo: acceso no autorizado a las instalaciones

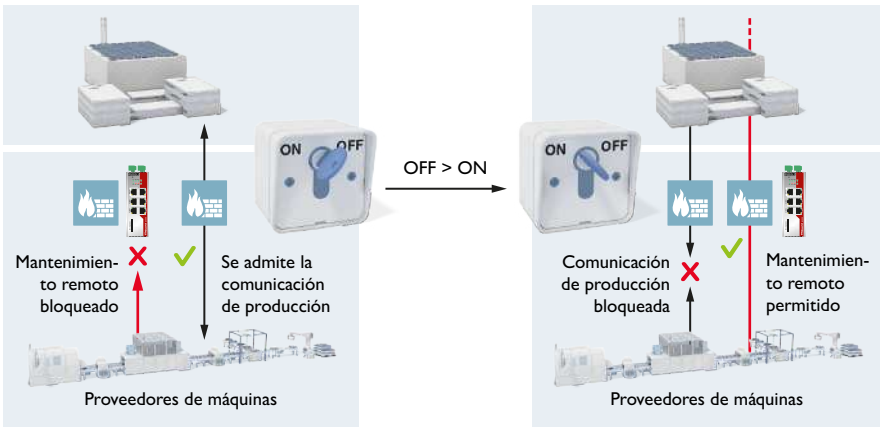
Puede que se realicen accidentalmente cambios remotos en el sistema incorrecto.



Solución: acceso remoto seguro

El acceso remoto seguro a una o más máquinas puede realizarse con diferentes soluciones tecnológicas. Por un lado, la comunicación externa está codificada, p. ej. a través de IPsec u OpenVPN. Por el otro, se puede iniciar el mantenimiento remoto en la máquina a través de un conmutador de llave.

De esta forma, se garantiza que solo se realicen los cambios en la máquina en la que está previsto. Al mismo tiempo, el conmutador de llave puede utilizarse para bloquear las reglas de comunicación en la red durante el tiempo del mantenimiento remoto.



Control del mantenimiento remoto con ayuda de un conmutador de llave

Riesgo: administración de usuarios insuficiente

Con frecuencia, se utilizan contraseñas colectivas para el acceso de los usuarios. Cuando los empleados dejan la empresa, estas contraseñas no se modifican ni se desactivan los accesos. El resultado es que demasiados empleados conocen la contraseña colectiva y pueden provocar usos inadecuados.

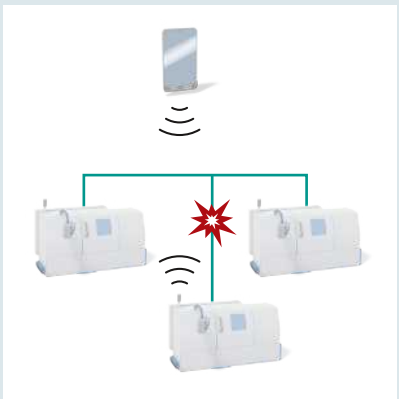
Solución: administración de usuarios centralizada

Este problema se puede solucionar mediante una administración de usuarios centralizada, en la que se concede un acceso individual a cada empleado. Muchos equipos de Phoenix Contact admiten la integración en una administración de usuarios centralizada.

Administración de usuarios centralizada con asignación de permisos individual

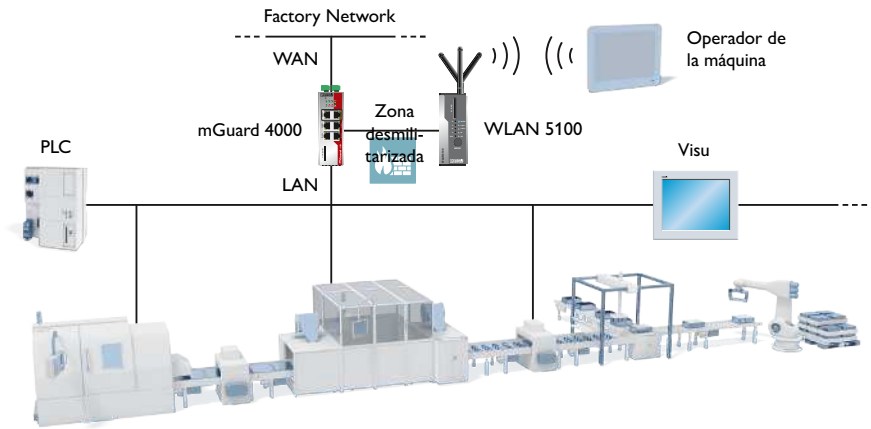
Riesgo: equipos terminales móviles

Los Smart Devices (dispositivos inteligentes) no autorizados se comunican a través de la interfaz WLAN.



Solución: asignación de contraseña WLAN segura

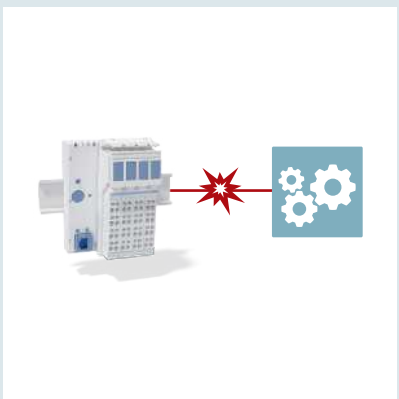
Si se conocen las contraseñas WLAN y no se cambian durante un largo periodo de tiempo, puede producirse un acceso incontrolado a la red de maquinaria. Los componentes WLAN de Phoenix Contact permiten una gestión de claves automatizada mediante el sistema de control de la máquina. De este modo, se permite fácilmente el acceso seguro a las máquinas WLAN mediante contraseñas únicas. Además, se puede proteger la comunicación WLAN con una zona desmilitarizada y aislarla del resto de la red.



Integración segura de equipos terminales móviles con contraseñas únicas y zona desmilitarizada

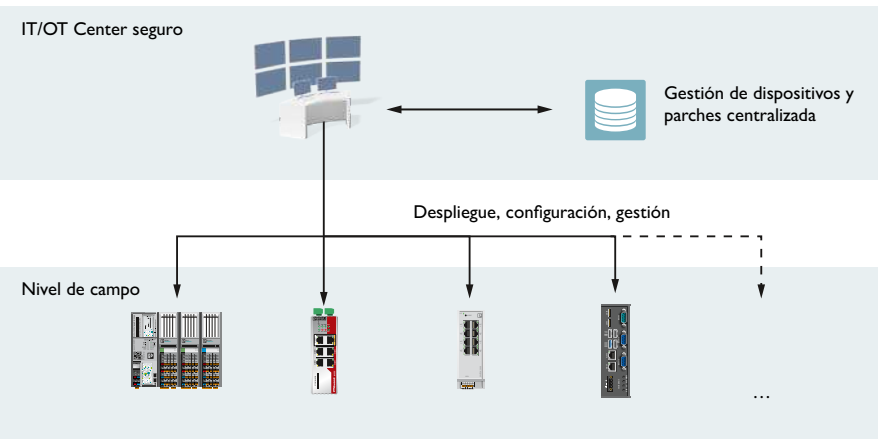
Riesgo: configuración de equipos incorrecta o insegura

Las configuraciones estándar de los equipos se han diseñado para garantizar que los componentes funcionen correctamente y que sean fáciles de poner en funcionamiento.
En este contexto, los mecanismos de seguridad juegan con frecuencia un papel secundario.



Solución: gestión de dispositivos y parches

Al gestionar varios equipos, una gestión de dispositivos y parches inteligente y eficiente puede automatizar procesos que requieren mucho tiempo y reducir además los riesgos de una configuración incorrecta. Ayuda a configurar, desplegar y gestionar los equipos y reduce los riesgos de seguridad y cumplimiento acortando los ciclos de parches y actualizaciones. La gestión de dispositivos y parches permite la creación y gestión centralizadas de todos los ajustes de los equipos relevantes para la seguridad, además de facilitar las actualizaciones de firmware.



Gestión de dispositivos y parches centralizada

Nuestro objetivo: lograr la seguridad IT

Las medidas organizativas y técnicas sostenibles, ajustadas al ciclo de vida de su instalación, minimizan el riesgo de posibles ataques. Para lograr la máxima estabilidad y transparencia de su infraestructura, le ayudamos a seleccionar el hardware adecuado y necesario, a desarrollar conceptos de protección personalizados y a impartir cursos de formación práctica.

Si lo desea, combinamos nuestra experiencia, productos y servicios para lograr soluciones industriales integrales.

Productos

Seguridad desde el desarrollo hasta la gestión de parches

La integración de la seguridad es uno de los componentes de nuestro desarrollo de productos. Comienza ya con un proceso de desarrollo seguro.

Además, muchos de nuestros productos ofrecen funciones de seguridad como la autenticación segura de usuarios, la segmentación de red, la monitorización de redes y cortafuegos o el uso de protocolos de comunicación seguros y codificados. Además, durante todo el ciclo de vida, nuestros productos se revisan para detectar lagunas de seguridad a través de un sistema de gestión de vulnerabilidades (PSIRT) y se les proporcionan parches y actualizaciones de seguridad.

Seguridad mGuard
Los routers de seguridad mGuard son la espina dorsal de la seguridad de su instalación. Ofrecen funciones especiales de cortafuegos para la industria, como cortafuegos condicionales y cortafuegos de usuario, Deep Packet Inspection para protocolos industriales y acceso seguro a la red para técnicos de servicio. Con mGuard Secure Cloud obtendrá además un sistema que permite un mantenimiento remoto sencillo y seguro.

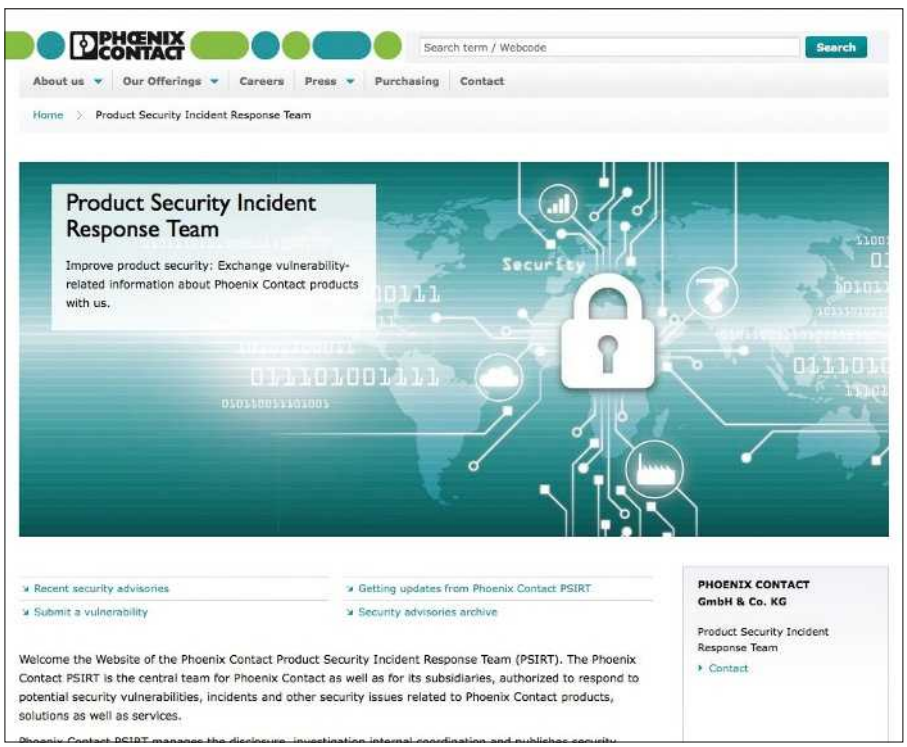
Seguridad PLCnext
Los sistemas de control PLCnext se han desarrollado conforme a criterios de Security by Design. Los procesos de desarrollo se han certificado según IEC 62443-4-1. El uso de un Trusted Platform Module (TPM), de un kernel de Linux configurable y del cortafuegos de Linux, así como la implementación de una Crypto Store para certificados y claves, son algunas de las medidas de seguridad importantes.

Gestión de vulnerabilidades: PSIRT

Para garantizar en todo momento su seguridad de forma óptima, Phoenix Contact ha consolidado el Product Security Incident Response Team (PSIRT). El equipo

- reacciona ante posibles lagunas de seguridad, incidentes y otros problemas de seguridad relacionados con los productos, las soluciones y los servicios de Phoenix Contact
- dirige la divulgación, investigación y coordinación interna de las indicaciones de seguridad
- publica indicaciones de seguridad sobre lagunas de seguridad confirmadas para las que se cuenta con medidas de mitigación o resolución.

Todas las indicaciones de seguridad actuales e históricas se indican de forma transparente en nuestra página web: https://phoenixcontact.com/psirt



Suscripción al boletín informativo PSIRT y notificación de lagunas de seguridad

Servicios

Evaluación y planificación

Basándonos en los estándares del sector creamos para usted soluciones y conceptos individuales
- para estructuras de redes con seguridad contra fallos,
- para proteger su máquina o para el mantenimiento remoto,
- para lograr redes inalámbricas potentes.

Inspeccionamos juntos su planta y analizamos sus amenazas y riesgos particulares, así como la documentación y los procesos.

Resultado:
Recibirá un informe detallado con las vulnerabilidades y acciones recomendadas, así como una lista de las medidas necesarias para la protección estándar de su instalación conforme a la protección básica de tecnología de la información.

Implementación

Para que pueda seguir centrándose en sus competencias principales, nos encargaremos de la implementación de sus requisitos de seguridad y de red:
- configuración y documentación
- introducción de sistemas de gestión
- detección y solución de anomalías
- mantenimiento de redes
- prueba de los sistemas puestos en funcionamiento

Resultado:
Las relaciones de comunicación de su red se optimizan y se aumenta su rendimiento y disponibilidad.

Mantenimiento y soporte

Para garantizar la disponibilidad de su instalación, se deben instalar actualizaciones regularmente, se deben adaptar las reglas del cortafuegos y es necesario evaluar los mensajes.
Le ayudaremos en los siguientes casos:
- la búsqueda de fallos (por ejemplo, fallos en la configuración de equipos)
- la detección de anomalías
- la solución de fallos in situ
- la asistencia de producto personalizada

Resultado:
Como usuario, las tareas administrativas que deberá realizar son escasas y cumplirá al mismo tiempo la obligación de carga de prueba para la aplicación de medidas de última tecnología.

Seminarios

La seguridad de la información afecta en su empresa a todos los empleados.
Le ofrecemos:
- formaciones básicas de seguridad
- formaciones de sensibilización sobre la seguridad
- formaciones básicas sobre Ethernet
- formaciones sobre productos
- formaciones prácticas personalizadas a medida de sus requisitos individuales.

Resultado:
Actuando de forma segura y responsable, se pueden evitar fallos y daños en sus instalaciones y contribuir así al éxito de su empresa.

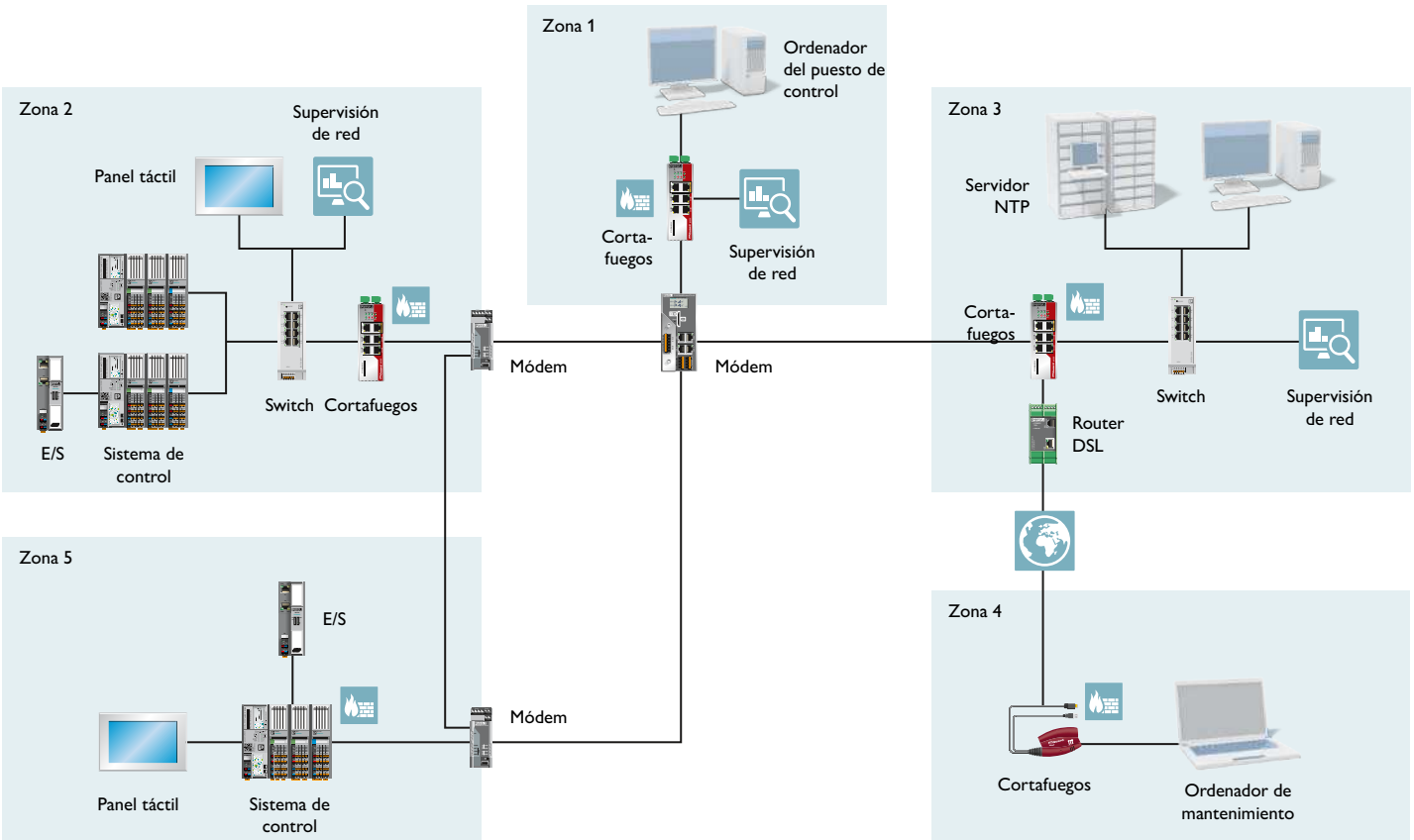
Soluciones

Soluciones de automatización seguras

Phoenix Contact tiene la capacidad de desarrollar y poner en funcionamiento soluciones de automatización seguras conforme a la norma internacional IEC 62443-2-4. Desarrollamos soluciones de automatización seguras en el marco de un análisis de los requisitos de protección y de los objetivos de protección relativos a la confidencialidad, integridad y disponibilidad. Se incluye en la oferta de servicios un análisis de amenazas, así como un análisis de riesgos de seguridad.

Para nosotros, Security by Design significa:

- determinación de los requisitos de protección
- realización de un análisis de riesgos y amenazas
- desarrollo de un concepto de red segura, con zonas y conductos, teniendo en cuenta la norma IEC 62443
- selección de productos de automatización seguros
- documentación y puesta en marcha de la instalación y
- servicios complementarios para la instalación (p. ej. gestión de parches) a lo largo del ciclo de vida.



Seguridad de los datos normalizada:

Phoenix Contact mantiene un sistema de gestión de la seguridad de la información ("SGSI") que se ha creado conforme a los requisitos de la norma ISO/IEC 27001. El ISMS define, entre otras cosas, el manejo de datos e información confidenciales, desde la seguridad IT y el tratamiento de datos confidenciales y de clientes hasta la seguridad de red.

Además, Phoenix Contact Energy Automation GmbH ha sido la primera empresa del grupo Phoenix Contact en obtener la certificación ISO/IEC 27001.

Haga la comprobación de seguridad

¿Cuál es el estado de la seguridad de su empresa? Esta lista de comprobación le ayudará a obtener una primera visión general del estado de seguridad de su sistema.

Estaremos encantados de enviarle por correo electrónico el "Quick Check" completo de ciberseguridad industrial o de asesorarle personalmente con un análisis detallado de la situación actual in situ.

Lista de verificación

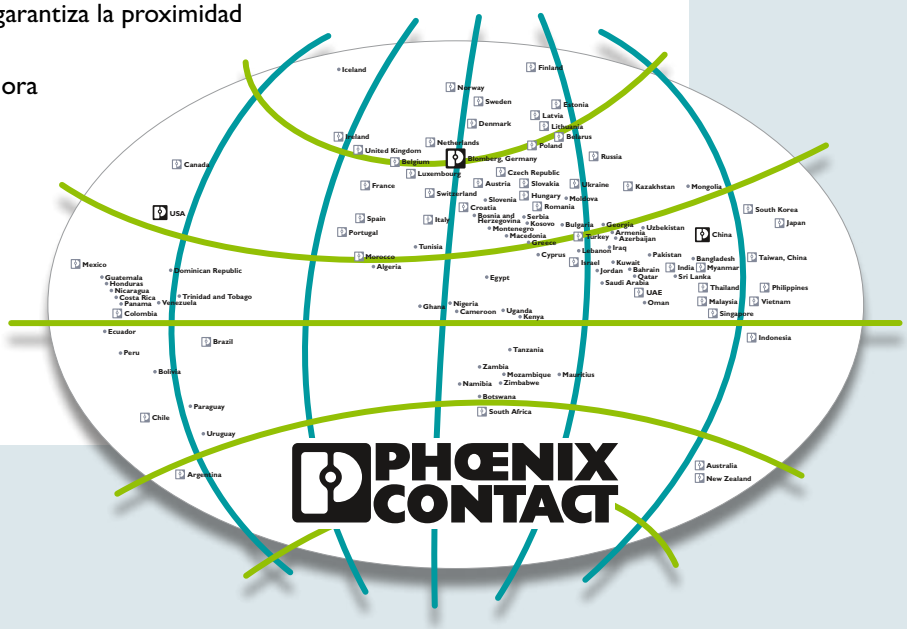
Requisitos	Sí	No	Notas
¿Han firmado todos los empleados internos y externos un acuerdo de confidencialidad?	☐	☐	
¿Se ha determinado qué permisos de acceso se han asignado a qué personas en el ámbito de sus funciones?	☐	☐	
¿Las contraseñas se personalizan y se cambian regularmente?	☐	☐	
¿Se forma o sensibiliza con regularidad a los empleados sobre cuestiones relacionadas con la seguridad de la información?	☐	☐	
¿Está prohibido el uso privado de hardware y software oficial?	☐	☐	
¿La integración de soportes de datos móviles (lápices USB, discos duros USB, etc.) en sistemas de tecnología de la información o de automatización está documentada y regulada en una directiva?	☐	☐	
¿Se han segmentado sus redes?	☐	☐	
¿Ha instalado cortafuegos que filtran la comunicación de datos en la red y regulan los permisos de acceso?	☐	☐	
¿Está desactivado el acceso de mantenimiento remoto durante el funcionamiento normal y está solo habilitado en casos excepcionales? ¿Se ha documentado el requisito?	☐	☐	
¿Está codificada la comunicación externa, por ejemplo, a través de un túnel VPN?	☐	☐	
¿Los sistemas se revisan regularmente para detectar vulnerabilidades y se actualizan?	☐	☐	
¿Saben los empleados qué deben hacer en caso de un incidente de seguridad? ¿Existe alguna guía que describa cómo restaurar el funcionamiento correcto después de un fallo grave?	☐	☐	

Si la respuesta es no a una o varias preguntas, póngase en contacto con Phoenix Contact.
Estaremos encantados de asesorarle y de apoyarle con los servicios y productos de consultoría adecuados.

En contacto con clientes y socios de todo el mundo

Phoenix Contact es un líder de mercado a escala internacional con sede en Alemania. El grupo empresarial es sinónimo de componentes, sistemas y soluciones innovadoras en el sector de la electrotecnia, la electrónica y la automatización. Una red global en más de 100 países con 17.400 empleados garantiza la proximidad al cliente.

Con una gama de productos amplia e innovadora ofrecemos a nuestros clientes soluciones sostenibles para distintas aplicaciones e industrias. Los principales sectores son la energía, la infraestructura, los procesos y la automatización de plantas.



Encontrará nuestro programa de productos completo en nuestra página web.

Alemania:
PHOENIX CONTACT GmbH & Co. KG
D-32823 Blomberg, Germany
Tel.: 0049 52 35 3 00
Fax: 0049 52 35 34 12 00
phoenixcontact.com

Argentina:
PHOENIX CONTACT S.A.
Edificio Madero Riverside,
Boulevard Cecilia Grierson 255, piso 8° Sur
1107 CABA, Buenos Aires
República Argentina
Tel.: 0054 11 3220 6400
Fax: 0054 11 3220 6438
e-mail: info@phoenixcontact.com.ar
phoenixcontact.com.ar

Chile:
PHOENIX CONTACT S.A.
Calle Nueva 1661-G
Huechuraba - Santiago - Chile
Tel.: 00562 652 2000
Fax: 00562 652 2050
phoenixcontact.cl

España:
PHOENIX CONTACT, S.A.U.
Parque Tecnológico de Asturias,
parcelas 16-17
33428 Llanera (Asturias)
Tel.: 0034 98 579 1636
Fax: 0034 98 598 5559
e-mail: info@phoenixcontact.es
phoenixcontact.es

México:
PHOENIX CONTACT S.A. DE C.V.
Lago Alberto 319 Piso 9
Colonia Granada
Delegación Miguel Hidalgo
11520 Ciudad de México
Tel.: 0052 55 1101-1380 al 1399
Fax: 0052 55 1101-1381
phoenixcontact.com.mx

Printed in Germany

AI 05-19.000.L3
MNR 1110045/2019-03-15/00

PHOENIX CONTACT
INSPIRING INNOVATIONS