REVISTA SOBRE CIBERSEGURIDAD DE AXIS COMMUNICATIONS

Socios para la protección

IDEAS E INSPIRACIÓN DEL MUNDO DE LA CIBERSEGURIDAD

Acceder >

AXIS COMMUNICATIONS

INTRODUCCIÓN

Cimientos sólidos para reforzar la protección

Como seguramente ya sabrá, no hay una única solución capaz de dar respuesta a todos los desafíos en materia de ciberseguridad ni tampoco productos infalibles en este terreno. La ciberseguridad es más bien una cuestión de confianza entre todas las partes implicadas, desde la cadena de proveedores hasta el fabricante y desde los instaladores e integradores hasta los usuarios finales, porque todos ellos tienen un papel importante. Y también de procesos, porque un hito aislado de poco sirve.

Esta recopilación de artículos, consejos e ideas nace de nuestra voluntad de contribuir a la mejora de la ciberseguridad. Creemos que pueden ayudarle a estar al día y proteger su negocio, y esperamos que le resulten útiles.

Antes de que pase a la siguiente página, me gustaría llamar su atención sobre el marco de gestión de riesgos del NIST (National Institute of Standards and Technology). La ciberseguridad tiene que ver básicamente con la gestión del riesgo. Y, por este motivo, un buen punto de partida en esta carrera de fondo es evaluar los riesgos potenciales de su negocio u organización en términos de probabilidad y nivel potencial de daños usando un marco de gestión de riesgos.

Hay muchos marcos, pero en Axis hemos decidido usar el del NIST como base de nuestra estrategia de ciberseguridad. Las pautas del NIST se utilizan a escala mundial y son apropiadas no solo para grandes empresas y organizaciones, sino también para pequeñas y medianas empresas. Incluso si su organización utiliza un marco diferente, es probable que sea compatible con el del NIST.

El marco del NIST tiene cinco pilares: Identificar, Proteger, Detectar, Responder y Recuperar. Encontrará más información sobre cada pilar, nuestro papel como su socio en ciberseguridad y sus responsabilidades en esta área en nuestro sitio web: www.axis.com/cybersecurity.

¡Pero ahora es momento de disfrutar de la revista!

ÍNDICE

Qué puede aprender la ciberseguridad de la seguridad física

Los riesgos asociados a la seguridad física son evidentes para la mayoría de la gente. Una puerta abierta aumenta el riesgo de acceso de personas sin autorización. La colocación de artículos de valor a la vista incrementa el riesgo de robo. Las personas, las instalaciones y los objetos pueden sufrir las consecuencias de errores y accidentes.

Prácticamente no hay diferencias a la hora de abordar la seguridad física y la ciberseguridad. Tanto si está al frente de la seguridad física de su organización como si se ocupa de la ciberseguridad, tendrá que aplicar los mismos principios:

- Identifique y clasifique sus activos y recursos (qué necesita proteger)
- Identifique posibles amenazas (de quién debe protegerse)
- Identifique las vulnerabilidades que las amenazas pueden intentar aprovechar (la probabilidad)
- Identifique los posibles costes de una amenaza consumada (las consecuencias)

El riesgo suele definirse como la probabilidad de una amenaza multiplicada por el daño que puede ocasionar. Una vez determinado este valor, debe preguntarse qué está dispuesto a hacer para prevenir un impacto negativo.

Identifique sus activos y recursos

Si nos fijamos en los sistemas de vídeo, el recurso que debemos proteger es el vídeo grabado por las cámaras. El activo son las grabaciones de vídeo del sistema de gestión de vídeo (VMS). El acceso se controla normalmente mediante privilegios otorgados a los usuarios. Otros activos que también debemos tener en cuenta son las cuentas de usuario y las contraseñas, las configuraciones, el sistema operativo, el firmware y el software, y los dispositivos con conectividad de red.

Seguir leyendo >

¿Qué amenazas debe tener en cuenta?

El primer paso en el camino para reforzar la ciberseguridad es conocer a qué ciberamenazas se enfrenta. La confidencialidad, la integridad y la disponibilidad deben centrar nuestros esfuerzos de protección en los sistemas de TI. Cualquier comportamiento que tenga un impacto negativo en uno de estos pilares está considerado un incidente de ciberseguridad. Veamos ahora cuáles son las ciberamenazas más habituales y qué vulnerabilidades aprovechan.

Las tres ciberamenazas más habituales en videovigilancia

1. Error humano involuntario o desconocimiento
2. Utilización fraudulenta del sistema
3. Sabotaje y manipulación física

Seguir leyendo >

1

Error humano involuntario o desconocimiento

Aunque utilice la mejor tecnología del mercado para proteger su red, si un atacante consigue que una sola persona haga clic en un enlace peligroso en un correo, estará dentro del sistema. Y, como es tan fácil, es la vía de entrada preferida por los ciberdelincuentes. Entre los errores humanos que abren la puerta a los ciberataques, encontramos:

- **Ingeniería social:** esta práctica consiste en utilizar la manipulación psicológica para que una persona cometa errores de seguridad o revele información confidencial. Algunos ejemplos de ingeniería social serían el phishing y el scareware.
- **Uso incorrecto de las contraseñas:** este supuesto incluye el uso de contraseñas poco seguras y también la falta de protección o actualización.
- **Falta de vigilancia con los componentes críticos:** el atacante consigue acceder al sistema porque hemos perdido o extraviado un componente esencial, como tarjetas de acceso, teléfonos, portátiles y documentación.
- **Gestión deficiente del sistema:** el acceso es más fácil cuando no se instalan actualizaciones del sistema o parches de seguridad.
- **Mejoras con efectos perjudiciales:** este supuesto se da cuando alguien intenta arreglar un problema, pero perjudica el funcionamiento del sistema.

Vulnerabilidades y errores humanos

Algunas de las vulnerabilidades más habituales provocadas por los errores humanos son un conocimiento insuficiente sobre la ciberseguridad y la falta de políticas y procesos de largo recorrido para gestionar el riesgo. Para reducir las amenazas vinculadas a los errores humanos, todas las personas de la organización deben recibir formación sobre las prácticas recomendadas en ciberseguridad. Asimismo, es recomendable limitar el acceso al vídeo y dar privilegios de acceso a un grupo de personas muy reducido a través del VMS.

Seguir leyendo >

Utilización fraudulenta del sistema

2

Otra de las ciberamenazas más habituales es la utilización fraudulenta del sistema de vídeo por parte de personas con autorización. Estos son algunos tipos de utilización fraudulenta:

- Acceso sin autorización y manipulación de servicios y recursos del sistema
- Robo de datos
- Acciones que provocan daños deliberados en el sistema

Vulnerabilidades y utilización fraudulenta

Es fundamental aplicar políticas y procesos de largo recorrido para gestionar las vulnerabilidades y minimizar el riesgo de una utilización fraudulenta del sistema. Es importante analizar bien a qué personas se le otorgan privilegios que dan acceso a datos delicados y también limitar el número de personas con estos privilegios. Los dispositivos deben tener cuentas distintas para la administración y para las operaciones del día a día (el VMS), además de una cuenta temporal de mantenimiento y resolución de problemas. Si se utiliza una misma cuenta para todo, es fácil que la contraseña circule por la organización y se abre la puerta a una utilización fraudulenta o errores accidentales.

Seguir leyendo >

3

Sabotaje o manipulación física

La protección física de los sistemas de TI es extremadamente importante desde el punto de vista de la ciberseguridad:

- Los equipos expuestos físicamente son fáciles de manipular.
- Los componentes expuestos físicamente son fáciles de robar.
- Los cables expuestos físicamente pueden desconectarse, cortarse o conectarse a otro sitio.

Vulnerabilidades y amenazas físicas

No solo las cámaras pueden ser objeto de manipulación; los cables de red también, y ofrecen una magnífica oportunidad para acceder a la red. Otras vulnerabilidades que abren la puerta a amenazas potencialmente peligrosas son el acceso a equipos de red, como servidores y switches en lugares no cerrados, cámaras en lugares accesibles y sin una carcasa protectora, y cables fuera de paredes o tubos.

Analice el impacto negativo para su organización

Los sistemas de vídeo no procesan transacciones financieras ni almacenan datos de clientes. Por lo tanto, un ataque a un sistema de vídeo es difícil de rentabilizar y tiene un interés limitado para los delincuentes organizados. Sin embargo, un sistema manipulado puede ser una amenaza para otros sistemas. Por todo ello, es complicado realizar una estimación de los costes. Por desgracia, en muchos casos las organizaciones aprenden la lección cuando viven una mala experiencia. La protección es como la calidad: recibes lo que pagas. Y si compras barato, al final puedes acabar pagando mucho más.

Las claves de una buena ciberhigiene

Entendemos por ciberhigiene las prácticas y medidas adoptadas por usuarios de sistemas y dispositivos con el objetivo de mantener una buena salud del sistema y mejorar la seguridad online. A menudo la ciberhigiene se integra en los procesos internos generales de la organización para reforzar la seguridad de la información sobre la identidad y otros datos que pueden ser objeto de robos o usos fraudulentos. Al igual que ocurre con la higiene física, la ciberhigiene debe convertirse en una práctica habitual si queremos evitar el deterioro natural y acabar con las amenazas más frecuentes.

Ventajas de una buena ciberhigiene

La implantación de prácticas rutinarias de ciberhigiene en los dispositivos y en el software refuerza la seguridad y facilita el mantenimiento.

- Un buen mantenimiento es clave para que el funcionamiento de los dispositivos y el software sea siempre el óptimo. Los archivos fragmentados y los programas desfasados aumentan el riesgo de sufrir vulnerabilidades. Los procedimientos de mantenimiento facilitan la identificación temprana de estos problemas y pueden evitar complicaciones graves. En general, los sistemas con un buen mantenimiento son menos vulnerables a los riesgos de ciberseguridad.
- Hackers, ladrones de identidad, virus, malware inteligente... Las organizaciones están siempre en peligro. Con un buen análisis de las amenazas y la implementación de unas prácticas de ciberhigiene apropiadas, es más fácil una detección temprana y también evitar que los riesgos se conviertan en una realidad.

Al igual que ocurre con la higiene física, la ciberhigiene debe convertirse en una práctica habitual

Seguir leyendo >

Use contraseñas seguras y no repetidas

Puede parecer obvio, pero la vía de entrada a un sistema más utilizada por los ciberdelincuentes son las contraseñas poco seguras. La mayoría de los dispositivos IP se entregan configurados con contraseñas y ajustes por defecto. Y, por lo tanto, es esencial cambiarlos inmediatamente siguiendo la política de la empresa o del departamento de TI. Las organizaciones tienen que instaurar un buen sistema de gestión de contraseñas: uso de contraseñas seguras y no repetidas (con un mínimo de 8 caracteres), renovación periódica de contraseñas y prohibición de compartir contraseñas entre sitios. Las políticas de contraseñas no pueden imponerse a través de sistemas informáticos. Cada organización debe poner los medios para formar a sus empleados sobre las prácticas recomendadas en este campo. Además, se recomienda usar certificados para cifrar las contraseñas y los nombres de usuario.

Una contraseña formada por una única palabra común o un nombre puede descifrarse en cuestión de segundos, independientemente de su longitud.

Siga la política de redes de seguridad o TI al implantar e instalar dispositivos

Evite dejar activados los servicios que no utilice al implantar un dispositivo, porque los ciberdelincuentes pueden usarlos para atacar e instalar aplicaciones maliciosas. Si desactiva los servicios que no utiliza e instala solo aplicaciones de confianza, se reducen las opciones de que un hacker pueda aprovechar una vulnerabilidad del sistema. Es importante también una correcta instalación física de los dispositivos, así como evitar que los puertos de red y los puertos de las tarjetas SD sean accesibles al público.

Seguir leyendo >

Defina unos privilegios de acceso claros

Es importante establecer unas reglas y procedimientos claros para que los empleados tengan los derechos de acceso correctos según su área de responsabilidad. Las organizaciones deben tener una consigna clara: conceder los usuarios acceso únicamente a los recursos que necesitan para hacer su trabajo. No hay que utilizar cuentas por defecto bajo ningún concepto. Si utiliza cuentas temporales para tareas de mantenimiento, debe eliminarlas cuando haya terminado.

No utilice nunca los ajustes por defecto de un dispositivo, y mucho menos la contraseña. Los nombres de usuario y las contraseñas usados por defecto en las cuentas de administración de los dispositivos más habituales pueden descifrarse con una sencilla búsqueda en Google, por lo que son una vía de entrada muy fácil para los hackers. No olvide activar y configurar los servicios de protección de los equipos y utilice los ajustes predeterminados solo para demostraciones.

61%
de los trabajadores usan sus dispositivos para cuestiones profesionales y personales

80%
de los empleados reconoce que usa aplicaciones de software como servicio (SaaS) no autorizadas en su trabajo

75%
de los accesos sin autorización a redes han sido posibles gracias a credenciales robadas o poco seguras

Seguir leyendo >

Utilice la última versión del firmware

¿Sus dispositivos tienen instalada la última versión del firmware? Los errores y los fallos de sistemas y equipos exponen las organizaciones a posibles ataques y abren la puerta al robo de claves privadas de servidores o contraseñas de usuarios. Es importante contar con un plan de gestión de actualizaciones de software/firmware bien documentado y poner los medios para que los dispositivos de red tengan instaladas siempre las últimas actualizaciones de firmware y seguridad.

Realice un análisis de los riesgos

¿Cuánto debería gastar su organización en protección de activos? Analice las posibles amenazas internas y externas, así como las implicaciones de pérdidas o daños en sus principales activos. Con esta información en la mano, sabrá cómo priorizar sus esfuerzos de protección. Existen también los marcos de gestión de riesgos, como el marco de ciberseguridad del NIST (National Institute of Standards and Technology), que pueden proporcionarle procesos y pautas.

El número de robos de datos creció exponencialmente en 2019 con más de

8.500 millones de datos

expuestos, una cifra que multiplica por tres el incremento interanual registrado en 2018.*

* IBM X-Force Threat Intelligence Index 2020. Gain knowledge on system protection and possible threats

Seguir leyendo >

¿Es segura su cadena de suministro?

Si suma esfuerzos con toda su cadena de suministro, entenderá mejor las posibles amenazas que pueden afectar a su red y a los dispositivos conectados. Actualmente, muchos fabricantes de TI ofrecen prácticas recomendadas o guías para reforzar la protección de los dispositivos en su red, además de documentación para una cadena de suministro segura. En caso de no tenerla, es importante hablar con el fabricante para que se ponga manos a la obra o buscar documentación generada por otros usuarios. Los dispositivos deben cumplir con su política de TI, individualmente y también como sistema.

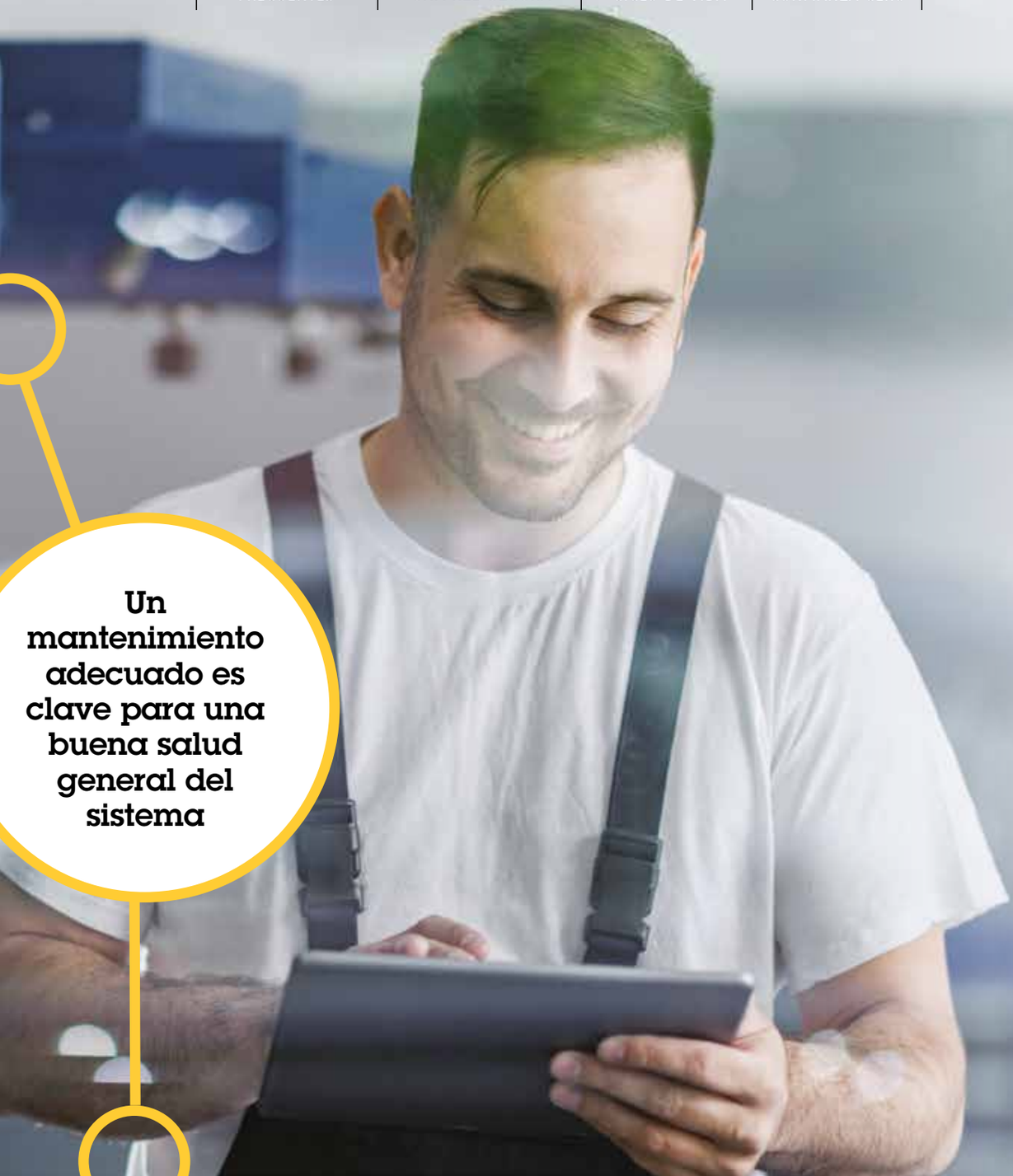
Utilice siempre conexiones cifradas

Sea cual sea su sector, es imprescindible el cifrado seguro de todos los datos. Las conexiones cifradas deben utilizarse también en todas las redes, incluso en las locales o "internas". Los protocolos de autenticación garantizan que la información se cifra antes de enviarla a través de la red y reducen considerablemente las probabilidades de sufrir ataques, puesto que el código malicioso "escucha" básicamente transmisiones no cifradas.

Protocolos seguros

- La autenticación (acceso) HTTP Digest es uno de los métodos contrastados que puede usar un servidor web para confirmar credenciales y la identidad de un usuario, como el nombre de usuario o la contraseña.
- HTTPS (HyperText Transfer Protocol Secure, protocolo seguro de transferencia de hipertexto) es el protocolo más habitual para el cifrado de datos. HTTPS es idéntico a HTTP, con la única diferencia de que hay una capa más de cifrado usando Secure Sockets Layer (SSL) o Transport Layer Security (TLS).
- SRTP (Secure Real-Time Transport Protocol, protocolo de transporte seguro en tiempo real) cifra la transmisión de vídeo para reforzar la protección del vídeo. Si utiliza un VMS o tarjetas SD para el almacenamiento local del vídeo, es importante que también estén cifradas.

Seguir leyendo >



Un mantenimiento adecuado es clave para una buena salud general del sistema

Proteja el perímetro de la red

¿Entiende sus cortafuegos y filtros? Si es capaz de proteger la columna vertebral de su red, le resultará más fácil implementar otras prácticas recomendadas para reforzar la ciberseguridad. El uso de mecanismos de segmentación de la red, como VLAN (redes de área local virtuales), en dispositivos de seguridad física reduce el riesgo de acceso sin autorización a información delicada y también los ataques a servidores y equipos de red concretos. Además, las ACL (listas de control de acceso) pueden ayudarle a controlar movimientos maliciosos en la red. Antes de invertir en nuevos dispositivos, pida a su proveedor una lista con los puertos de la red para asegurarse de que la solución funcionará en toda la red.

Realice un buen mantenimiento de los sistemas y procesos

Un mantenimiento adecuado es clave para una buena salud general del sistema. Es importante revisar periódicamente los registros de dispositivos y sistemas para detectar cualquier intento de acceso sin autorización. En el mundo de la tecnología los cambios se producen a una velocidad vertiginosa y constantemente aparecen nuevas actualizaciones, funciones y prácticas recomendadas. De ahí que sea vital documentar los procedimientos de mantenimiento; solo así conseguiremos que todo el mundo los entienda.

Las aplicaciones de software de gestión de dispositivos, como AXIS Device Manager, pueden ayudar a las organizaciones a obtener un inventario en tiempo real de todos los dispositivos y software conectados a la red. Estas aplicaciones analizan toda la red y registran toda la información clave, como el número de modelo, las direcciones IP y MAC, la versión del firmware y el estado del certificado.

¿Por qué es vital implementar una gestión efectiva del ciclo de vida?

La seguridad de una red es directamente proporcional a la seguridad de los dispositivos que están conectados a ella. Y, aunque las organizaciones suelen implementar prácticas de protección por capas para reforzar sus redes, deben contar con procedimientos efectivos para gestionar el ciclo de vida de sus equipos físicos. Sin embargo, a menudo no actualizan su software cuando hay nuevas versiones del firmware. Y eso pasa porque no tienen una visión de conjunto de todas las tecnologías de su red.

Un dispositivo, dos ciclos de vida

Hay dos tipos de ciclos de vida asociados a los dispositivos basados en software.

1. El ciclo de vida funcional del dispositivo, es decir, durante cuánto tiempo puede funcionar un dispositivo realizando una estimación realista. Por ejemplo, una cámara de red suele tener un ciclo de vida funcional de 10-15 años.

2. El ciclo de vida económico del dispositivo, esto es, cuánto tiempo debe pasar para que el coste del mantenimiento sea superior al de adoptar una nueva tecnología más eficiente. Por ejemplo, una cámara IP puede funcionar 15 años, pero su vida útil suele ser más corta a causa de los rápidos cambios en el mundo de la ciberseguridad.

Apueste por una gestión proactiva

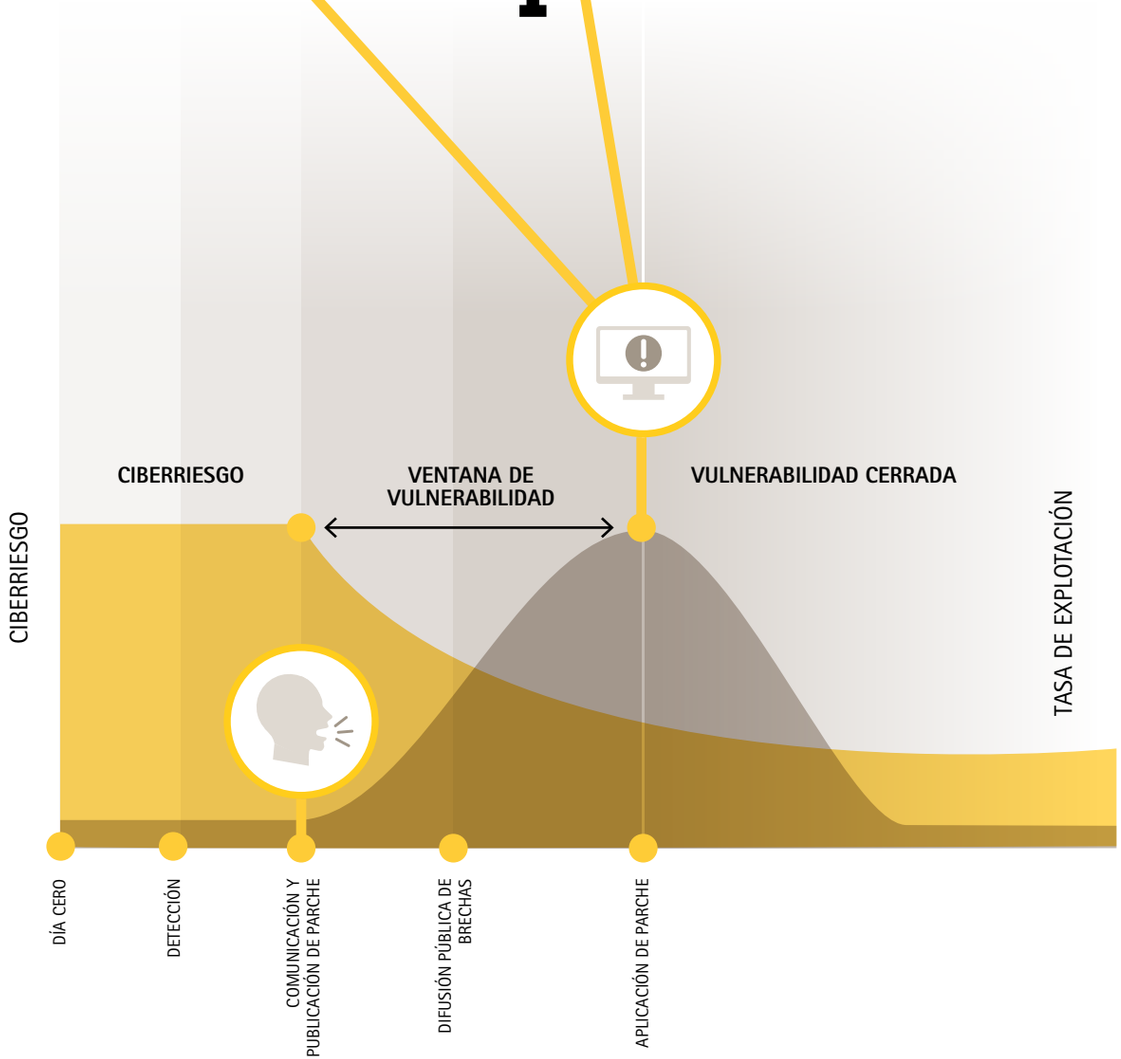
La gestión del ciclo de vida consiste en gestionar de manera efectiva tanto el ciclo de vida funcional como económico de sus equipos físicos. Para las organizaciones es vital tener una visión de conjunto de todas las tecnologías implantadas en su red. Solo así podrán supervisar de cerca qué ocurre en sus redes y con sus datos críticos, además de protegerse frente a amenazas y vulnerabilidades.

Según datos de la Information Commissioner's Office (ICO) del Reino Unido

"El 60% de los ataques llegaron a través de vulnerabilidades para las que había un parche, que no se aplicó."

Seguir leyendo >

No hay nada como un buen plan



En algún punto, todos los dispositivos tecnológicos (desde cámaras de red hasta VMS) necesitan actualizaciones y parches para evitar que los hackers aprovechen las vulnerabilidades conocidas y pongan en jaque las protecciones existentes.

Las actualizaciones y los parches son la mejor forma de mejorar la ciberseguridad, pero no siempre están disponibles en tecnologías con varios años a sus espaldas. La razón es sencilla: el fabricante ha dejado de ofrecer actualizaciones. Y, desde la perspectiva de la ciberseguridad, las tecnologías antiguas y sin parches son las que representan un mayor riesgo. Es vital que las organizaciones estén al día de las últimas amenazas y sigan en todo momento las prácticas recomendadas más recientes. Un solo dispositivo fuera de control puede ser la vía de entrada que necesitan los hackers.

Infórmese sobre las nuevas amenazas

Una gestión efectiva del ciclo de vida es clave para reforzar la seguridad de una organización. Y también para que pueda prepararse de cara al futuro. Pero eso solo es posible si conocemos los riesgos a los que nos enfrentamos y estamos al día sobre posibles vulnerabilidades. Esta información es especialmente importante en el caso de los sistemas de seguridad, porque si una cámara de vigilancia de red deja de estar operativa, las consecuencias pueden ser nefastas.

Los dispositivos físicos también deben actualizarse

Los fabricantes publican periódicamente actualizaciones de firmware y parches de seguridad para corregir vulnerabilidades o errores y para solucionar otros problemas de funcionamiento, siempre con el objetivo de mejorar la estabilidad y la seguridad del sistema. Y aunque muchas organizaciones entienden la importancia de instalar los parches en sistemas operativos y aplicaciones, a menudo olvidan el firmware que constituye la base de su hardware. Esta falta de mantenimiento puede aumentar el riesgo de ciberataques y puede tener como consecuencia desde la filtración de valiosos datos de clientes hasta cuantiosas multas de los reguladores por incumplimiento de la normativa.

Seguir leyendo >

Gestión optimizada del ciclo de vida

Con un programa de gestión del ciclo de vida estructurado, las organizaciones pueden prepararse para el futuro con todas las garantías. Estos programas utilizan las tecnologías más avanzadas y apropiadas para minimizar las amenazas de seguridad y las vulnerabilidades. Un software de gestión de dispositivos como AXIS Device Manager puede ayudar a automatizar esta tarea y facilitar la gestión de equipos.

¿Cómo funciona?

El software de gestión de dispositivos puede generar un inventario completo y en tiempo real de todas las cámaras, codificadores, componentes de control de acceso, equipos de audio y otros dispositivos conectados a la red. Analiza toda la red en busca de dispositivos nuevos o actualizados y, cuando los encuentra, registra toda la información clave, como el número de modelo, las direcciones IP y MAC, la versión del firmware y el estado del certificado.

Visión completa de la red

Con una visión al detalle de todo el ecosistema de la red, es fácil implementar políticas y prácticas uniformes de gestión del ciclo de vida en todos los dispositivos y también gestionar de forma segura todas las tareas importantes de instalación, implementación, configuración, seguridad y mantenimiento.

Ahórrese tiempo y esfuerzos

Un software de gestión de dispositivos ayuda a las organizaciones a ahorrarse mucho tiempo y quebraderos de cabeza en la gestión de los riesgos de ciberseguridad. Con este tipo de software, podrá agilizar el mantenimiento del sistema:

- Envíe cambios en el sistema, actualizaciones de firmware y nuevos certificados a todos los dispositivos relevantes simultáneamente.
- Cree y reconfigure fácilmente ajustes de seguridad y aplíquelos en toda la red para asegurarse de que todos los dispositivos cumplen con las políticas y prácticas de seguridad más recientes.
- Compruebe que todos los dispositivos utilizan la última versión del firmware, que es siempre la más segura.
- Gestione los niveles de privilegios de los usuarios en toda la red e introduzca modificaciones.

Seguir leyendo >

La información que necesita, en tiempo real

Las herramientas de gestión de dispositivos ofrecen a las organizaciones información en tiempo real sobre el estado de su ecosistema. Por ejemplo, puede ver qué dispositivos están actualizados con los últimos parches, actualizaciones de software y certificados. Y descubrirá si se recomienda la retirada de algún equipo concreto porque el fabricante ha dejado de actualizarlo. Este dato es muy útil, porque le ayudará a determinar si su dispositivo puede ser presa de algún tipo de malware. Y, además, tendrá acceso a toda la información que necesita para atajar otras vulnerabilidades antes de que pongan en peligro su red.

Seguridad proactiva en todo el ecosistema

La automatización de los procesos de gestión de dispositivos resulta útil para proteger las redes frente a amenazas y vulnerabilidades. Sin embargo, las organizaciones deben asegurarse también de que aplican las políticas y prácticas de ciberseguridad más relevantes. Por ejemplo, ¿su organización cuenta con políticas que definan el nivel de seguridad de las contraseñas y la frecuencia con que deben cambiarlas los usuarios? ¿Ha incluido en sus prácticas recomendadas la necesidad de desactivar los servicios que no se utilizan para reducir las vías de entrada para posibles ataques? ¿Con qué frecuencia se analizan los dispositivos en busca de vulnerabilidades? ¿Tiene pautas de actuación para evaluar los niveles de riesgo cuando un fabricante alerta de vulnerabilidades conocidas? Estas son algunas de las preguntas que debería hacerse para identificar e implementar medidas que le permitan proteger su ecosistema de red de forma proactiva.

5 ventajas de la gestión automatizada del ciclo de vida

1. Centre su atención en la tecnología crítica de su entorno
2. Infórmese con antelación sobre qué tecnologías llegarán al final de su vida
3. Evite sorpresas como la necesidad de sustituir un componente importante del sistema de repente
4. Planifique tranquilamente la sustitución de dispositivos
5. Presupueste la sustitución de un porcentaje previsible de dispositivos cada año

¿Qué son las redes de confianza cero?

Las redes son cada vez más vulnerables. Las amenazas son dobles: por un lado, ciberataques cada vez más sofisticados y numerosos y, por el otro, el crecimiento exponencial de los dispositivos conectados (y cada uno representa una nueva posible vía de entrada para un ataque a la red). Y, este contexto, ha surgido el concepto de "confianza cero" y, con él, las redes y arquitecturas de confianza cero. Para los fabricantes de hardware, incluido Axis, es esencial prepararse para un futuro de confianza cero. Un futuro que está más cerca de lo que imaginamos.

La consigna es no confiar en nada ni en nadie

Como sugiere su nombre, en una red de confianza cero la idea es que no confiamos en ningún elemento que se conecte a la red o esté dentro de la misma, tanto si trata de una persona como de una máquina. Este principio se aplica independientemente de su ubicación y de su modalidad de conexión. La filosofía es "no confiar nunca, verificar siempre".

Privilegios de acceso: los mínimos imprescindibles

Este sistema exige verificar varias veces y de distintas formas la identidad de cualquier elemento que pretenda acceder a la red o esté dentro de la misma, siempre según el comportamiento y el nivel de confidencialidad asociado a los datos consultados. En resumen, las personas o equipos deben tener los privilegios de acceso mínimos imprescindibles para cumplir su cometido.

En una red de confianza cero, la idea es que no confiamos en ningún elemento que se conecte a la red o esté dentro de la misma.

Seguir leyendo >

3 razones por las que un cortafuegos no es suficiente

Históricamente, las organizaciones han confiado su protección a la seguridad del cortafuegos de la empresa, pero este planteamiento genera cada vez más inconvenientes.

1 El potencial de daños es elevado

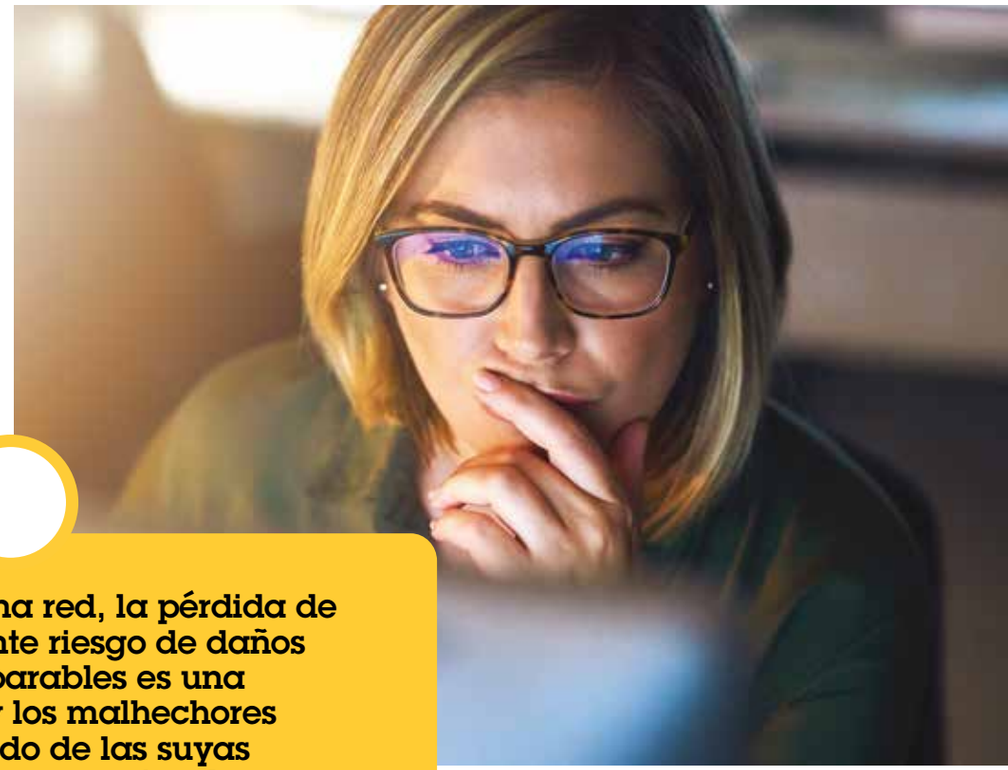
Aunque confiar en un cortafuegos parece una buena opción para proteger el acceso a la red, la contrapartida es que si alguien consigue superarlo podrá moverse con mucha libertad por la red.

2 Un cortafuegos ya no es suficiente

Son tantos los dispositivos conectados a la red actualmente que proteger el perímetro de la red con una única solución ya no es factible.

3 Las redes más “permeables” ofrecen sus ventajas

La utilización de los servicios en la nube más allá de la red y las ventajas de los sistemas de clientes y proveedores conectados sin fisuras han transformado el funcionamiento de la seguridad en red.



> **“Una vez dentro de una red, la pérdida de datos y el consiguiente riesgo de daños potencialmente irreparables es una amenaza muy real y los malhechores pueden estar haciendo de las suyas durante semanas o meses antes de que nadie los descubra (si es que lo hace).**
>
> Wayne Dorris, Directora Regional de Arquitectura e Ingeniería, Axis Communications

Seguir leyendo >

Confianza cero: cómo funciona

Los métodos de confianza cero emplean técnicas como la seguridad adaptada del perímetro de la red y la microsegmentación de la red. La primera está basada en usuarios y dispositivos: utiliza sus ubicaciones físicas y otros datos de identificación para determinar si sus credenciales son de confianza y pueden acceder a la red. La segunda aplica diferentes niveles de seguridad a partes específicas de la red en las que se almacenan datos más sensibles.

Un nivel extra de seguridad

Conceder a las personas acceso únicamente a las partes de la red y los datos que necesitan para desempeñar su trabajo tiene ventajas evidentes desde el punto de vista de la seguridad. Sin embargo, identificar los comportamientos anómalos asociados a estas identidades aporta un nivel adicional de protección. Por ejemplo, un administrador de redes puede tener amplios permisos de acceso para el mantenimiento de servidores de I+D o finanzas.

Alerta de seguridad

Se generaría una alerta de seguridad si las credenciales de ese administrador de redes se utilizaran para descargar determinados archivos esenciales o datos clave en mitad de la noche y se enviaran fuera de la red. En una red de confianza cero deberían utilizarse autenticaciones adicionales o bien se señalaría la actividad anómala en tiempo real y se notificaría al centro de operaciones de seguridad, que debería entonces investigarla.

Los comportamientos anómalos pueden ser indicio de un robo de credenciales de seguridad, un empleado enfadado o alguien en plena misión de espionaje industrial.

Seguir leyendo >

Entre en el motor de la políticas...

La base de una red de confianza cero es un motor de políticas, esto es, un software que permite a una organización crear, supervisar y aplicar reglas sobre el acceso a los datos y recursos de una red. Los motores de políticas utilizan una combinación de analítica de redes y reglas programadas para conceder permisos vinculados a funciones y basados en diferentes factores.

Peticiones: sí o no

A grandes rasgos, el motor de políticas compara cada petición de acceso a la red y el contexto con la política e indica al supervisor si se autorizará la petición o no. En una red de confianza cero, el motor de políticas define y aplica las políticas de seguridad de datos y acceso en diferentes modelos de alojamiento, ubicaciones, usuarios y dispositivos.

Definición y aplicación de reglas

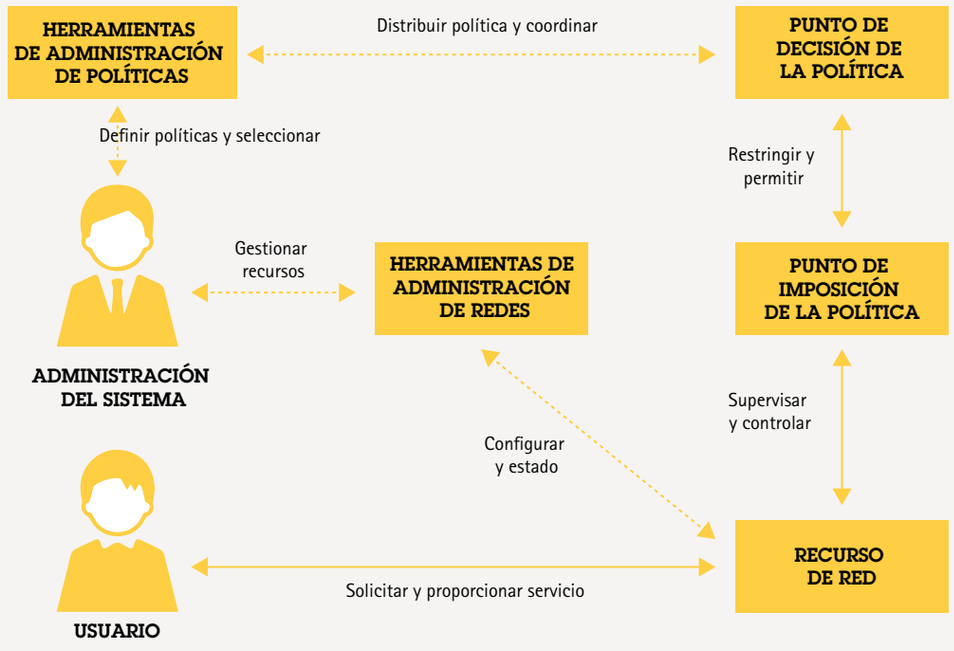
Para que un motor de políticas funcione, las organizaciones deben definir reglas y políticas vinculadas a controles de seguridad esenciales, como cortafuegos de última generación (NGFW), pasarelas de seguridad de correo electrónico y la nube, y software de prevención de pérdidas de datos (DLP). Combinados, estos controles aplican microsegmentaciones a la red que van más allá de los modelos de alojamiento y las ubicaciones.

¿Cómo se puede acceder a los datos y los recursos de la red?

Los motores de políticas permiten:

- Crear reglas
- Supervisar reglas
- Aplicar reglas

Motores de políticas: visión general



Motores de políticas de hoy y del futuro

Actualmente tal vez sea necesario definir políticas en la consola de gestión de cada solución, pero la generalización de las consolas integradas permitirá definir y actualizar automáticamente políticas para varios productos.

La gestión de la identidad y del acceso (IAM), la autenticación multifactor, las notificaciones push, los permisos de los archivos, el cifrado y la orquestación de la seguridad tienen un papel importante en el diseño de arquitecturas de red de confianza cero.

Seguir leyendo >

Redes de confianza cero y videovigilancia

En el origen de las conexiones a una red están naturalmente las personas, pero hoy en día los que más se conectan a las redes son los dispositivos. Por ejemplo, cámaras de vigilancia de red y sus dispositivos asociados conectados a una red. En el camino de las organizaciones hacia las arquitecturas de red de confianza cero, será fundamental que los dispositivos de red cumplan con la máxima de "no confiar nunca, verificar siempre".

Ironías de la vida

¿Qué ocurriría si una cámara de vigilancia diseñada para proteger físicamente una organización fuera la responsable de un fallo de ciberseguridad? Esta situación demostraría una vez más que los métodos tradicionales para garantizar la seguridad de los dispositivos ya no son suficientes. Al igual que un malhechor puede sustraer las credenciales de acceso de un empleado, puede hacer lo mismo con el certificado de seguridad de un dispositivo. En una red de confianza cero, hace falta encontrar nuevas soluciones que permitan a los dispositivos demostrar que son fiables.

Una solución con sorpresa

Una tecnología capaz de ofrecer una raíz de confianza inquebrantable para los dispositivos de hardware conectados es la tecnología blockchain o de cadenas de bloques. Para muchos, esta tecnología está asociada a las criptomonedas y es, por tanto, de dudosa reputación. Sin embargo, la cadena de bloques en sí no es más que un libro de registros abierto y distribuido capaz de anotar transacciones entre dos partes de una forma eficaz, verificable y permanente. Las organizaciones pueden utilizar cadenas de bloques privadas para usar raíces de confianza de hardware y establecer así claves de confianza inmutables entre dispositivos.

Según las previsiones habrá más de

75.000 millones

de dispositivos IoT en uso en 2025

Por qué funciona la tecnología de cadenas de bloques

A causa de la estructura de la cadena de bloques, ninguna transacción de datos en la cadena puede modificarse sin la autorización de los nodos de consenso de todas las transacciones anteriores, conectadas todas ellas criptográficamente. Por tanto, si las claves de confianza de las partes identificables de un dispositivo de hardware están integradas en la cadena de bloques, se crean credenciales inmutables para el dispositivo en sí.

La carrera armamentística con IA, en el ciberespacio

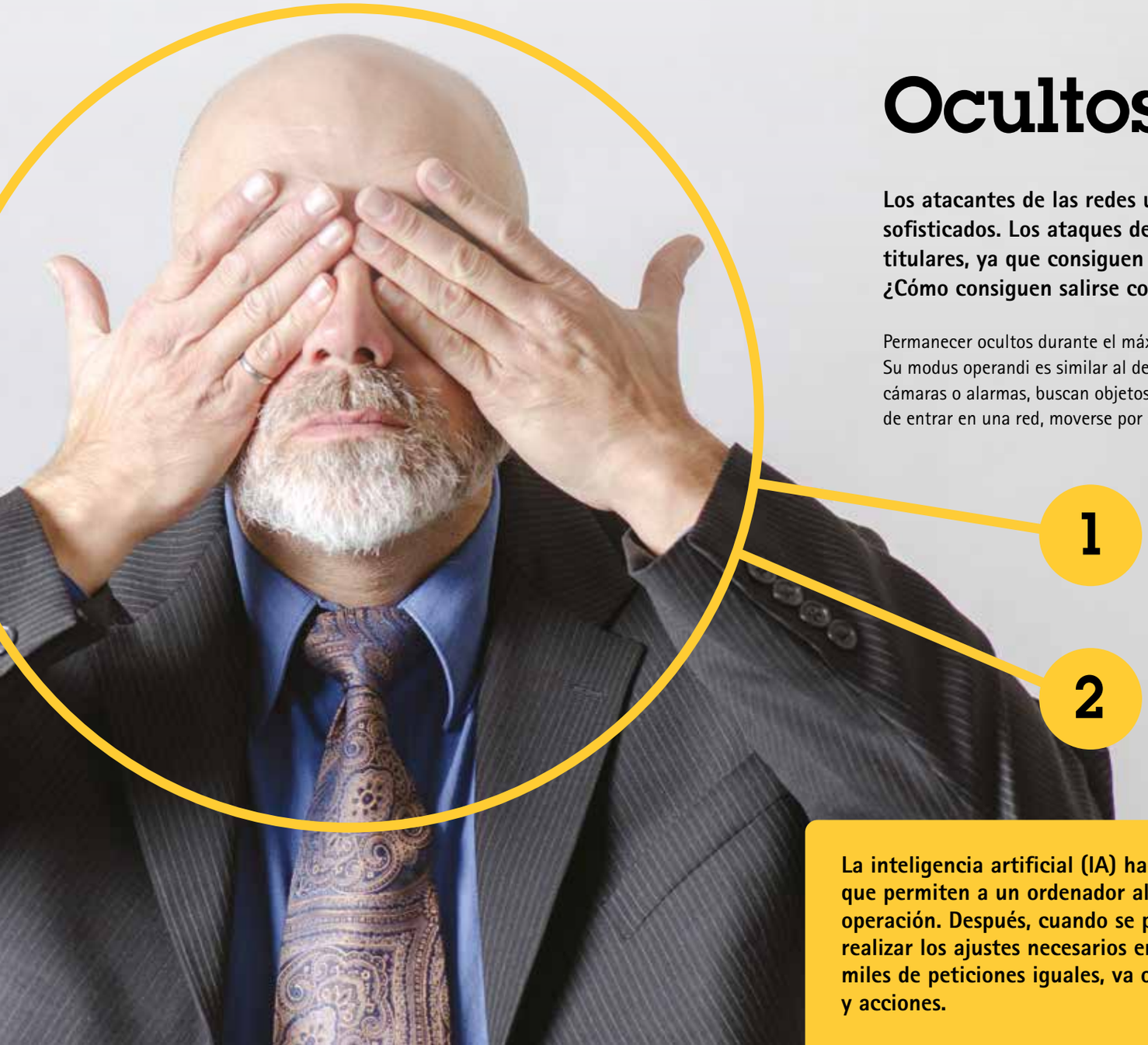
Como ocurre siempre con los avances tecnológicos, lo único seguro es que los malhechores no tardarán en tratar de aprovecharlos para seguir realizando sus actividades delictivas. Cuando los ciberdelincuentes planifican ataques de ransomware o el robo de información financiera, o cuando un estado intenta alterar la infraestructura esencial de un adversario (o algo peor), las nuevas tecnologías pueden servir para reforzar todavía más su arsenal.

Estas organizaciones pueden tener unas fuentes de financiación tan buenas como cualquier empresa legítima. Pueden innovar aplicando nuevas tecnologías como inteligencia artificial (IA), aprendizaje automático (ML) y aprendizaje profundo (DL). Y no están sometidas a legislaciones nacionales o internacionales, códigos de moral ni principios éticos.

Simplemente buscarán cómo aprovechar estas tecnologías para alcanzar sus objetivos delictivos.

Las nuevas tecnologías (también la IA) siempre terminarán en manos de los delincuentes. **Por suerte, las organizaciones expuestas a sus ataques también pueden usarlas para protegerse.**

Seguir leyendo >



Ocultos delante de todos

Los atacantes de las redes utilizan la inteligencia artificial para lanzar ataques cada vez más sofisticados. Los ataques de denegación de servicio (DDoS) a gran escala suelen copar los titulares, ya que consiguen inutilizar sitios web o servicios online ampliamente conocidos. ¿Cómo consiguen salirse con la suya?

Permanecer ocultos durante el máximo tiempo posible es el objetivo número uno de los principales ciberdelincuentes. Su modus operandi es similar al de los ladrones de casas: van de una habitación a otra, sin llamar la atención de cámaras o alarmas, buscan objetos de valor y se van sin hacer ruido. De una forma similar, los ciberdelincuentes tratan de entrar en una red, moverse por su interior y salir sin que nadie los detecte.

1

Un recurso es intentar hacerse pasar por un usuario legítimo de la red, ya sea una persona o un dispositivo. Y en este terreno la IA y el ML pueden convertirse en una poderosa arma, ya que permiten a los ciberdelincuentes conocer los comportamientos de usuarios y dispositivos en las redes, desarrollar rápidamente nuevas estrategias de malware y phishing y desplegarlas a gran escala.

2

La forma más sencilla de acceder a una red, sin embargo, sigue siendo engañar a un usuario legítimo para que haga clic en un enlace y abra la puerta. Y un falso correo electrónico de un superior (prácticamente imposible de diferenciar del real por el tono y el estilo) a veces es la llave más eficaz.

La inteligencia artificial (IA) hace referencia un conjunto de algoritmos que permiten a un ordenador almacenar y analizar el resultado de una operación. Después, cuando se produce una petición similar, puede realizar los ajustes necesarios en esta operación. A base de cientos y miles de peticiones iguales, va optimizando poco a poco sus respuestas y acciones.

Seguir leyendo >

Caminos para llegar a Roma

Los ciberdelincuentes utilizan numerosas herramientas de IA a lo largo del ciclo de vida del ataque, desde los "chatbots" para interactuar con los empleados a través de perfiles falsos en las redes sociales, hasta las redes neuronales para identificar y extraer los datos más valiosos.

El movimiento lateral por la red, una vez obtenido el acceso, es una de estas técnicas. Este paso es fundamental, ya que el punto de entrada a la red (que tal vez sea un dispositivo no protegido en una ubicación remota) raras veces es el destino final pretendido.

En última instancia, el intruso irá avanzando hasta áreas más privadas de la red, recopilando credenciales de usuarios por el camino, especialmente las de usuarios con privilegios, como los administradores de la red, para disponer de la llave de acceso a la red.

Seguir leyendo >

La peligrosa relación entre la TI y la TO

Ante el auge imparable de los dispositivos conectados y el internet of things (IoT), los riesgos se multiplican, más todavía teniendo en cuenta la estrecha integración entre la red de tecnologías de información (TI) y el entorno de la tecnología operativa (TO).

A grandes rasgos, la red de TI gestiona el flujo de información digital. En cambio, la TO controla el funcionamiento de los procesos físicos, los equipos y los recursos de una empresa o una ubicación concreta. Para los malhechores que, más que robar, buscan sobre todo sembrar el caos y la destrucción, el acceso a la TO es fundamental. No cuesta mucho imaginar los daños que pueden derivarse del acceso a la maquinaria de una central energética, una refinería o un hospital.

Seguir leyendo >

La hora de los detectives

El uso de la IA por parte de los ciberdelincuentes dibuja un panorama muy sombrío. Sin embargo, estas mismas tecnologías también están a disposición de quienes trabajan para impedir que los intrusos penetren en las redes. Y, en muchos sentidos, quienes defienden tienen ventaja sobre quienes atacan.

En muchos sentidos, quienes defienden tienen ventaja sobre quienes atacan.

DARKTRACE

Darktrace es un referente en todo el mundo por el uso de la IA en la ciberseguridad. Naturalmente, también conocen al dedillo cómo la ciberdelincuencia internacional echa mano de la IA. Darktrace no deja de innovar en el uso de la IA y la ML para ir siempre un paso por delante de los malhechores.

Seguir leyendo >

La IA como defensa y también como ataque

En las próximas páginas hablamos con Jeff Cornelius, vicepresidente ejecutivo de Darktrace, para saber cómo esta empresa utiliza la IA y el ML para ir siempre un paso por delante de los ciberdelincuentes.

Entrevista a Jeff Cornelius, de Darktrace

P

¿Es preocupante la situación?

"Para empezar, y a pesar de la imagen que puedan transmitir los medios de comunicación, el desarrollo de la IA o el ML no es precisamente un juego de niños... Y aunque los delincuentes y los estados con agendas de ciberataques son rivales duros de roer, también hay factores que juegan a nuestro favor.

"El más importante de todos es que, gracias al acceso que nos ofrecen nuestros clientes, podemos ver toda la actividad de la red. A partir de aquí podemos entender el comportamiento de cada dispositivo y usuario. En cambio, los malhechores tendrán únicamente una visión parcial de la actividad. Desde su punto de acceso inicial, cada nuevo paso que den será como adentrarse a ciegas en un entorno que nosotros conocemos y ellos no.

"Al final, para alcanzar sus objetivos deben realizar actividades que no forman parte de la normalidad de la empresa. Nuestro objetivo número uno es identificar y corregir estas anomalías en el comportamiento de la red. Sin embargo, tenemos que abrir muchísimo el foco, ya que no sabemos cuándo ni dónde puede aparecer nuestro enemigo ni qué métodos u objetivos concretos tendrá."

Seguir leyendo >

Una analogía inquietante

Entrevista a Jeff Cornelius, de Darktrace

P ¿Podría darnos más detalles?

"Haciendo una analogía, es como si alguien que estudia mis movimientos desde fuera de mi casa consigue hacerse una idea bastante precisa de mis hábitos: a qué hora salgo de casa cada día, mi ruta hacia el trabajo, dónde salgo a comer, etc. Seguramente conseguirán reproducir de una forma aceptable estas partes de mi vida.

"Pero si no ven qué ocurre dentro de mi casa, al intentar adivinar qué tomo para desayunar seguramente cometerán un error y otro miembro de la familia detectará algo raro. En internet normalmente es fácil encontrar información para lanzar un ataque individualizado con un correo de spear phishing elaborado, pero una vez dentro están sentados a nuestra mesa."

Seguir leyendo >

Aprendizaje automático supervisado...

Entrevista a Jeff Cornelius, de Darktrace

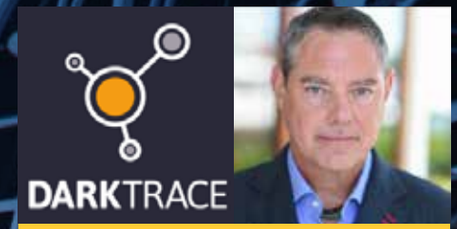
P **Cuéntenos más sobre el aprendizaje automático.**

"Desde la perspectiva de la ciberseguridad, los modelos de aprendizaje se basan en malware conocido. Y aquí es donde tiene lugar la auténtica carrera entre los delincuentes y la ciberseguridad: los malos utilizan el ML para crear nuevas versiones de malware, y en este campo observamos un crecimiento exponencial. Las empresas de ciberseguridad, por su lado, tratan de seguir el ritmo diseñando nuevos modelos para construir unas defensas basadas en el ML supervisado. Es como si una academia de la lengua intenta seguir el ritmo de un mundo en el que cada día aparecen nuevas palabras e incluso idiomas. Y seguir este ritmo cada día es más difícil, cuando no imposible.

"Es importante hacer la distinción entre el aprendizaje automático supervisado y el no supervisado. En el primer caso, se entrenan los ordenadores utilizando un conjunto de datos conocidos. Los ordenadores vuelven constantemente a estos datos para comprobar si el resultado obtenido es el previsto.

Seguir leyendo >

...o aprendizaje automático no supervisado



Entrevista a Jeff Cornelius, de Darktrace

P Pero, ¿hay otra vía?

"Sí. En lugar de confiar en la información de amenazas pasadas, los algoritmos de ML no supervisados clasifican los datos de forma autónoma y detectan patrones prevalentes. Analizan los datos de la red a gran escala y realizan miles de millones de cálculos de probabilidad basados en la información observada. A partir de aquí, determinan cuáles son los comportamientos «normales» asociados a dispositivos, usuarios o grupos de dispositivos y usuarios en una red. Así pueden detectar desviaciones respecto a este patrón que puedan ser indicativas de una amenaza. Este sistema de alerta precoz nos ayuda a ir un paso por delante de los ciberdelincuentes y malhechores."

Un esfuerzo conjunto para combatir las amenazas a la ciberseguridad

Proteger empresas, organizaciones, infraestructuras esenciales y nuestras ciudades es un trabajo colectivo. No existe una fórmula mágica ni hay una solución única. Para mantener unos buenos niveles de ciberseguridad, hace falta la colaboración entre una larga lista de actores, en la que figuran también los usuarios finales.

Crear una cultura de ciberseguridad

En este terreno también es clave unir esfuerzos. Es importante considerar todos y cada uno de los miembros de su organización como integrantes de su equipo de ciberseguridad. ¿Qué puede hacer?

- Invertir en formación en ciberseguridad para los empleados
- Concienciar a los nuevos empleados nada más incorporarse a la empresa
- Animar a las personas con más responsabilidad a aplicar las políticas de ciberseguridad
- Informarse e informar siempre sobre las nuevas ciberamenazas nada más detectarlas
- Priorizar la ciberseguridad como requisito indispensable al invertir en nuevos equipos de red
- Apostar por una política de uso de dispositivos propios (BYOD)
- Diseñar y aplicar una estrategia de respuesta a incidentes de ciberseguridad

Si consigue que toda su organización reme en la misma dirección en sus esfuerzos de ciberseguridad, lo tendrá todo a favor para garantizar la seguridad de su red y sus dispositivos.

Seguir leyendo >

Una responsabilidad compartida

La ciberseguridad implica los productos, las personas, la tecnología y los procesos. Y una cosa está clara: debemos sumar fuerzas para asegurarnos de que cada eslabón de la cadena de seguridad sea lo más fuerte posible. La ciberseguridad es una responsabilidad compartida en que todos los agentes indicados a continuación tienen que poner de su parte, incluidos los usuarios finales.

Integradores e instaladores

Su responsabilidad es comprobar que todos los equipos instalados dispongan de las últimas actualizaciones y cuenten con un antivirus avanzado. También debe colaborar con los diferentes actores implicados para garantizar que se aplica una estrategia sólida en materia de contraseñas, acceso remoto y mantenimiento del software y los dispositivos conectados.

Distribuidores

Para los distribuidores que no manipulan directamente los productos que comercializan, la ciberseguridad no presenta excesivas complicaciones. Los distribuidores con valor añadido, en cambio, deben tener en cuenta los mismos aspectos que integradores e instaladores, especialmente si compran equipos a un fabricante y lo distribuyen con la etiqueta de otra marca (o la suya propia). La transparencia es fundamental. El origen del equipo debe estar claro.

Consultores

Los consultores ayudan a definir los requisitos de los sistemas y también el mantenimiento a lo largo del ciclo de vida, explicando siempre los posibles costes asociados de una forma transparente. En el caso de los equipos OEM/ODM, las responsabilidades en materia de ciberseguridad no siempre están claras, por lo que este aspecto debe tenerse en cuenta también en toda conversación en torno a ciberseguridad.

Fabricantes de dispositivos

La ciberseguridad empieza aquí. Los fabricantes deben aplicar las prácticas de seguridad recomendadas en las fases de diseño, desarrollo y pruebas, con el objetivo de minimizar el riesgo de errores. La integración de funciones de seguridad, el desarrollo interno de los chips y un control estricto de su propia cadena de suministro son también aspectos importantes. Tan importantes como proporcionar herramientas para una gestión de dispositivos asequible y automatizada o compartir con distribuidores y socios información sobre vulnerabilidades conocidas.

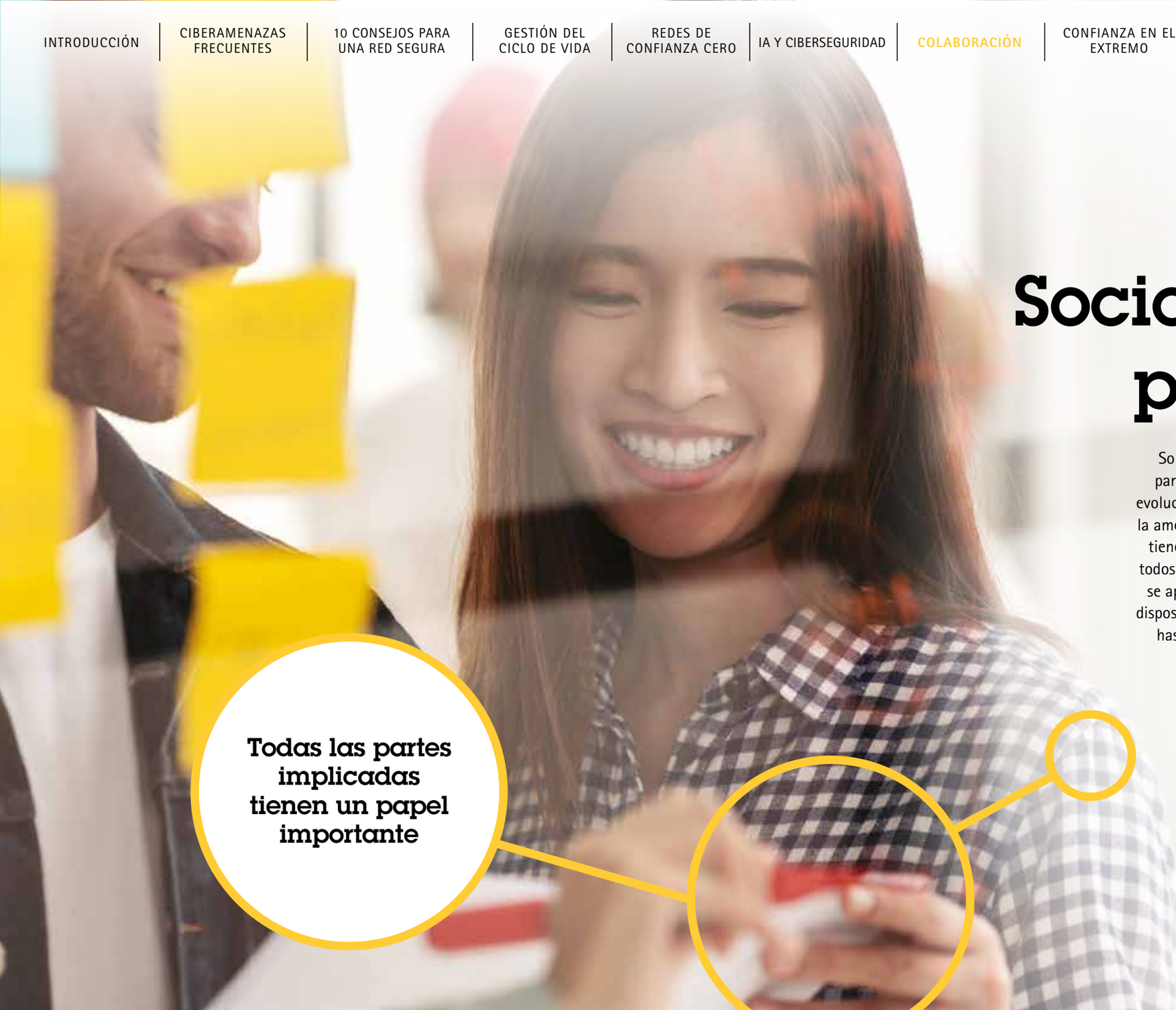
Investigadores

A menudo descubren vulnerabilidades en dispositivos. Si la vulnerabilidad no es buscada, los investigadores normalmente informan al fabricante y le dan la posibilidad de corregirla antes de publicarla. En cambio, si una vulnerabilidad crítica es buscada, suelen optar por dar difusión pública al problema para que los usuarios conozcan la situación.

Usuarios finales

Cada organización tiene unas necesidades concretas en materia de ciberseguridad, por lo que no hay una solución universal en este terreno. Sin embargo, es importante contar con una serie de políticas para proteger la información con el objetivo de definir el nivel de seguridad necesario. Algunas consignas útiles en la mayoría de casos son eliminar las cuentas por defecto, definir contraseñas seguras y no repetidas, guardarlas en un lugar seguro y cambiarlas periódicamente, asignar privilegios diferenciados e instalar siempre los parches y las actualizaciones.

Seguir leyendo >



Socios para la protección

Solo uniendo esfuerzos conseguiremos prepararnos para hacer frente a unas amenazas que no dejan de evolucionar y también para reaccionar con celeridad si la amenaza se materializa. Todas las partes implicadas tienen un papel clave a la hora de asegurarse de que todos los aspectos de las soluciones de ciberseguridad se aplican correctamente, desde la fabricación de los dispositivos o el diseño y la instalación de los sistemas hasta el mantenimiento y la gestión de los equipos. Esta es la receta para ir un paso por delante.

Todas las partes implicadas tienen un papel importante

La ciberseguridad impulsa un cambio de paradigma

El mundo en el extremo

En estos primeros meses de 2021, estamos viendo como gana terreno rápidamente el procesamiento en local, esto es, en el extremo de la red. El hecho de que miles de millones de los llamados dispositivos **IoT** estén ya conectados a la red y que esta cifra **suba rápidamente** no es una novedad. Sin embargo, la naturaleza y las necesidades de estos dispositivos sí tienen algunas implicaciones importantes para la ciberseguridad.

IoT

IoT (internet of things) hace referencia a una red de dispositivos que están conectados a internet y pueden "comunicarse" entre sí. Forman parte de esta categoría desde dispositivos tecnológicos, como smartphones y wearables, hasta dispositivos inteligentes para el hogar como contadores inteligentes y equipos industriales como máquinas inteligentes. Los dispositivos IoT utilizan sensores y procesadores para obtener y analizar datos de su entorno y generar acciones en respuesta a esta información.

Rápido crecimiento

En 2025, las previsiones apuntan a que habrá más de 75.000 millones de dispositivos IoT conectados en funcionamiento. Esta cifra prácticamente multiplica por tres la base instalada de equipos IoT de 2019.

Seguir leyendo >

El mundo en el extremo

> “Existe la tendencia a realizar en la cámara cada vez más partes del procesamiento de datos y análisis.

La idea de fondo es que muchas de las "cosas" que están conectadas a la red necesitan tener la capacidad de saber al instante qué ocurre, decidir qué hacer y tomar cartas en el asunto. En otras ocasiones, es un plus más que deseable.

Los vehículos autónomos son un claro ejemplo

En el contexto de los vehículos autónomos, las decisiones deben procesarse en décimas de segundo, tanto si tienen relación con comunicaciones con el entorno (por ejemplo, con señales de tráfico) como en el caso de sensores diseñados para detectar riesgos (por ejemplo, cuando de repente aparece un objeto delante del vehículo). La latencia entre el envío de los datos del coche a través de la red para su procesamiento y análisis en un centro de datos y la comunicación de la decisión sobre la acción recomendada es inaceptablemente larga.

La videovigilancia se encuentra en la misma situación

Si nuestro objetivo es priorizar la vigilancia proactiva frente a la reactiva (para prevenir incidentes en lugar de responder a hechos consumados), es necesario que el procesamiento de los datos y el análisis se realicen cada vez más en la cámara. Sin embargo, el aumento del número de dispositivos en el extremo de la red y su papel cada vez más importante para la seguridad tienen también sus consecuencias, que analizaremos en las próximas páginas.

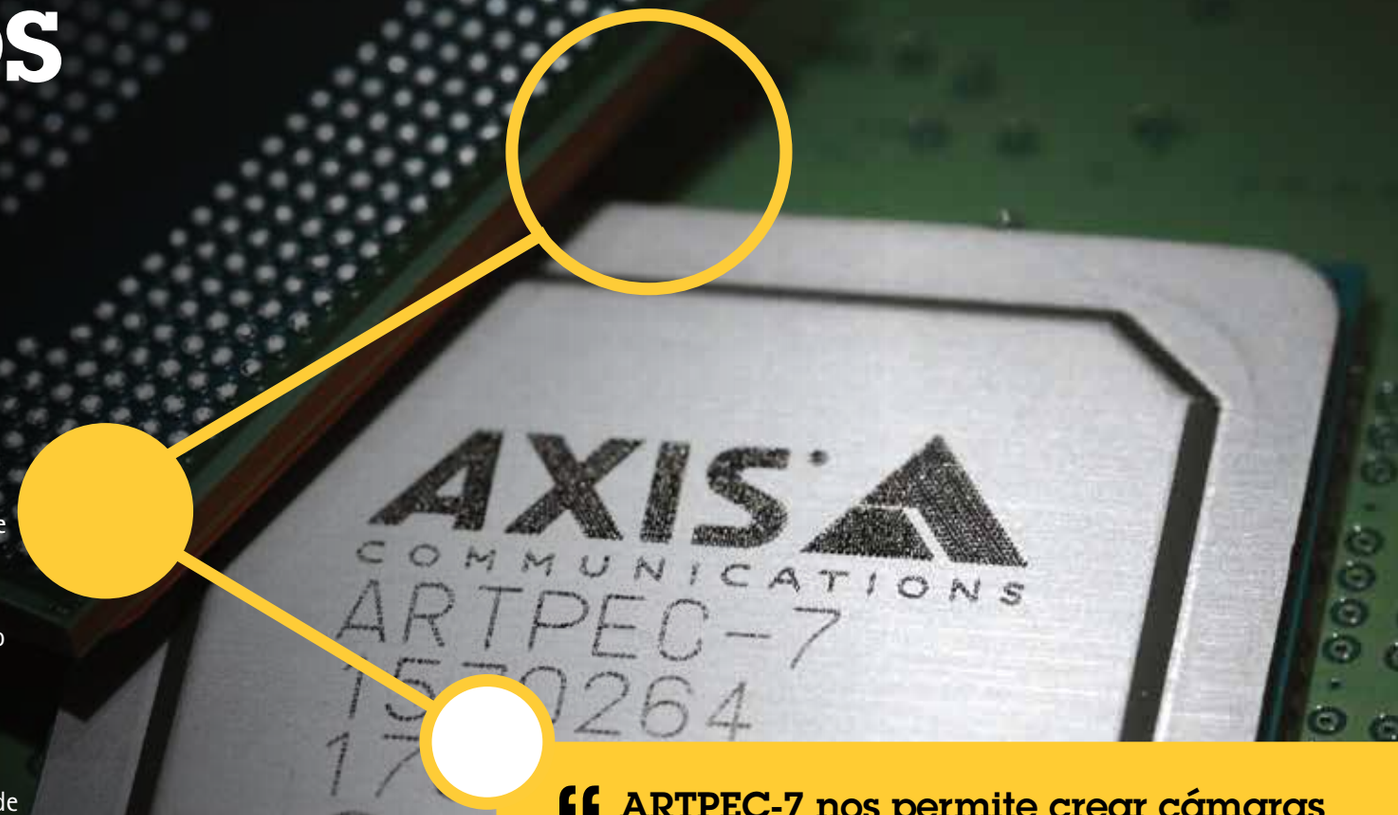
Seguir leyendo >

El poder de los dispositivos dedicados

El hardware y el software optimizado y dedicado (es decir, diseñado para una aplicación específica) son fundamentales en esta transición hacia la computación en el extremo. Los dispositivos conectados necesitarán más potencia de procesamiento y también un diseño y sistema de fabricación que tenga en cuenta la ciberseguridad desde el primer al último componente.

Esta nueva realidad explica por qué son importantes los chips de procesamiento integrados con tecnología propia. Por ejemplo, los dispositivos de Axis usan un "sistema en chip" diseñado internamente que los protege frente a los ciberataques, como actualizaciones de firmware maliciosas no autorizadas que crearían una "puerta trasera" en el sistema. En su última versión, el procesador ARTPEC-7 está diseñado específicamente para dar respuesta a las necesidades de videovigilancia de hoy y también de mañana, poniendo por delante la seguridad.

Concebido específicamente para el sector de la videovigilancia, la última versión del chip ARTPEC-7 de Axis multiplica por 50 el rendimiento del primer chip. La posibilidad de controlar el diseño y la fabricación del chip permite a Axis crear productos optimizados para las necesidades de los clientes y, a la vez, tener muy presente la evolución de factores externos, como las amenazas a la ciberseguridad.



> **"ARTPEC-7 nos permite crear cámaras de red con una calidad de imagen altísima, además de un rendimiento excepcional, una buena eficiencia del ancho de banda y la posibilidad de ejecutar analítica en el extremo.**
>
> Stefan Lundberg, Ingeniero Sénior, Axis Communications

Seguir leyendo >

La confianza llega al extremo

La confianza adopta muchas formas:

- **Confianza en que las organizaciones recopilarán y usarán nuestros datos de forma responsable**
- **Confianza en que los dispositivos y los datos están protegidos de la acción de los ciberdelincuentes**
- **Confianza en que los datos son exactos y la tecnología funcionará según lo previsto**

El extremo será el punto en que se creará o destruirá esta confianza.

La confianza en toda la cadena de suministro será vital. Aunque la integración de chips espía en el hardware es una posibilidad bastante remota, sería relativamente sencillo instalar una "puerta trasera" espía en un dispositivo mediante una actualización de firmware en el lugar de fabricación.

Seguir leyendo >

La confianza llega al extremo

Los temas relacionados con la privacidad personal seguirán en el centro del debate en todo el mundo. Aunque pueden usarse tecnologías como la anonimización dinámica y las máscaras para proteger la privacidad en el extremo, las actitudes y las regulaciones varían según el país y la región. A las empresas del sector de la vigilancia no les quedará otra que estar pendiente de los diferentes marcos legales internacionales, como hasta ahora.

La ciberseguridad es más crítica que nunca

El procesamiento y el análisis de los datos en el propio dispositivo es una tendencia creciente y, en este contexto, la ciberseguridad es todavía más importante. Sin embargo, son muchas las organizaciones que siguen sin instalar siquiera las actualizaciones de firmware más básicas, pese al constante aumento de unos ciberataques cada vez más sofisticados. La seguridad del sistema pasa por el control de cada dispositivo concreto y también por una gestión exhaustiva del ciclo de vida de toda la solución de vigilancia, mediante unas políticas claras sobre el hardware, el software y los usuarios.

La amenaza del incumplimiento

En los últimos años, compañías como British Airways y Marriott International han recibido cuantiosas sanciones por el incumplimiento de normativas. La amenaza de sanciones ha sacudido el panorama empresarial y ha tenido una traducción directa en los presupuestos destinados a la ciberseguridad.

Además, las organizaciones tienen que hacer frente a otros ataques cuidadosamente estudiados, como ransomware, malware y phishing. Las consecuencias pueden ser la caída del sistema, la pérdida de datos, la interrupción de la actividad, la publicidad negativa, la pérdida de clientes y la disminución de los ingresos.

¿Qué es el cumplimiento?

A menudo pensamos que el cumplimiento hace referencia a las normativas gubernamentales y las normas internacionales. Sin embargo, esta es solo una parte de la historia. Las organizaciones deben implementar y aplicar también controles internos y prácticas recomendadas, además de asegurarse de que sus socios cumplen también con estos estándares.

Las organizaciones ahora tienen la responsabilidad de proteger correctamente los datos de sus clientes.

Son tres las áreas que debemos tener en cuenta:

1. **Cumplimiento normativo**
   Regulaciones gubernamentales como el RGPD y normas y marcos internacionales como ISO o NIST
2. **Cumplimiento interno**
   Políticas internas de la compañía y prácticas recomendadas
3. **Cumplimiento externo**
   Cumplimiento en la cadena de suministro

Seguir leyendo >

Nuestra obligación de cumplir la ley

Las leyes de protección de datos, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, están pensadas para controlar cómo se utiliza la información personal de los consumidores en las organizaciones, las empresas y las administraciones. Y si nos fijamos en lo que afecta a la ciberseguridad, estas leyes a menudo están estrechamente relacionadas con las soluciones de seguridad que tienen las empresas.

Aunque el RGPD es una ley europea, tiene implicaciones para la mayoría de las organizaciones internacionales de un modo u otro. Por ejemplo, las compañías estadounidenses que almacenan datos en la UE deben cumplir con el RGPD. Asimismo, si una organización tiene un contrato con un tercero que usa el tratamiento de datos, ambas partes deben cumplir con el RGPD. En Estados Unidos, cada uno de los 50 estados tiene sus propios reglamentos de protección de datos, lo que dificulta el trabajo para las organizaciones con relaciones con distintos estados.

La gobernanza interna es más cara

Los hackers no hackean normas: analizan una empresa, determinan sus vulnerabilidades concretas y deciden por dónde pueden entrar. Las organizaciones podrían destinar todo su presupuesto a ciberseguridad. Sin embargo, el objetivo debe ser garantizar un nivel de protección suficiente pero sin poner trabas a la innovación. Es una cuestión de equilibrio y depende del riesgo que quiera asumir la organización. Algunas organizaciones implementan controles todavía más estrictos de lo que exige la ley, porque si hay un incidente de ciberseguridad tienen que demostrar que tomaron las medidas correctas para proteger el negocio.

Cumplimiento en la cadena de suministro

Las organizaciones con cadenas de suministro complejas tienen también otros requisitos de cumplimiento. Por ejemplo, las organizaciones con sede en Europa que hacen negocios con el gobierno estadounidense tienen que cumplir normas como la Cybersecurity Maturity Model Certification, que obliga a obtener un certificado de auditoría basado en la gestión interna de los procedimientos de ciberseguridad. En el peor de los casos, terceros (como los proveedores) pueden ser considerados corresponsables del incumplimiento y, por lo tanto, tener que asumir un porcentaje de las sanciones impuestas.

Aunque las obligaciones externas son importantes, la recomendación es que las políticas internas de la organización vayan un paso más allá. Porque, al fin y al cabo, es su responsabilidad garantizar el cumplimiento y garantizar la protección de los datos frente a cualquier tipo de ataque.

Seguir leyendo >

¿Qué regulaciones le afectan?

Controlar el cumplimiento en una organización es un trabajo constante. Las regulaciones sobre ciberseguridad y gestión de datos que afectan a cada organización normalmente dependen del sector al que pertenezca. Sin embargo, hay algunas aplicables en varios sectores y países.

Las organizaciones tienen que estar siempre al día de las nuevas pautas y los cambios que puedan introducirse en la legislación. Si están atentas a las amenazas y ataques actuales y saben qué leyes y regulaciones tienen que cumplir, les resultará más fácil decidir qué modificaciones tienen que realizar para superar los nuevos controles de cumplimiento.

Auditorías de ciberseguridad

Cuando haya identificado qué regulaciones debe cumplir su organización, será el momento de averiguar su nivel de cumplimiento global. Con una auditoría de ciberseguridad interna, podrá evaluar sus procesos de gobernanza de seguridad de TI. En general, las organizaciones tienen que someterse a una auditoría de ciberseguridad cada año. Sin embargo, la recomendación es implantar unos controles continuos para poder actuar rápidamente si hay alguna deficiencia. Además, es importante documentar periódicamente esta evaluación continua de los controles de seguridad, ya que puede resultar útil para futuras auditorías.

Qué debe tener en cuenta durante una auditoría de seguridad:

- **Gestión del riesgo:** ¿Qué proceso utiliza su organización para identificar y gestionar riesgos asociados al cumplimiento normativo? Por ejemplo, ¿cómo se comunican los riesgos y qué procesos se utilizan para garantizar que son analizados?
- **Proceso de auditoría interno:** las organizaciones tienen que establecer un proceso de auditoría interno para un control continuo del cumplimiento. Por ejemplo, ¿qué procesos utiliza para identificar, evaluar y controlar los cambios realizados en las prácticas sobre ciberseguridad?
- **Formación en seguridad y privacidad:** ¿Sus empleados tienen la formación necesaria para identificar deficiencias en las necesidades de seguridad de TI? Por ejemplo, ¿dispone de un programa de formación para gestionar el phishing a través del correo? Contar con un programa de formación es solo una parte del trabajo. Los controles internos determinarán si es efectivo. Si un área está considerada de alto riesgo en una organización, puede ser interesante realizar controles trimestrales en lugar de anuales.

Seguir leyendo >

Supervisión del cumplimiento

El resultado de una auditoría interna puede utilizarse para crear un plan de supervisión del cumplimiento. Este plan puede servir luego para analizar de forma continua el conjunto de esfuerzos de la organización en este campo y abordar todos los riesgos identificados durante la auditoría. Hay que priorizar los riesgos que representan una amenaza más grande para la organización. Mediante la evaluación de los controles de cumplimiento implementados, podrá identificar cualquier deficiencia en sus controles de ciberseguridad.

Al decidir qué personas tendrán la responsabilidad de supervisar los riesgos de ciberseguridad, hay que analizar los conocimientos necesarios para desempeñar esta función. Si quiere agilizar el proceso de selección, pregúntese qué empleados tienen las habilidades imprescindibles y qué actividades de supervisión de riesgos pueden combinarse.

¿Está al día?

Los fabricantes suelen publicar periódicamente actualizaciones de firmware para corregir vulnerabilidades y siempre que aparecen nuevas legislaciones. Sin embargo, es importante tener una visión clara de todos los dispositivos y el estado de su ciclo de vida para estar siempre a punto cuando el fabricante deja de ofrecer actualizaciones para un producto. Herramientas de gestión de dispositivos como AXIS Device Manager son útiles para controlar si los productos están actualizados y cumplen las regulaciones vigentes. Estas herramientas envían notificaciones sobre la renovación de la suscripción para licencias, cuándo llega el momento de realizar mantenimiento o autorizaciones para garantizar que las organizaciones cumplen los requisitos normativos y están al día. Además, si es necesario para las auditorías, estas herramientas también pueden proporcionar la documentación necesaria.

Demuestre qué está haciendo las cosas bien

Los clientes piden a menudo a los fabricantes de dispositivos que respondan encuestas sobre su nivel de ciberseguridad. Las organizaciones deben responder preguntas sobre sus planes de continuidad, cómo implementarán las certificaciones y cómo protegen los datos de la red. Con toda esta información disponible para compartirla, los clientes están más tranquilos porque saben que la organización cumple con todo lo establecido.

> **“ El coste de los incumplimientos es enorme. Si piensa que cumplir es caro, pruebe con no cumplir.**
>
> **Paul McNulty, ex Fiscal General adjunto**
> **https://youattest.com/**

Seguir leyendo >

Documentar, documentar, documentar

La documentación es crucial para poder demostrar el cumplimiento de las normativas. Sus políticas pueden incluir explicaciones como:

- ¿Qué graba y por qué?
- ¿Utiliza carteles para informar al público del uso de tecnologías de supervisión?
- ¿Sus soluciones de vigilancia muestran personas? Si es así, afecta a su privacidad y es necesario tenerlo en cuenta y documentarlo. ¿Quién tiene acceso a las grabaciones?
- ¿Cómo se almacenan los datos y durante cuánto tiempo? ¿El almacenamiento de los datos es seguro físicamente y desde el punto de vista de la ciberseguridad? ¿Cómo controla que se eliminan las grabaciones antiguas?

Debe contar también con documentación sobre escenarios concretos. Por ejemplo, si detecta la presencia de un intruso, ¿cómo debe gestionarse la situación? ¿Quién será el responsable de controlar los datos y qué procesos están previstos? Además, se recomienda informar a los consejos reguladores de cualquier fallo identificado durante las auditorías internas, así como de las iniciativas impulsadas por la organización para subsanarlos.

Los objetivos de cumplimiento cambian constantemente

Las leyes y regulaciones evolucionan con frecuencia y es importante ser consciente de que ni siquiera los planes de supervisión del cumplimiento más estrictos son un antídoto infalible frente a las sanciones. Las organizaciones deben revisar sus niveles de cumplimiento continuamente y ser capaces de demostrar que actúan según lo estipulado.

Ahora es el momento de actuar

No hay duda de que el cumplimiento es un componente clave de la ciberseguridad y que ha llegado para quedarse. Las organizaciones y los consumidores están alerta y son conscientes de la amenaza: saben que sus sistemas y datos son vulnerables a los ataques si no actúan rápidamente. Aunque las organizaciones quieren innovar y crecer con confianza, también necesitan minimizar los riesgos planteados por los ciberdelitos. Por otro lado, los consumidores velan por la seguridad de sus datos y esperan que las organizaciones sepan cómo gestionarlos. Las regulaciones gubernamentales solo pueden cumplirse con una estrategia colaborativa entre proveedores, fabricantes y usuarios finales, en la que todos asuman su responsabilidad por la ciberseguridad. Esta es la mejor receta para minimizar el riesgo de un ataque y los consiguientes daños.

No hay duda de que el cumplimiento es un componente clave de la ciberseguridad y que ha llegado para quedarse.

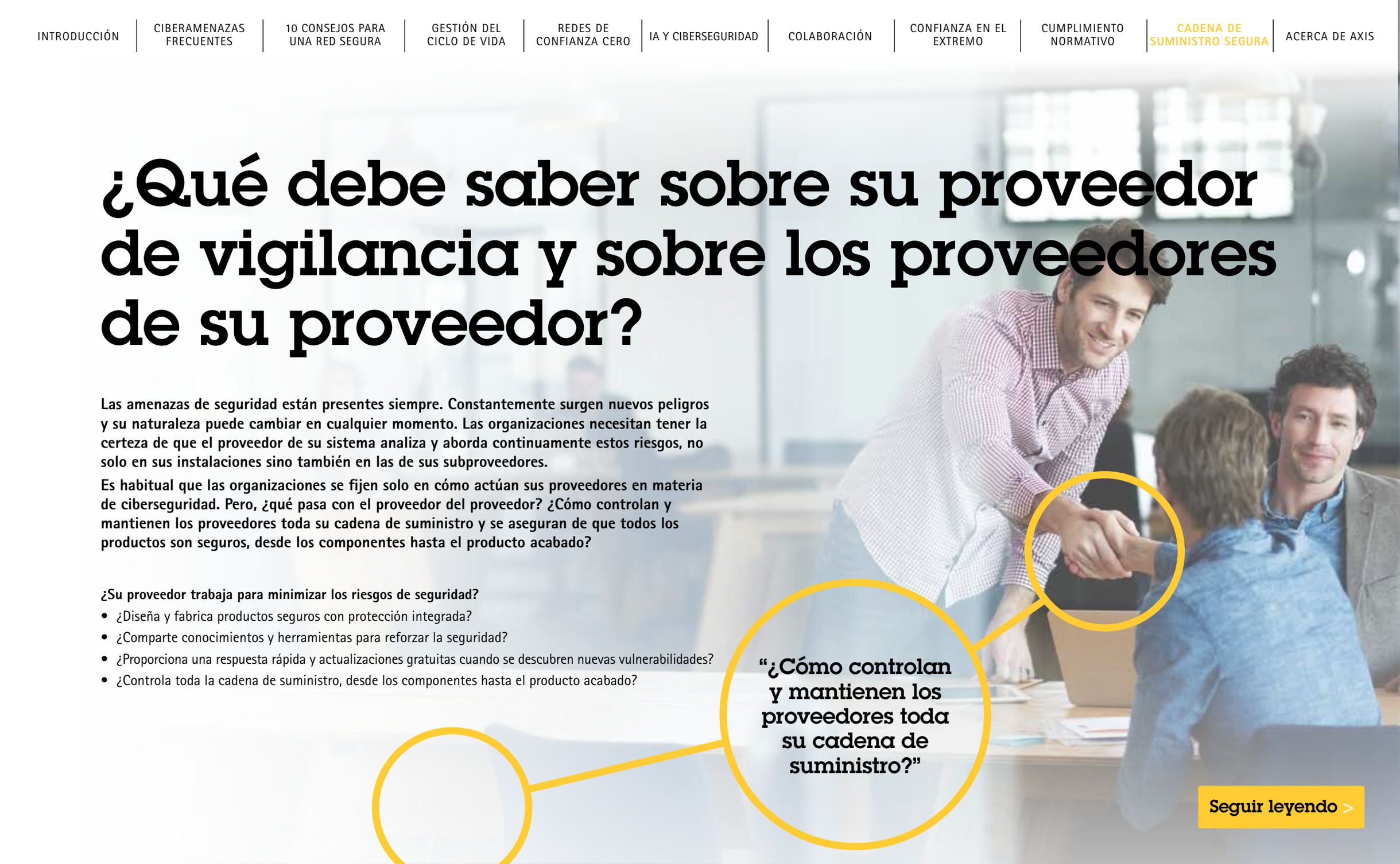
¿Qué debe saber sobre su proveedor de vigilancia y sobre los proveedores de su proveedor?

Las amenazas de seguridad están presentes siempre. Constantemente surgen nuevos peligros y su naturaleza puede cambiar en cualquier momento. Las organizaciones necesitan tener la certeza de que el proveedor de su sistema analiza y aborda continuamente estos riesgos, no solo en sus instalaciones sino también en las de sus subproveedores.

Es habitual que las organizaciones se fijen solo en cómo actúan sus proveedores en materia de ciberseguridad. Pero, ¿qué pasa con el proveedor del proveedor? ¿Cómo controlan y mantienen los proveedores toda su cadena de suministro y se aseguran de que todos los productos son seguros, desde los componentes hasta el producto acabado?

¿Su proveedor trabaja para minimizar los riesgos de seguridad?

- ¿Diseña y fabrica productos seguros con protección integrada?
- ¿Comparte conocimientos y herramientas para reforzar la seguridad?
- ¿Proporciona una respuesta rápida y actualizaciones gratuitas cuando se descubren nuevas vulnerabilidades?
- ¿Controla toda la cadena de suministro, desde los componentes hasta el producto acabado?



“¿Cómo controlan y mantienen los proveedores toda su cadena de suministro?”

Seguir leyendo >

La importancia de elegir el socio correcto

La seguridad de la cadena de suministro empieza con la elección de los socios correctos a través de un riguroso proceso de evaluación. Este proceso debe incluir un análisis del proceso de gestión de la sostenibilidad y la calidad de cada empresa. El requisito mínimo debería ser una certificación externa conforme con las normas ISO 9001 o IATF 16949.

Evaluación de los subproveedores

Su proveedor debe evaluar también los procesos de sus subproveedores en materia de gestión de riesgos, así como sus instalaciones y procesos de producción. Es necesario realizar visitas sobre el terreno y también auditorías presenciales para comprobar si la empresa cumple los requisitos y los estándares exigidos para la autorización de proveedores. En el marco de la evaluación de un nuevo socio potencial, los proveedores deben llevar a cabo un análisis exhaustivo de la situación financiera de la organización y de su estructura de propiedad.

Subproveedores estratégicos

Las relaciones con proveedores de componentes críticos y socios de fabricación suelen ser especialmente cercanas y de largo recorrido. Son subproveedores estratégicos, con los que el proveedor diseña y desarrolla proyectos conjuntos, define objetivos, y sella compromisos y planes a largo plazo. En estos casos, la colaboración y la comunicación es cercana y estrecha, con visitas frecuentes sobre el terreno.

Todos los componentes críticos de los productos de su proveedores deben ser entregados directamente por los subproveedores y almacenados internamente. Los componentes no críticos pueden llegar a través de socios de producción, pero solo procedentes de proveedores que figuren en la lista de proveedores autorizados.

¿Es segura la producción de su proveedor?

- ¿Los procesos de fabricación están definidos y son objeto de supervisión?
- ¿Desarrolla y produce equipos de producción críticos?
- ¿Su proveedor ofrece un sistema para probar los componentes, módulos y productos durante la producción, junto con software, equipos de prueba y demás infraestructura de hardware de TI?
- ¿Su proveedor recopila datos de producción las 24 horas y los 7 días de la semana para poder realizar un análisis en tiempo real, evaluar posibles riesgos de seguridad y aplicar planes de contingencia?

Seguir leyendo >

Auditorías a proveedores

Lo mejor que puede hacer su proveedor para garantizar que sus subproveedores cumplen con los requisitos especificados es realizar auditorías sobre el terreno de forma periódica, cada año o cada dos años.

Las auditorías deben abarcar diferentes aspectos de gran importancia:

- Conformidad y documentación de los procesos
- Seguridad de las instalaciones
- Manipulación física en las plantas
- Gestión de inventario
- Maquinaria de producción
- Control de calidad
- Registros de trazabilidad

Las revisiones trimestrales también resultan útiles para comprobar que los resultados se ajustan a las expectativas. En el caso de subproveedores estratégicos, recomendamos que la revisión se pilote desde el nivel de dirección superior.

Seguridad física

Todos los actores de la cadena de suministro, desde el proveedor de los componentes hasta el centro de distribución, deben cumplir con unos estrictos requisitos para garantizar la seguridad de las instalaciones:

- Las entradas y salidas deben contar con vigilancia y controles de acceso permanentes, y los registros de visitantes deben documentarse y almacenarse. Algunos puntos pueden requerir una vigilancia continua, tal vez incluso con vigilantes, para proteger el recinto y su perímetro.
- Es necesario utilizar escáneres para detectar objetos o materiales no deseados.
- El transporte debe dejarse en manos únicamente de expedidores reconocidos y de contrastada solvencia, que apliquen estrictos controles y criterios de seguridad. Los conductores y los camiones deben cumplir con las normativas de seguridad en las recogidas y las entregas.
- Todos los cargamentos realizados por transporte aéreo deben someterse a un escáner de rayos X. También es habitual sellar los cargamentos en origen, para evitar posibles intrusiones no detectadas.
- Los productos recibidos y enviados a menudo se vigilan y documentan utilizando cámaras CCTV.

Seguir leyendo >

Transferencia de datos y seguridad de la información

La transferencia de datos en la red de la cadena de suministro debe estar protegida mediante protocolos de seguridad, aplicando métodos de cifrado y autenticación. Los subproveedores y los socios deben garantizar un elevado nivel de seguridad de la información para atajar cualquier riesgo de fugas en la cadena de suministro.

Su proveedor debe contar con un sistema definido para identificar y gestionar la información confidencial de la empresa. Este sistema debe abarcar las personas, los procesos, los sistemas de TI y los espacios físicos, y debe cumplir con la norma ISO 27001 y el Reglamento General de Protección de Datos (RGPD) de la UE. De este modo conseguirá reforzar la concienciación en esta materia y gestionar los riesgos de una forma eficaz.

Seguridad del personal

Saber a quién contratamos es fundamental, no solo desde la perspectiva del currículo, las competencias o la experiencia laboral, sino también desde la óptica de la seguridad. Por ejemplo, para Axis la calidad y la seguridad en el proceso de selección de personal son innegociables y, por este motivo, apuesta por verificar las identidades, solicitar referencias y realizar comprobaciones de antecedentes antes de cualquier contratación. Los nuevos empleados y consultores deben firmar un contrato de confidencialidad para proteger la propiedad intelectual y otra información confidencial, tanto durante la relación laboral como cuando finaliza su vinculación con la empresa.

Más herramientas para sus empleados,menos riesgos para su empresa

Desde Axis queremos asegurarnos de que los empleados están siempre al día en todo lo relacionado con la seguridad de la información. Creemos que unos empleados preparados dispondrán de la información necesaria para saber qué hacer en cada momento y conocer los riesgos de cada situación. Cada empleado de Axis aporta su granito de arena a nuestro compromiso con la seguridad y la transparencia, por lo que todos reciben formación e indicaciones en materia de seguridad de la información.
Y todos tienen claro que deben extremar las precauciones y mantenerse alerta. El acceso a la información, los sistemas y los recursos está restringido y solo se concede a los empleados que realmente lo necesitan para realizar su trabajo. De forma similar, los trabajadores de nuestros proveedores y socios de producción comparten información, sistemas y recursos con Axis.

Seguir leyendo >

Integridad de los productos

Al igual que cualquier otro producto, los productos de vigilancia deben funcionar de la forma prevista inicialmente en el diseño y garantizar su integridad. Y, para alcanzar este objetivo, el hardware y el firmware del producto deben estar protegidos frente a modificaciones no autorizadas o manipulaciones a lo largo del recorrido del producto por la cadena de suministro.

Controles de calidad

Junto con nuestros proveedores y socios en la cadena de producción, Axis aplica diferentes controles de calidad para proteger la integridad de nuestros productos. Los componentes siempre se obtienen de un proveedor de nuestra lista de proveedores autorizados, según la lista de materiales de la especificación de Axis. El proveedor no puede modificar la especificación, las instrucciones de trabajo ni los documentos de inspección de calidad sin la autorización de Axis. Todos los cambios aprobados deben documentarse y registrarse.

Trazabilidad

Todos los procesos de manipulación de materiales permiten conocer en todo momento el estado de los materiales y cualquier posible desviación susceptible de perjudicar la calidad. Los proveedores y los socios de producción deben disponer de un sistema de trazabilidad para poder realizar el seguimiento de los lotes producidos, desde la recepción del material hasta el componente terminado. Durante la producción, el componente físico se somete a numerosas pruebas para verificar la conformidad y detectar posibles desviaciones.

Detección de componentes falsificados

Una inspección óptica automática (AOI) ayuda a verificar que no se instala ningún componente falsificado. En Axis, desarrollamos y producimos nuestros equipos de producción más importantes, así como el sistema para comprobar los componentes, módulos y productos en las diferentes fases de producción. Este proceso minimiza el riesgo de manipulaciones. Y para reforzar todavía más la seguridad, todos los datos de las pruebas se comparten con Axis de forma permanente, lo que permite identificar al instante cualquier modificación no autorizada.

¿Por qué Axis?

Soluciones para un mundo más inteligente y seguro

Calidad en todo lo que hacemos: todos nuestros productos se someten a exhaustivas pruebas para brindar a nuestros clientes la máxima tranquilidad.

Tecnologías innovadoras: combinamos la tecnología y la imaginación humana para mejorar el rendimiento y la usabilidad de productos basados en estándares abiertos, flexibles, escalables y fáciles de integrar.

Sostenibilidad en todos los niveles: Axis mantiene desde siempre un firme compromiso con un desarrollo respetuoso con el medio ambiente y con el uso de materiales sostenibles. En esta línea, el 80% de las cámaras y codificadores Axis no contienen PVC.

Líderes en ciberseguridad: supervisamos de forma continua las amenazas y sus consecuencias, y adoptamos medidas de forma rápida y decidida. Incluso después de la instalación, seguimos reforzando la ciberseguridad de los dispositivos con mejoras, actualizaciones y nuevas instalaciones.

Presencia global con una visión local: Axis cuenta con la mayor base instalada del mundo de productos de vídeo en red y cuenta con empleados en más de 50 países. Compartimos información y experiencias y estamos siempre en la vanguardia del sector.

El poder de la colaboración: nuestra apuesta por la colaboración nos ha convertido en la marca de cámaras con un mayor nivel de integración del mercado.

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones en red que mejoran la seguridad y suponen una nueva manera de hacer negocios. Como líder de la industria del vídeo en red, Axis pone a su disposición productos y servicios de videovigilancia y analítica, control de accesos y sistemas de audio e intercomunicación. Axis cuenta con más de 3.800 empleados especializados en más de 50 países, y proporciona soluciones a sus clientes en colaboración con empresas asociadas de todo el mundo. Fue fundada en 1984 y su sede central se encuentra en Lund, Suecia.

Para más información sobre Axis, visite nuestro sitio web www.axis.com.