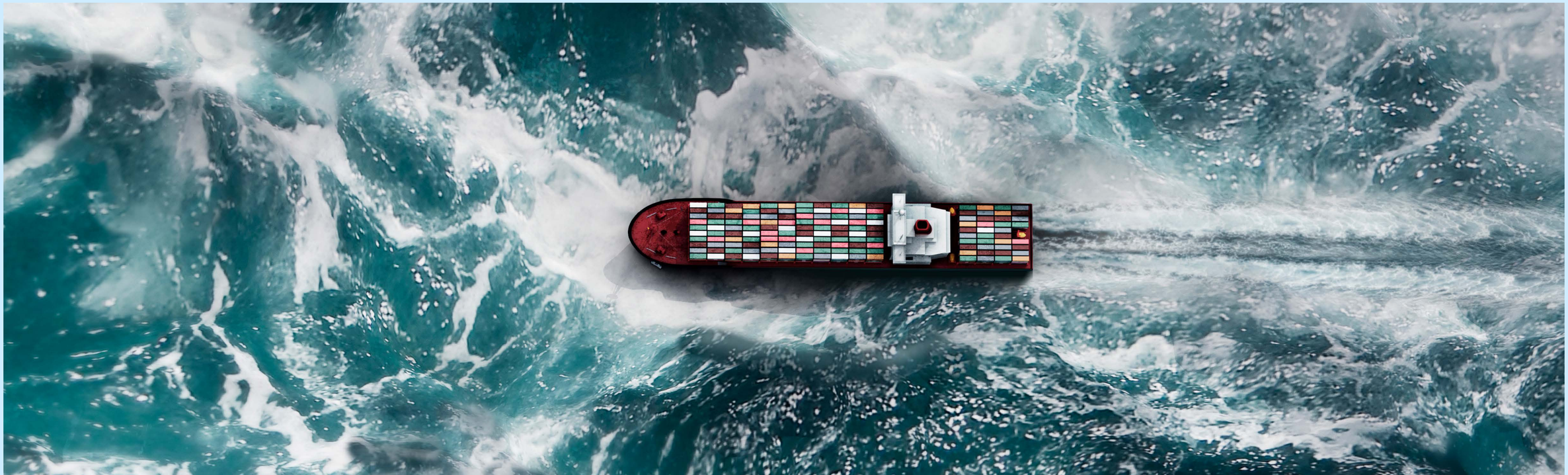
MARSH

Abril
2026

12 Controles de Ciberseguridad

Ciberresiliencia



Contenido

1. Multifactor de Autenticación (MFA) para el acceso remoto y el acceso privilegiado o de administrador 5
2. Filtrado de correo electrónico y seguridad web 7
3. Copias de seguridad cifradas y comprobadas 9
4. Gestión de accesos privilegiados (PAM) 12
5. Detección y respuesta de endpoints (EDR) 14
6. Gestión de parches y vulnerabilidades 17
7. Planes de respuesta a incidentes 19
8. Formación en materia de ciberseguridad y pruebas de phishingtesting 22
9. Mitigación del protocolo de escritorio remoto (RDP) y otras técnicas de bastionado 24
10. Accesos y monitorización 26
11. Sustitución o protección de los sistemas obsoletos 28
12. Gestión de riesgos cibernéticos en la cadena de suministro digital 30

A partir de aquí 32

Más información 33

Ciberresiliencia: 12 controles clave para reforzar su seguridad

Los ciberataques siguen dominando los titulares de las noticias. Los autores de estos ataques ahora exigen pagos de rescates multimillonarios, ya que paralizan las operaciones de una empresa, llevándolas a un punto muerto hasta que se realice un pago.

Una vez superada la etapa de endurecimiento del mercado —impulsada, entre otros factores, por el aumento descontrolado de la siniestralidad, especialmente en relación con los eventos de ransomware de 2021 y 2022—, las aseguradoras han entendido mejor los aspectos a los que deben prestar especial atención en sus procesos de suscripción y han desarrollado una visión mucho más estratégica y precisa de los riesgos cibernéticos, identificando una correlación entre ciertos controles de ciberseguridad y los correspondientes incidentes de ciberseguridad y/o privacidad.

A través de este análisis y del examen continuo de la tipología de incidentes sufridos, el sector asegurador ha desarrollado una comprensión más detallada de los pasos técnicos que las organizaciones pueden tomar para reforzar su posición en ciberseguridad y resiliencia tecnológica. Como resultado, la adopción de determinados controles se ha convertido en un requisito mínimo por parte de las aseguradoras, con la asegurabilidad de las organizaciones en juego y la posibilidad de acceder a mejores condiciones y coberturas más favorables para el cliente.

En este contexto, el enfoque de Marsh en los 12 controles de ciberseguridad recomendados se convierte en un análisis clave dentro de la forma en que apoyamos a nuestros clientes incluyendo la la contratación del seguro Cyber. Su objetivo es ofrecer una visión estructurada y basada en datos del nivel de exposición cibernética de la organización, permitiendo evaluar su grado de madurez en los principales ámbitos de seguridad y traducirlo en términos de riesgo y asegurabilidad desde la perspectiva del mercado.

Las organizaciones están poniendo, más que nunca, el foco en los controles “esenciales” de ciberseguridad para ayudar a mitigar sus riesgos y mejorar su posición general de ciberseguridad y resiliencia tecnológica. Se recomienda, por ello, aplicar una serie de controles de higiene de ciberseguridad que resultan clave para lograr la resiliencia y asegurabilidad.

Aunque estos controles han sido considerados mejores prácticas durante ya varios años, algunas empresas todavía tienen dificultades para adoptarlos, en la mayoría de los casos porque no han podido justificar el coste de su implementación, no los han desplegado de forma exhaustiva o no han entendido —o no han percibido— la necesidad de aplicarlos.

En muchos sectores regulados, donde los controles de resiliencia cibernética se han exigido durante años, el esfuerzo se ha centrado con frecuencia más en cumplir un requisito formal que en mejorar realmente la seguridad.

En esta serie de artículos, Marsh presenta los 12 controles de ciberseguridad recomendados, junto con sus características y requisitos.



1. Multifactor de Autenticación (MFA) para el acceso remoto y el acceso privilegiado o de administrador

¿Qué es este control?

El Multifactor de Autenticación (MFA) es una barrera de seguridad adicional para verificar la identidad de un usuario cuando solicita acceso a un recurso informático. La MFA requiere que el usuario proporcione dos o más pruebas de las siguientes categorías para ser autenticado: "algo que sabe" (como una contraseña/PIN), "algo que tiene" (por ejemplo, un dispositivo de identificación criptográfica o token), y "algo que es" (por ejemplo, un biométrico).

¿Por qué hay que adoptar este control?

La MFA es una parte esencial de una estrategia de gestión de acceso a la identidad (IAM) sólida, que impide el acceso remoto no autorizado a los recursos informáticos.

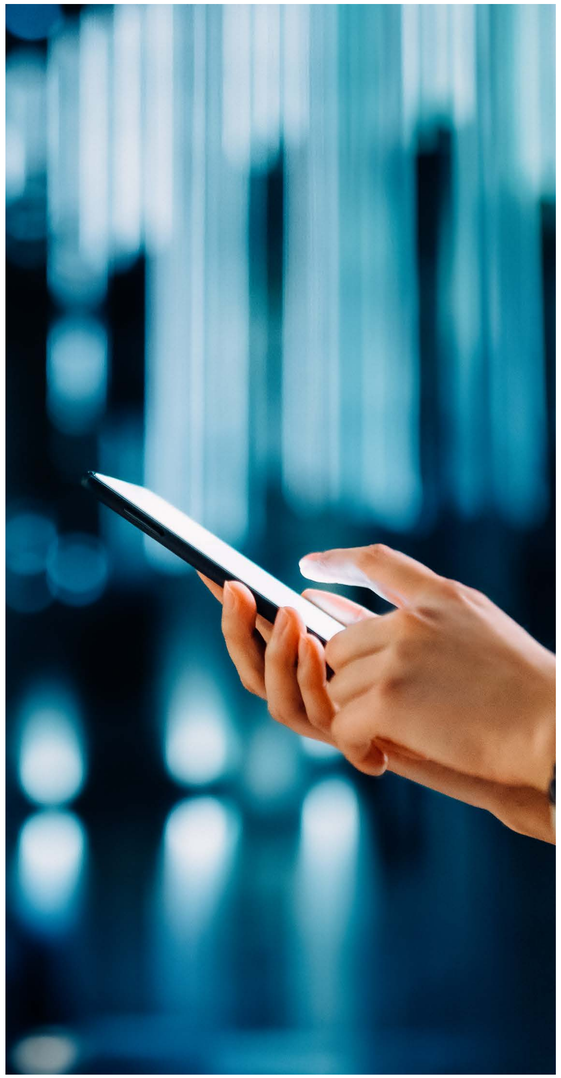
ElMFA debe estar habilitada en todos los sistemas, aplicaciones y cuentas accesibles de forma remota, para todos los accesos de usuarios de todo tipo, y para todos los accesos a datos críticos o sensibles.

En muchos casos, la correcta implementación del MFA puede ayudar a prevenir incidentes cibernéticos, como un ataque de ransomware con graves consecuencias económicas

Las aseguradoras están exigiendo a las organizaciones una mayor resiliencia cibernética, con el MFA como punto de partida clave. En última instancia, esto reforzará su seguridad y les ayudará a convertirse en mejores candidatos para la cobertura del ciberseguro.

Como mínimo, las empresas deberían buscar la aplicación de MFA en:

- Activos críticos.
- Cuentas con privilegios de administrador.
- Aplicaciones remotas.





¿Qué debe hacer una empresa para poner en marcha este control?

Para implantar este control de forma adecuada, se recomienda a las empresas:

1. Exigir el MFA para todos los inicios de sesión remotos en la red corporativa utilizando un acceso remoto seguro, como la red privada virtual (VPN) y el protocolo de escritorio remoto (RDP).

2. Exigir el multifactor de autenticación y los canales cifrados para todos los accesos a cuentas administrativas, independientemente de la ubicación del usuario.

3. Exigir MFA para el acceso a los datos o sistemas más críticos o sensibles, independientemente de la ubicación de un usuario.

4. Exigir contraseñas largas y complejas que tengan más de 14 caracteres y utilicen letras mayúsculas y minúsculas, números y símbolos.

Como base para cumplir e implementar los requisitos mencionados, se aconseja que una organización debe:

- Identificar:
  - Todos los sistemas y aplicaciones a los que se puede acceder de forma remota.
  - Los datos críticos y sensibles, así como todos los sistemas y aplicaciones en los que se almacenan.
  - Todos los usuarios con privilegios de administrador.
- Implantar la autenticación basada en el riesgo, que es un método que consiste en aplicar distintos niveles de rigor a los procesos de autenticación en función de la probabilidad de que el acceso a un determinado sistema pueda ponerlo en peligro.
- Combinar la VPN y cualquier solución remota con MFA.
- Identificar todos los dispositivos corporativos, especialmente los que aceptan biometría (como ordenadores portátiles y teléfonos móviles), para su posible uso como factor adicional.
- Comprobar la normativa local sobre protección de datos, privacidad y datos biométricos. Puede haber limitaciones en el uso de dispositivos privados, o datos biométricos, como medio para conseguir el factor adicional.
- Desplegar los factores en todos los dispositivos para evitar que un incidente los afecte a todos.
- Formar e informar a los empleados sobre el valor de las capas/barreras adicionales de seguridad antes de implementar el MFA para reducir la resistencia y evitar cualquier malentendido.

Consulte el documento NIST SP 800-63-4 para obtener más información.

2. Filtrado de correo electrónico y seguridad web

¿En qué consiste este control?

El software de filtrado de correo electrónico se utiliza para analizar el tráfico de correo electrónico entrante o saliente en abusca de contenido no deseado. Puede tratarse de correos electrónicos no deseados menos dañinos que se dirigen al destinatario en relación con acciones específicas -por ejemplo, la venta de un producto o la solicitud de donaciones- o de correos electrónicos de suplantación de identidad que representan una grave amenaza para la ciberseguridad.

Estos correos detectados se filtrarían automáticamente, para que no lleguen al usuario, o se marcarían para que el usuario se sensibilice ante el contenido potencialmente malicioso o no deseado. A través del software de seguridad del correo electrónico, los archivos adjuntos sospechosos y potencialmente maliciosos se prueban además en un entorno seguro “sandbox”.

El filtrado de contenidos web puede aplicarse mediante soluciones basadas en hardware o en software, así como el seguimiento y la regulación del acceso a sitios web en los que los usuarios no deben entrar. El motivo puede ser que el contenido esté sujeto a regulación -como suele ocurrir con el material de los sitios web de juegos de azar- o que se sospeche que es un contenido malicioso. El filtrado del sistema de nombres de dominio (DNS), por su parte, es un tipo especial de criba de contenidos que utiliza la capa DNS para regular el acceso a los sitios web en función de las direcciones IP, con el fin de filtrar el uso de la web y reducir la exposición al malware.

¿Por qué hay que adoptar este control?

Los enlaces y archivos maliciosos son la principal forma de introducir programas maliciosos en los sistemas de las organizaciones, o de robar las contraseñas de los usuarios y, finalmente, acceder a los sistemas críticos. El filtrado de la web y el correo electrónico se considera una “primera línea de defensa” para defenderse de los ciberataques relacionados con el correo electrónico o la navegación web, incluso antes de que los usuarios -la “segunda línea de defensa”- puedan ser víctimas de un ataque de phishing o entrar en sitios web con contenido malicioso. El filtrado es necesario, ya que el phishing por correo electrónico es uno de los principales vectores de ataque iniciales que conducen a incidentes cibernéticos graves, especialmente los ataques de ransomware. Los ciberdelincuentes suelen utilizar

las campañas de phishing para robar los nombres de usuario y las contraseñas de sus víctimas, lo que proporciona a los atacantes un acceso inicial al entorno informático de la víctima. Mediante la aplicación de tecnologías de seguridad del correo electrónico y de filtrado de la web, un gran porcentaje de los ciberataques potencialmente graves pueden detenerse desde el principio.

Como mínimo, las organizaciones deberían preseleccionar los correos electrónicos en busca de archivos adjuntos y enlaces potencialmente maliciosos, y utilizar herramientas para supervisar el contenido de la web y bloquear el acceso a sitios web vulnerables. Las aseguradoras también están imponiendo requisitos de ciberresiliencia a los asegurados para poder asegurarlos. La implantación de tecnología de seguridad del correo electrónico y de filtrado de la web permitirá a una organización mejorar su perfil en relación con la presentación de su ciberriesgo a los suscriptores de seguros. Estos controles son un elemento clave para poder optar a la cobertura del ciberseguro, ya que, si se aplican, las aseguradoras prevén que se reduzca el número total de incidentes cibernéticos graves y, por tanto, costosos.

¿Qué debe hacer una empresa para poner en marcha este control?

Los controles de seguridad relacionados con la protección contra el malware, la seguridad del correo electrónico y el filtrado de la web que podrían ponerse en práctica abarcan lo siguiente:

- Utilizar la tecnología para escanear y filtrar los correos electrónicos entrantes en busca de archivos adjuntos y enlaces maliciosos.
- Impedir que los archivos con macros se ejecuten por defecto.
- Evaluar los archivos adjuntos de los correos electrónicos en un entorno sandbox antes de su entrega al usuario, con el fin de determinar si los archivos son maliciosos.
- Utilizar la tecnología para supervisar el contenido de la web y bloquear el acceso a sitios o contenidos web maliciosos.



3. Copias de seguridad cifradas y comprobadas

¿En qué consiste este control?

La fiabilidad y disponibilidad de las copias de seguridad son esenciales para garantizar la resiliencia de la empresa. Las copias de seguridad deben estar protegidas, preferiblemente aislándolas de la red, o implementando el acceso controlado por multifactor de autenticación y el cifrado. También es fundamental realizar pruebas periódicas para garantizar la integridad y disponibilidad de los datos.

¿Por qué hay que adoptar este control?

A medida que las organizaciones pasan cada vez más a soluciones de copia de seguridad basadas en la nube, los atacantes buscan las credenciales de administrador para acceder a ellas, antes de borrarlas o cifrarlas. La falta de copias de seguridad disponibles aumenta la probabilidad de que la víctima pague un rescate para recuperar los sistemas y los datos, ya que no tiene otra opción.

Es fundamental realizar pruebas periódicas de las copias de seguridad: de nada sirve tener copias de seguridad si no están disponibles, o están incompletas, cuando se necesita restaurar los sistemas. Las pruebas periódicas también permiten a los equipos de TI y de ciberseguridad comprender la complejidad del proceso de restauración e identificar a los terceros que pueden ser necesarios para ayudarles. No suele ser tan sencillo como pulsar un interruptor.

Las copias de seguridad viables permiten a las organizaciones recuperarse de los ataques con mayor rapidez y eficacia. En el caso del ransomware, tener copias de seguridad reduce la ventaja que los actores de la amenaza tienen sobre la víctima y puede reducir, en gran medida, la necesidad de pagar un rescate.

Cuando los sistemas están cifrados, las empresas suelen ser incapaces de operar, por lo que sufren importantes pérdidas por interrupción del negocio. Las copias de seguridad protegidas pueden reducir el tiempo de recuperación y permitir la vuelta a la normalidad más rápidamente que negociar con los actores de la amenaza para obtener dudosas claves de descifrado. Las copias de seguridad probadas permiten a la empresa poder confiar en los datos respaldados: los errores o fallos en el proceso de copia de seguridad se detectarán y rectificarán rápidamente.

¿Qué debe hacer una empresa para poner en marcha este control?

Las organizaciones deben revisar sus sistemas y activos críticos y asegurarse de que los procedimientos de copia de seguridad son adecuados y se prueban regularmente. También es esencial asegurarse de disponer de una copia de seguridad desconectada.

Deben establecerse planes de recuperación de desastres, continuidad del negocio y respuesta a incidentes para documentar con precisión el proceso que se seguiría para recuperar los sistemas a partir de las copias de seguridad.

Existen innumerables soluciones de copia de seguridad diferentes y puede ser difícil evaluar el mejor proveedor y la mejor propuesta para una organización. Centrarse en proporcionar una solución para los sistemas, datos y activos que son realmente críticos -las “joyas de la corona” - es un buen punto de partida.




En términos de ciberseguridad,
los humanos suelen ser
el eslabón más débil.

4. Gestión de accesos privilegiados *(PAM)*

¿En qué consiste este control?

La gestión de accesos privilegiados (PAM) es una tecnología de seguridad que ofrece un nivel de acceso elevado o “privilegiado” para proteger cuentas, credenciales y operaciones. El acceso privilegiado se diferencia del acceso “normal” porque puede permitir funciones de seguridad o de mantenimiento, cambios de configuración en todo el sistema o la aplicación, y la elusión de los controles de seguridad establecidos mediante el acceso de superusuario.

¿Por qué hay que adoptar este control?

En términos de ciberseguridad, los humanos suelen ser el eslabón más débil, lo que hace que cualquier organización sea vulnerable a un ataque. Las herramientas PAM controlan el acceso privilegiado de las máquinas (sistemas o aplicaciones) para la comunicación interna o de máquina a máquina, incluso para las personas que administran o configuran los sistemas y aplicaciones.

Se basa en el principio de “mínimo privilegio”, lo que significa que los usuarios sólo reciben el nivel mínimo de acceso que necesitan para realizar sus funciones laborales. Los componentes de una solución PAM típica supervisan las sesiones utilizadas por las cuentas de administrador y generan alertas para cualquier uso anómalo de las sesiones. Las anomalías pueden incluir que una cuenta intente acceder a áreas fuera de su dominio de responsabilidad o fuera de su ventana de operaciones.

¿Qué debe hacer una empresa para poner en marcha este control?

En un principio, la organización deberá identificar el caso de uso, es decir, las acciones o pasos para los que quiere invertir en un PAM. Por ejemplo, puede adoptar un enfoque basado en el riesgo para identificar los activos críticos que están en mayor riesgo de exposición, como resultado del compromiso de las cuentas privilegiadas, y luego sólo implementar la solución para esos activos.

Una vez que la PAM está en marcha, para evitar cualquier idea errónea sobre la solución, la organización puede distribuir contenido a sus empleados acerca de sus diferentes componentes, su propósito y por qué son necesarios como parte de la combinación global de ciberseguridad. La organización

también debe establecer un programa de gobernanza y supervisión para PAM para que el rendimiento no se degrade con el tiempo. Esto debe incluir el establecimiento de criterios de selección y rendimiento para los proveedores y productos y la realización de evaluaciones de rendimiento posteriores a la implementación.

En cuanto a la escalabilidad de PAM, las hojas de ruta para el crecimiento de la empresa pueden tener en cuenta los activos adicionales relevantes que requieren este control, de modo que las licencias estén disponibles para acomodarlas cuando se implementen.



5. Detección y respuesta de endpoints (EDR)

¿En qué consiste este control?

Los EDR (Endpoint Detection and Response) por sus siglas en inglés es un mecanismo de detección y respuesta a las amenazas para un endpoint: un dispositivo remoto como un ordenador de sobremesa, un portátil, un teléfono móvil, un servidor o el Internet of Things (IoT) que se comunica con una red interna, de forma externa.

Como los endpoints son los puntos de entrada para prácticamente cualquier tipo de ataque malicioso en una red, su monitorización es vital para detectar y detener un ataque antes de que se extienda a la red interna más amplia. Una solución EDR supervisa continuamente los endpoints, recoge datos de los dispositivos y proporciona una respuesta basada en reglas definidas.

¿Por qué hay que adoptar este control?

La supervisión de los endpoints es fundamental para detectar y detener un ataque antes de que se extienda a la red interna más amplia.

Además, cuando el EDR está en funcionamiento, supervisa y registra la actividad en esos endpoints. Esos datos pueden analizarse para detectar amenazas persistentes o vulnerabilidades de “día cero” -es decir, fallos que aún no han sido parcheados- que han sido comprometidos. Si se detecta una amenaza a la seguridad, el log (registro de eventos) puede ser revisado para determinar cuándo comenzó esa amenaza, el alcance del compromiso y origen.

Por ejemplo, una organización que sea víctima de un ataque de ransomware tardará más en recuperarse si no tiene instalado el EDR. Esto se debe a que no tendrá visibilidad sobre el alcance del evento, y específicamente, sobre cuántos endpoints han sido infectados. La organización no podrá detectar si hay cargas útiles aun operando en el backend, ni si los ajustes de configuración relevantes están funcionando como se esperaba o necesitan ser revisados. Todo esto significa que el esfuerzo de recuperación llevará más tiempo y deberá ser más profundo.

¿Qué debe hacer una empresa para poner en marcha este control?

Disponer de una sólida base de buenas prácticas de ciberseguridad suele permitir a una organización implantar la EDR sin problemas.

También es vital encontrar una solución de EDR que pueda proporcionar el máximo nivel de protección y que al mismo tiempo requiera la menor cantidad de esfuerzo e inversión, añadiendo, en última instancia, valor a su equipo de seguridad sin exigir muchos recursos.Los aspectos clave que las organizaciones deben buscar en una solución son:

- Visibilidad en todos sus endpoints. Debe proporcionar visibilidad en tiempo real para que se puedan detectar las actividades sospechosas, incluso mientras intentan atacar su entorno, y detenerlas inmediatamente.

- Una solución que recoja una cantidad significativa de telemetría de los endpoints, de modo que pueda ser extraída en busca de señales de ataque con una variedad de técnicas de análisis de datos.

- Una detección y respuesta eficaz de los endpoints requiere enfoques de comportamiento que busquen indicadores de ataque (IOA), de modo que sea alertado de las actividades sospechosas antes de que pueda producirse un compromiso.

- Una solución que integre la inteligencia sobre amenazas, incluyendo detalles sobre el adversario que le está atacando u otra información sobre el ataque.

- Una respuesta rápida, las soluciones deben operar en tiempo real, proporcionar alertas precisas y automatizar la respuesta a las amenazas. Esto requiere motores de detección que produzcan un mínimo de falsos positivos y la capacidad de establecer políticas de respuesta automatizadas.

- Contar con una solución de detección y respuesta de endpoints basada en la nube `es la única manera de garantizar un impacto cero en los endpoints. Esta solución debe integrarse sin problemas con los sistemas actuales y proporcionar un acceso remoto intuitivo a los controles.



La gestión de parches y vulnerabilidades es una práctica de seguridad diseñada para prevenir, de manera proactiva, la explotación de las vulnerabilidades de TI que existen dentro de una organización.[3]

6. Gestión de parches y vulnerabilidades

¿En qué consiste este control?

La gestión de la vulnerabilidad es una capacidad que identifica las vulnerabilidades en los dispositivos de software y hardware que pueden ser utilizados por los atacantes para comprometer un dispositivo y utilizarlo como una plataforma desde la que comprometer aún más la red.

La gestión de parches es la notificación sistemática, identificación, despliegue, instalación y verificación de un sistema operativo y las aplicaciones . Estas revisiones se conocen como parches, hot fixes y service packs.

No todas las vulnerabilidades tienen parches relacionados. Por lo tanto, un proceso adecuado de gestión de vulnerabilidades considerará otros métodos de remediación, o soluciones temporales -como el cambio de configuración del software y la formación de los empleados- para limitar o aislar la exposición.

¿Por qué hay que adoptar este control?

Las organizaciones siempre tendrán un cierto nivel de riesgo debido a las vulnerabilidades en sus entornos de TI. Un riesgo puede definirse como la probabilidad de que una determinada amenaza a la seguridad explote la vulnerabilidad de un sistema.[1]

Las vulnerabilidades pueden ser explotadas por varias amenazas cibernéticas en los dispositivos de software y hardware que son utilizados frecuentemente por una organización. Por lo tanto, sin tener una visión clara y continua de las vulnerabilidades existentes, las organizaciones tendrán dificultades para identificar y responder a las amenazas de manera oportuna.

Por otra parte, cada organización tendrá una tolerancia al riesgo única basada en su salud financiera, exposición a la reputación y requisitos de cumplimiento. Establecer una relación entre la gestión adecuada de la vulnerabilidad de TI y la tolerancia al riesgo es complejo, y puede ser difícil de defender frente a una junta directiva, ya que la administración puede no entender completamente qué vulnerabilidades de TI presentan el mayor riesgo.

Una función adecuada de gestión de parches y vulnerabilidades reducirá, o eliminará, el potencial de explotación de estas vulnerabilidades e implicará mucho menos tiempo, esfuerzo y dinero que la respuesta posterior a un ataque.

1. Según el NIST SP 800-16 Sin embargo, existen múltiples definiciones de riesgo. Aunque hemos incluido la forma más sencilla de definir un riesgo, esta definición considera las características más importantes: probabilidad de ocurrencia, amenaza o evento, vulnerabilidad e impacto.

Las vulnerabilidades no parcheadas siguen siendo una de las principales causas de intrusiones en los sistemas, con cientos de vulnerabilidades reveladas cada mes para múltiples aplicaciones y sistemas.

Cuando los entornos tecnológicos no se parchean a tiempo, los atacantes tratarán de explotar las vulnerabilidades.

¿Qué debe hacer una empresa para poner en marcha este control?

Aunque la implantación de un proceso de gestión de vulnerabilidades es muy compleja, se puede resumir en cinco pasos:[2]

1. **Preparación:** Realizar un análisis de vulnerabilidad, definir el alcance de los activos, informar a las partes interesadas y a los propietarios de los activos, y planificar los escaneos de vulnerabilidad.

2. **Identificación y detección de vulnerabilidades:** Esto puede lograrse a través de un escaneo de vulnerabilidad.

3. **Definición de las acciones correctoras:** Para definir adecuadamente las acciones correctoras, debe realizarse una evaluación de riesgos informáticos. Dependiendo de la corrección (como un parche o un cambio de configuración), las restricciones del software y la disponibilidad de soluciones, pueden surgir diferentes opciones, entre ellas:

   - Mitigar - mediante la aplicación de acciones correctoras.

   - Aceptar - lanzando un proceso de excepción[3] e investigando los posibles indicadores de compromiso (IOC).

4. **Implementación de las acciones definidas:** Despliegue de las tareas identificadas en las actividades anteriores.

5. **Seguimiento de las vulnerabilidades:** Como cada minuto surgen nuevas vulnerabilidades, comprometerse a una verdadera monitorización continua es esencial para gestionarlas adecuadamente.

   La mayoría de las vulnerabilidades pueden ser remediadas mediante la aplicación de parches y la actualización de los sistemas. Los sistemas de TI con vulnerabilidades conocidas con limitaciones para instalar el parche, o sin una solución disponible, pueden ser investigados para detectar la presencia de indicadores de compromiso y, si estos sistemas se ven comprometidos, deben iniciarse planes de respuesta a incidentes y de recuperación. Además, también puede aplicarse un plan de aislamiento para los sistemas heredados. Por último, si la evaluación de riesgos de TI indica un retraso en la reparación debido a las limitaciones operativas, debe establecerse un proceso de excepción.

   También es probable que las compañías de seguros exijan las siguientes acciones:

   - Realización periódica de un análisis de vulnerabilidad.

   - Realización de pruebas de penetración -es decir, un ciberataque simulado para comprobar las vulnerabilidades explotables- al menos una vez al año.

   - Mantenimiento y actualización continuos del panorama de las tecnologías de la información y las comunicaciones (TIC).

   - Aplicación de parches con CVE[4] 8 o superior en menos de tres a siete días, tras su publicación, en los sistemas informáticos expuestos.

   - Se espera que los parches no críticos se apliquen en menos de 30 días tras su publicación.

   La frecuencia y especificaciones de estas acciones están ligados al perfil de riesgo cibernético de una organización, a la industria y al entorno de los ciberataques.

2. Estos pasos se amplían en el documento del Instituto SANS Implementación de un proceso de gestión de vulnerabilidades.

3. Proceso de excepción: una condición que no se ajusta a las expectativas formales de seguridad definidas por la política, la norma y/o el procedimiento; por ejemplo, no se aplica un parche.

4. CVE son las siglas en ingles de vulnerabilidades y exposiciones comunes. Es un programa lanzado por MITRE para identificar y catalogar las vulnerabilidades en el software o el firmware.

7. Planes de respuesta a incidentes

¿En qué consiste este control?

Los planes de respuesta a incidentes documentan un "conjunto predeterminado de instrucciones o procedimientos para detectar, responder y limitar las consecuencias de un ciberataque malicioso contra los sistemas de información de una organización ".[5] Deben estar en consonancia con otros planes y capacidades relacionados disponibles, entre ellos:

- Un plan de recuperación de desastres de TI (DRP), que describe cómo una organización recupera los datos durante y después de una crisis o desastre.

- Un plan de continuidad del negocio (BCP), que establece cómo una organización garantiza que los procesos empresariales esenciales estén disponibles durante y después de una crisis o desastre.

La respuesta a los incidentes sólo funcionará sin problemas cuando todas las partes interesadas estén familiarizadas con el plan de respuesta. Por lo tanto, la comprobación periódica de los procedimientos es una parte esencial de este control.

¿Por qué hay que adoptar este control?

Los planes de respuesta a incidentes son una parte integral del aumento de la resiliencia cibernética de una organización. Estos programas no son marcos aislados, sino que deben reflejar el perfil de riesgo específico y único de una organización y requieren la integración dentro de una estrategia general de gestión de riesgos cibernéticos.

Para mitigar el ciberriesgo, el primer enfoque y la primera línea de defensa serán siempre las medidas de prevención técnicas y organizativas. Cuando se producen ciberincidentes, es crucial detectarlos lo antes posible y responder a ellos de forma rápida y profesional.

Un plan de respuesta a incidentes actualizado y un equipo formado proporcionan eficacia, rapidez y calidad en la respuesta a los ciberincidentes. Cuando se combina con un enfoque organizativo holístico de los 12 controles clave -así como la implementación de controles técnicos apropiados y la recuperación de incidentes y desastres (como copias de seguridad seguras, cifradas y probadas)-, un programa de respuesta a incidentes ayuda significativamente a mitigar

5. Según la definición del Computer Security Resource Center.

los impactos de un evento cibernético en las operaciones y la reputación de una organización.

¿Qué debe hacer una empresa para poner en marcha este control?

Se aconseja a las organizaciones que incluyan las siguientes capacidades básicas en su enfoque de la planificación y las pruebas de respuesta a incidentes:

- El plan de respuesta a incidentes debe contener procesos y procedimientos definidos para llevar a cabo la gestión, notificación y recuperación de incidentes cibernéticos.

- Las funciones, tareas y responsabilidades de los miembros del equipo de respuesta a incidentes durante un incidente de seguridad deben estar claramente definidas. Además, es obligatorio definir claramente las vías de escalada y los procesos/responsabilidades de toma de decisiones.

- Deben planificarse y documentarse las partes de la respuesta a incidentes que se cubrirán externamente (como las investigaciones forenses de TI), y anotarse la información de contacto pertinente.

- Debido al significativo aumento de los incidentes de ransomware y su enorme potencial de pérdidas, debería definirse un manual de respuesta específico adaptado al escenario de crisis del ransomware.

- Los planes de respuesta a incidentes sólo son valiosos cuando los miembros del equipo de respuesta están familiarizados con sus funciones y responsabilidades, y cuando hay claridad en los procesos subyacentes. Debe realizarse un ejercicio de mesa anual para entrenar al equipo en escenarios específicos y para evaluar la preparación de la organización ante un incidente.

- Además, los planes deben ser revisados y actualizados periódicamente, incorporando los últimos acontecimientos, como los cambios de personal y las nuevas amenazas previstas.



Las empresas operan en un mundo en que la mayoría de los problemas de ciberseguridad pueden deberse a errores humanos.

8. Formación en materia de ciberseguridad y pruebas de phishing

¿En qué consiste este control?

La formación en materia de ciberseguridad es un control utilizado para educar a los empleados y usuarios de TI sobre los riesgos y amenazas cibernéticas. Les ayuda a identificar y reconocer los distintos ataques, y les equipa con la información necesaria sobre cómo protegerse a sí mismos y a sus organizaciones previniendo los eventos en primer lugar, y haciendo lo correcto después de un ataque o un intento de violación.

Las pruebas de phishing forman parte de un programa de formación en materia de seguridad que simula ataques de phishing mediante el envío de correos electrónicos falsos, pero muy realistas, de phishing a los empleados para medir su concienciación. Pone a prueba la eficacia de la formación en materia de seguridad, evaluando la reacción de los empleados a los correos electrónicos, y determina los comportamientos que deben mejorarse.

¿Por qué hay que adoptar este control?

Las empresas se basan en las personas, los procesos y la tecnología. Invertir en la seguridad de los procesos y la tecnología es muy importante, pero insuficiente, si se ignora el aspecto humano. Las empresas operan en un mundo en el que el 95% de los problemas de ciberseguridad pueden deberse a errores humanos.

A pesar de una seguridad informática muy avanzada, factores humanos como la carga de trabajo, el estrés, la falta de habilidades, el creciente uso del modelo de trabajo híbrido y la naturaleza humana básica pueden conducir a errores humanos. Sin embargo, este eslabón más débil de la cadena de seguridad puede convertirse en la mejor capa de defensa, cuando recibe el enfoque y la atención adecuados.

El elemento humano es también una preocupación para los reguladores. Algunas normativas -entre las que se incluyen, pero no se limitan a, el Estándar de Seguridad de Datos de la Industria de las Tarjetas de Pago (PCI-DSS), el Instituto Nacional de Estándares y Tecnología (NIST), la HIPAA y el Reglamento General de Protección de Datos (GDPR)- pueden exigir que los empleados reciban una formación periódica de concienciación en materia de seguridad.

Con el fin de establecer una cultura de seguridad, hacer que las personas formen parte del programa de ciberseguridad, cumplir con las



regulaciones y, en última instancia, proteger a una organización de los impactos de un posible incidente cibernético, la formación de concienciación sobre ciberseguridad y las pruebas de phishing se han vuelto extremadamente importantes.

¿Qué debe hacer una empresa para poner en marcha este control?

Las organizaciones deben tomar las siguientes medidas al establecer la formación de concienciación cibernética:

1. Realizar un análisis anual para identificar las brechas en su conjunto de habilidades de ciberseguridad y desarrollar e implementar hojas de ruta de formación y/o planes de proyectos para cerrar las brechas identificadas.

2. Establecer una formación anual (como mínimo) sobre ciberseguridad y un programa de concienciación sobre ciberseguridad que:

   – Sea obligatorio para todos los empleados, proveedores/contratistas y terceros asociados con acceso a la red corporativa.

   – Forme a los usuarios para evitar los riesgos y amenazas cibernéticas más comunes, como la ingeniería social y el phishing.

   – Proporcione contenidos actualizados con frecuencia -al menos anualmente para incorporar las últimas técnicas de ataque e ingeniería social.

3. Realizar, al menos anualmente, campañas internas de phishing.

4. Disponer de un proceso para informar de los correos electrónicos sospechosos a un equipo de seguridad interno para que los investigue.

5. Tener un proceso para responder a las campañas de phishing.

6. Etiquetar los correos electrónicos externos para alertar a los empleados de que el mensaje procede de fuera de la organización.

El NIST de EE.UU. también se centra en la concienciación y la formación en materia de seguridad dentro de la “función de protección” de su marco cibernético. Para más orientación, véase: “NIST Special Publication 800-50 Revision 1 (SP 800-50r1).

9. Mitigación del protocolo de escritorio remoto (RDP) y otras técnicas de bastionado

¿En qué consiste este control?

Bastionado hace referencia al proceso de aplicar configuraciones de seguridad a los componentes del sistema, incluidos los servidores, las aplicaciones, los sistemas operativos, las bases de datos y los dispositivos de seguridad y de red, de acuerdo con las mejores prácticas. Estas configuraciones se definen con el fin de reducir la superficie de ataque de una organización, limitando la exposición de cada plataforma en la red interna o que pueda estar frente a Internet.

¿Por qué hay que adoptar este control?

Bastionado hace referencia al proceso de aplicar configuraciones de seguridad a los componentes del sistema, incluidos los servidores, las aplicaciones, los sistemas operativos, las bases de datos y los dispositivos de seguridad y de red, de acuerdo con las mejores prácticas. Estas configuraciones se definen con el fin de reducir la superficie de ataque de una organización, limitando la exposición de cada plataforma en la red interna o que pueda estar frente a Internet.

¿Qué debe hacer una empresa para poner en marcha este control?

Normalmente, las organizaciones definen un conjunto de configuraciones seguras para sus principales sistemas y servicios, basadas en las mejores prácticas, comúnmente conocidas como líneas de base de seguridad o guías de bastionado. Se implementa un proceso para desplegar estas configuraciones, y revisarlas periódicamente, con el fin de identificar cualquier error de configuración o desviación.

Aunque varían entre cada plataforma, las configuraciones que comúnmente forman parte de estas líneas base de seguridad pueden incluir lo siguiente :

- Gestión de usuarios y accesos.
- Políticas de contraseñas.
- Servicios y protocolos seguros.
- Configuraciones de cortafuegos.
- Configuraciones de red.
- Acceso remoto.
- Gestión de logs (registro de eventos) y políticas de auditoría.
- Protecciones antivirus/antimalware.
- Control de aplicaciones.
- Actualizaciones de seguridad.
- Cifrado.
- Otras configuraciones de seguridad específicas de la plataforma.

Para garantizar el despliegue oportuno de estas configuraciones, las organizaciones pueden utilizar imágenes de sistemas con configuraciones o herramientas de seguridad ya aplicadas y luego realizar un análisis de las deficiencias periódicamente.

Un tema importante que preocupa a las aseguradoras es la exposición a Internet de protocolos o servicios débiles o comúnmente atacados, como el protocolo de escritorio remoto (RDP), el bloque de mensajes de servidor (SMB), el secure shell (SSH), el protocolo de transferencia de archivos (FTP), así como los puertos de bases de datos.

Las organizaciones necesitan tener un estricto proceso de bastionado para eliminar el uso de este tipo de puertos expuestos a Internet. Si son necesarios, como resultado de un requisito empresarial específico, las organizaciones deben implementar controles compensatorios para mitigar el riesgo asociado.

Uno de los obstáculos más comunes a la hora de implantar un proceso de bastionado es la ausencia de un inventario completo de activos, que proporcione a la organización un conocimiento detallado de las tecnologías existentes en la red, que pueden estar soportando procesos críticos.

Se aconseja a las organizaciones que definan un proceso estructurado de gestión de cambios para desplegar estas líneas básicas de seguridad. Sin un proceso adecuado, algunos de estos arreglos pueden afectar a la disponibilidad de los sistemas al deshabilitar configuraciones que son necesarias en el momento del despliegue. Pueden necesitar un análisis más profundo para encontrar un método seguro de funcionamiento o incluso pueden requerir un cambio en una aplicación. En la actualidad, los proveedores y las organizaciones de ciberseguridad publican constantemente líneas de base de seguridad para los sistemas y servicios más comunes. El Centro de Seguridad de Internet (CIS) es una de las fuentes más importantes de líneas de base a las que pueden acceder todas las organizaciones.

10. Accesos y monitorización

¿En qué consiste este control?

Para poder reaccionar a tiempo ante un ciberataque, las organizaciones necesitan establecer sólidas capacidades de accesos y monitorización que les permitan identificar cualquier actividad sospechosa en la red. Estas capacidades requieren conocimientos, herramientas y procesos específicos para poder detectar actividades maliciosas. Todos estos factores son normalmente ejecutados por un centro de operaciones de seguridad (SOC) o un proveedor de servicios de seguridad gestionado externo (MSSP). El SOC o el MSSP pueden incluir diferentes capacidades, dependiendo de su nivel de madurez y sofisticación.

¿Por qué hay que adoptar este control?

El actual panorama global de amenazas requiere que las empresas no sólo implementen un conjunto de controles para proteger a sus organizaciones de un ciberataque, sino que también identifiquen a tiempo cualquier actividad sospechosa que pueda indicar un posible ataque en curso y que pueda desencadenar un plan de respuesta a ciberincidentes. Esto sólo puede llevarse a cabo mediante una adecuada configuración de accesos en los principales sistemas y aplicaciones de la empresa, las herramientas apropiadas para recopilar, correlacionar y alertar en caso de una situación, así como el equipo adecuado capaz de analizar y actuar en caso de un incidente.

¿Qué debe hacer una empresa para poner en marcha este control?

Se recomienda a las empresas:

1. Esquematizar e implementar la auditoría de logs (registro de eventos) y los sistemas o plataformas a monitorizar, incluyendo cortafuegos, sistemas de prevención de intrusiones y sistemas de detección de intrusiones, directorio activo, antivirus/antimalware, tecnologías de seguridad de punto final como EDR y XDR, prevención de pérdida de datos (DLP), aplicaciones, Microsoft 365, y otras plataformas importantes definidas por la organización.

2. Implementar un sistema de gestión de incidentes y eventos de seguridad (SIEM) e integrar las principales plataformas en este sistema. Los logs (registro de eventos) deben ser accesibles durante al menos los últimos tres meses y tener una copia de seguridad de un año como mínimo.

3. Analizar los logs (registro de eventos) en la red y definir un conjunto de casos de uso o patrones comunes que la organización quiera monitorizar y ante los que reaccionar, en el caso de que se encuentren. La información también debería utilizarse junto con la información de inteligencia de amenazas.

4. Definir procesos para revisar, periódicamente, las actividades de los administradores o usuarios con altos privilegios en los sistemas críticos.

5. Definir y formar un equipo de profesionales especializados en la monitorización de eventos de seguridad y respuesta a incidentes.

   - Deben definirse procesos específicos o playbooks para que el SOC y el MSSP puedan reaccionar si se detecta un incidente de ciberseguridad. Si este servicio se subcontrata, estos procedimientos deben incluir también las tareas que la organización tendría que ejecutar para contener, erradicar y restablecer la normalidad de las operaciones.

   - Definir y supervisar los indicadores clave de rendimiento para la mejora continua.

El desarrollo de mecanismos adecuados de accesos y monitorización puede requerir una inversión y recursos significativos por parte de la organización. Además, el establecimiento de estas capacidades requiere una revisión continua para garantizar que los procesos establecidos son capaces de detectar actividades sospechosas en escenarios de la vida real.



11. Sustitución o protección de los sistemas obsoletos

¿En qué consiste este control?

Los sistemas obsoletos son aquellos que llegan al final de su ciclo de vida, lo que impide a los usuarios recibir actualizaciones. Estos sistemas suponen un riesgo porque el proveedor ya no ofrece parches ni otras formas de soporte de seguridad. Una vez que la tecnología no recibe soporte, estará expuesta a vulnerabilidades no corregibles.

La única forma totalmente eficaz de mitigar este riesgo es dejar de utilizar el producto obsoleto y sustituirlo o actualizarlo por una solución más reciente que siga ofreciendo soporte. Cuando esto sea imposible, los sistemas obsoletos tendrán que ser protegidos mediante controles compensatorios, como restringir el acceso a esos sistemas, asegurarse de que no están orientados a Internet y de que están air gapped, es decir, aislados físicamente de otros sistemas conectados.

Los sistemas obsoletos suelen ser utilizados por organizaciones con sistemas antiguos o cuyo ciclo de via es más largo, especialmente cuando los sistemas se utilizan para controlar la tecnología operativa (OT), que puede ser difícil y costosa de actualizar regularmente.

¿Por qué hay que adoptar este control?

Las vulnerabilidades de los sistemas obsoletos seguirán sin parchear y serán cada vez más explotables por los hackers que buscan formas fáciles de acceder a los sistemas. Las vulnerabilidades conocidas se discuten abiertamente en los foros, y los hackers son capaces de escanear fácilmente los sistemas obsoletos que siguen en uso.

Mientras que los puertos abiertos y el phishing por correo electrónico siguen siendo vectores de ataque populares, las vulnerabilidades de software conocidas también son un punto de entrada común, ofreciendo una ruta fácil para entrar en los sistemas. Una vez dentro, los hackers intentarán acceder a toda la red, buscando datos valiosos que robar y sistemas que cifrar.

¿Qué debe hacer una empresa para poner en marcha este control?

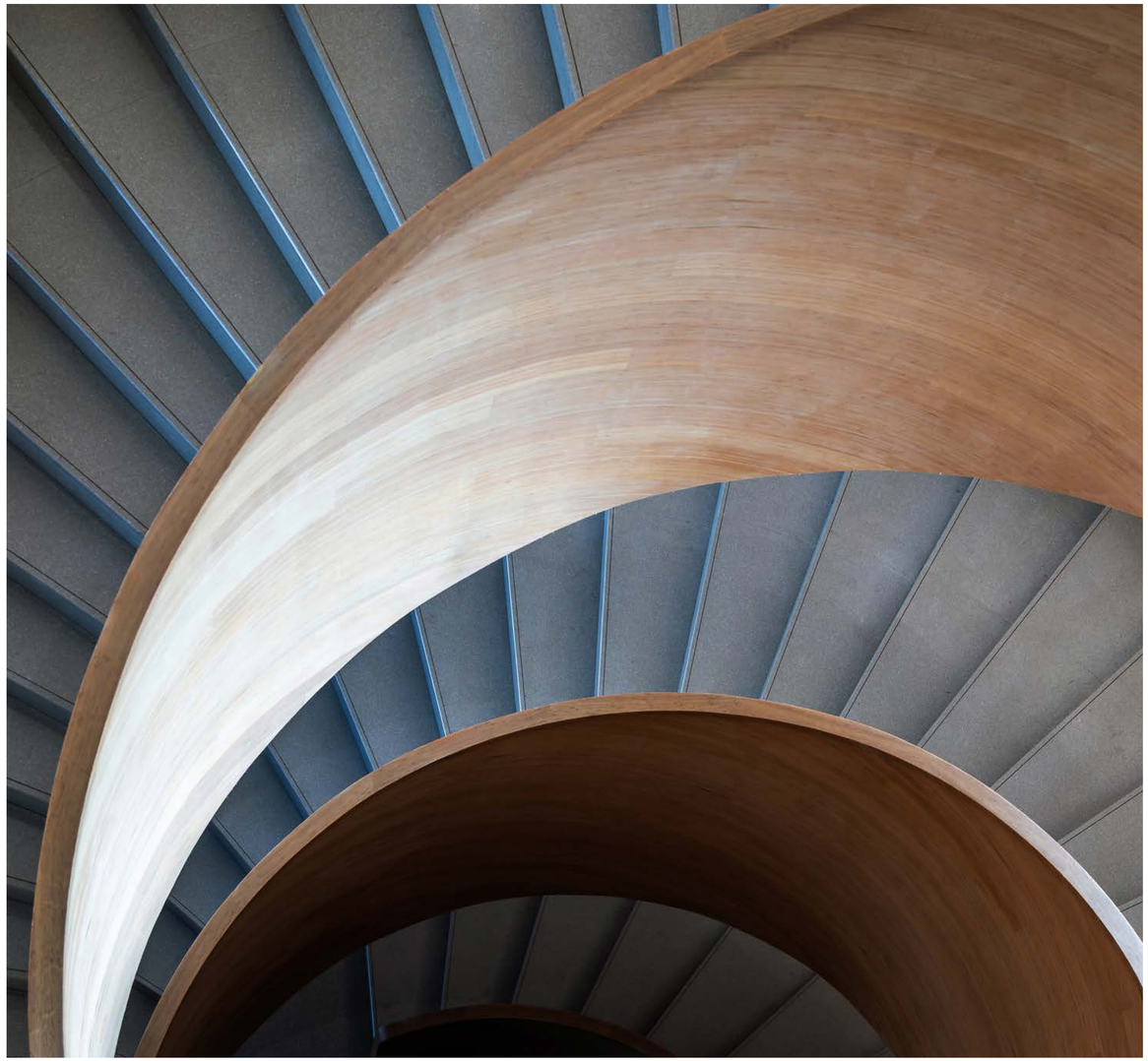
Lo ideal es que las organizaciones dejen de utilizar cualquier producto obsoleto. Si esto es inviable, es esencial asegurarse de que los sistemas antiguos están protegidos.

Limitar el acceso a estos productos desde fuera del entorno es un paso fundamental: si los atacantes no pueden llegar a un dispositivo, el riesgo de explotación se reduce considerablemente. En la medida de lo posible, deben implementarse estos huecos de aire (air gaps) en la red. Si esto no es posible, debe considerarse la posibilidad de instalar un cortafuegos de red discreto y supervisar los flujos de datos hacia los servidores obsoletos. Una buena regla general es tratar todo el acceso desde Internet como no fiable.

También se pueden tomar medidas para limitar el impacto potencial de un compromiso, como evitar que esos sistemas obsoletos accedan o almacenen datos o sistemas críticos y sensibles, lo que significa que un compromiso del dispositivo obsoleto no sería tan perjudicial.

La actualización de los sistemas y productos obsoletos tendrá un precio potencialmente elevado. En el caso de las organizaciones con un importante patrimonio y sistemas tecnológicos operativos, un producto EOL puede significar la necesidad de revisar, actualizar o sustituir todo el sistema.

Cuando las organizaciones optan por seguir utilizando el producto obsoleto , las medidas de protección y mitigación de riesgos necesarias requerirán una implementación exhaustiva y normalmente exigirán la colaboración de los equipos de seguridad de TI y OT, y también pueden requerir conocimientos y herramientas externas. Para los fabricantes y otras organizaciones con amplios sistemas de OT, esta implementación puede ser compleja y requerir mucho tiempo.



12. Gestión de riesgos cibernéticos en la cadena de suministro digital

¿En qué consiste este control?

La cadena de suministro digital engloba a todos los proveedores de tecnologías de la información (TI) y de servicios operativos (OT) que, junto con los equipos de una organización, prestan servicios digitales. En términos de riesgo cibernético, la cadena de suministro digital plantea un desafío cada vez mayor.

Un proveedor digital puede presentar el punto de entrada perfecto para cientos de empresas y sus datos sensibles. Al vulnerar con éxito una vulnerabilidad dentro de un solo proveedor digital, los ciberdelincuentes pueden obtener acceso a una multitud de redes y dispositivos de sus clientes. Se necesita un marco sólido para gestionar el ciberriesgo de la cadena de suministro digital.

¿Por qué hay que adoptar este control?

La creciente digitalización y el uso de la tecnología de la información y las comunicaciones para realizar funciones críticas ha introducido nuevos aspectos de ciberriesgo que deben ser gestionados. Las organizaciones están consumiendo nuevos y diferentes servicios digitales de varios proveedores de servicios, que ofrecen desde paquetes de software hasta productos completos subcontratados y de software como servicio (SaaS)[6]. Al mismo tiempo, el hecho de que las cadenas de suministro se hayan vuelto tan globales ha creado nuevos riesgos, en términos de confidencialidad, integridad y disponibilidad.

Dada la omnipresencia de los servicios digitales, cada vez es más complejo gestionar la cadena de suministro digital. Los equipos de TI pueden no ser conscientes de todos los servicios que consume la organización, lo que provoca el problema de la shadow IT o TI en la sombra[7]. Pero además, no siempre es evidente lo que constituye exactamente un servicio y las potenciales vulnerabilidades que conlleva. Los ciberdelincuentes utilizan estas cadenas de suministro digitales como mecanismo para los ciberataques. De hecho, la mayoría de los productos de software dependen de miles de paquetes preescritos producidos por los proveedores. Los componentes de la cadena de suministro de software de terceros más utilizados son objetivos muy apreciados por los ciberdelincuentes, ya que el acceso no autorizado a un proveedor de servicios digitales puede permitir el acceso a sus numerosos clientes.

6. El software-as-a-service o software como servicio (SaaS) es un modelo de distribución de software en el que un proveedor de la nube aloja aplicaciones y las pone a disposición de los usuarios finales a través de Internet.

7. La TI en la sombra se refiere a los programas, proyectos o sistemas de tecnología de la información implementados fuera de los departamentos de TI o de seguridad de la información.



Por lo tanto, este control tiene como objetivo proteger el riesgo cibernético de los proveedores digitales mediante un conjunto de actividades centradas en el análisis, la gestión y la respuesta al riesgo cibernético.

¿Qué debe hacer una empresa para poner en marcha este control?

Se aconseja a las organizaciones que consideren las siguientes acciones para gestionar el riesgo de la cadena de suministro digital:

- Adoptar un marco de gestión del riesgo de la cadena de suministro digital, que incluya la calificación del riesgo de los vendedores/proveedores de primer nivel, basándose en una cuantificación avanzada del riesgo. Esto ayudará a la organización a tomar decisiones estratégicas sobre la gestión de riesgos y la asignación de capital.

- Implementar un marco de ciberseguridad. Esto puede incluir, pero no está limitado a:

- Gestión de cuentas basada en las expectativas de “confianza cero” o zero trust y el principio de “necesidad de conocer” o need-to-know.

  Aplicación de limitaciones estrictas de las cuentas privilegiadas y genéricas.

  – Aplicación del Multifactor deautenticación (MFA) adecuada basada en el riesgo.

  – Enlazar con el centro de operaciones de seguridad (SOC) interno para desarrollar casos de uso específicos para supervisar los accesos de terceros.

- Desarrollar y probar playbooks de respuesta a incidentes para escenarios de proveedores/cadena de suministro digital e incluir a terceros.

- Evaluar los contratos, los acuerdos de servicio y los protocolos de escalada para cada proveedor digital.

- Colaborar con el departamento de compras para incluir controles y responsabilidades de ciberseguridad adecuados en los nuevos contratos y en las renovaciones. Esto puede incluir formaciones y certificaciones de seguridad.



A partir de aquí

En Marsh, creemos que el nuevo paradigma de riesgo cibernético requiere que las organizaciones se sientan más cómodas con la realidad de que el tejido conectivo de los negocios modernos es digital. Como tal, las organizaciones necesitan adoptar nuevos métodos para comprender, medir y gestionar el ciberriesgo de forma continua. Con disciplina, previsión y agilidad para cambiar el enfoque, las organizaciones pueden lograr mejores resultados al tiempo que se adoptan, colectivamente, los nuevos riesgos cibernéticos.

Cuando una organización aplique los controles recomendados, evitará, o estará equipada, para responder a la mayoría de los ciberataques, de forma que se minimice su impacto. Estarán bien preparadas para defenderse y se sentirán más seguras de su ciberresiliencia. Teniendo en cuenta el actual panorama cibernético y la creciente amenaza que se extiende sobre las organizaciones con la irrupción de la IA, la resiliencia cibernética ya no puede ser una idea tardía o un ejercicio opcional: se ha convertido en un requisito mínimo.

Más información

El conocimiento de primera mano de la ciberresiliencia tiene un valor incalculable. Con más de 25 años de experiencia cibernética y conocimientos basados en datos, Marsh está a la vanguardia de la comprensión del riesgo cibernético y de las amenazas emergentes que afectan a las empresas de todo el mundo. Estamos en una posición única para ayudarle a alinear las estrategias de riesgo, el seguro y la ciberseguridad, vinculando el riesgo cibernético con el riesgo empresarial para favorecer la toma de decisiones prudentes de inversión de capital.

Trabajamos con los clientes para mejorar la gobernanza del riesgo cibernético a nivel empresarial, creando una amplia involucración entre las principales partes interesadas de la organización y apoyando la toma de decisiones a nivel ejecutivo y del consejo de administración.

Con un equipo dedicado de asesores de riesgo cibernético, Marsh está capacitado para operar en la intersección de los seguros y la ciberseguridad y proporcionarle una visión cuantificada del riesgo cibernético en toda la empresa, además de ayudarle en la planificación de la resiliencia al riesgo cibernético.

Ofrecemos soluciones de asesoramiento y seguros cibernéticos a medida para ayudarle a gestionar sus riesgos cibernéticos y crear opciones eficaces de transferencia de riesgos.

Para saber más sobre cómo su empresa puede entender, medir y gestionar mejor el ciberriesgo, póngase en contacto con su representante de Marsh o con nosotros aquí.

Conocimiento experto de los procesos de ciberseguridad con más de 25 años de experiencia en ciberseguridad.

Contactos

Gonzalo Ayala
Manager, Technology Risk Practice Leader, Marsh
+34 673 51 08 83
gonzalo.ayala@marsh.com

Sofía García-Ollauri
Director, FINPRO & CYBER Coverage Counsel & Product Leader
Turnaround & Restructuring Practice Leader, Marsh
+34 603 75 49 26
sofia.garcia-ollauri@marsh.com

Nelia Argaz Durango
Head of Cyber-Digital Risks & Resilience Consulting,
Europe Risk Consulting Marsh
+34 603 75 49 26
nelia.argaz@marsh.com



Sobre Marsh

Marsh (NYSE: MRSH) es líder global en gestión de riesgos, reaseguros y capital, personas e inversiones y consultoría de gestión, asesorando a clientes de 130 países. Con unos ingresos anuales de 27.000 millones de dólares y más de 95.000 empleados en todo el mundo, Marsh ayuda a las organizaciones a prosperar gracias al poder de la perspectiva. Más información en corporate.marsh.com o en nuestros perfiles de LinkedIn y X.
Este documento es material de marketing.

La información contenida en este documento es privada y confidencial y tiene únicamente validez a efectos informativos.
Está destinada al uso exclusivo del destinatario y solo puede ser utilizada para la finalidad para la que se ha realizado. Todos los derechos de propiedad intelectual, con independencia de que estén o no registrados, de todas y cada una de las informaciones, contenidos, datos y gráficos que se incluyen en el documento pertenecen a Marsh, S.A. Mediadores de Seguros (en adelante Marsh), y el destinatario no obtendrá, ni deberá tratar de obtener, ningún derecho sobre la titularidad de dicha propiedad intelectual. Queda terminantemente prohibido que el documento se reproduzca, distribuya, publique, transforme y/o difunda, total o parcialmente, con terceras personas, físicas o jurídicas, públicas o privadas (incluidos los consultores y asesores del destinatario), sea con fines comerciales o no, a título gratuito u oneroso, sin el previo consentimiento por escrito de Marsh. MARSH, S.A. Mediadores de Seguros, Correduría de Seguros y Reaseguros, con domicilio social en Paseo de la Castellana, nº 216, 28046 Madrid y con N.I.F. A-81332322.
Se encuentra inscrita en el Registro Mercantil de Madrid en el Tomo 10.248, Libro: 0, Folio: 160, Sección: 8, Hoja: M-163304, Inscripción: 1 y en el Registro de la Dirección General de Seguros y Fondos de Pensiones con la clave nº J-0096 (Correduría de Seguros) y la clave nº RJ-0010 (Correduría de Reaseguros). Tiene concertados los Seguros de Responsabilidad Civil y de Caución, según se establece en la normativa de mediación de seguros y reaseguros privados aplicable.

© 2026 Marsh. Reservados todos los derechos.
26190357-EU