Riesgos y amenazas en productos fuera de soporte: prevención y protección

Abstract: el empleo de tecnología, sistemas y productos que entran en su final de ciclo de soporte por parte del fabricante supone un aumento del riesgo de la superficie de exposición. Las organizaciones deben ser conscientes de esta problemática y adoptar las medidas necesarias en materia de ciberseguridad.

Contenido:

1 INTRODUCCIÓN

En el ecosistema de productos tecnológicos existentes en las organizaciones puede darse la presencia de productos cuyo soporte haya finalizado o esté próximo a finalizar. Esta situación suele ocurrir periódicamente y provoca que las organizaciones tengan que realizar un esfuerzo para mantener en condiciones óptimas su base de tecnología y productos.

Los fabricantes desarrollan y publican actualizaciones tanto funcionales como de seguridad para los productos que se encuentran en soporte. Por el contrario, los productos que no tengan este soporte no dispondrán de estas actualizaciones y, en consecuencia, se quedarán obsoletos y facilitarán su exposición a la ciberamenaza.

Suele ser habitual que los productos más utilizados en las organizaciones sean también los más antiguos. Este hecho suele ir ligado a que su soporte esté próximo a finalizar o

que ya haya finalizado. Por tanto, su actualización o sustitución plantea una situación compleja para sus administradores, ya que **mantener productos sin soporte en la infraestructura supone que aumente su superficie de exposición y el riesgo asociado**.

Dependiendo de la tipología del producto a tratar, la situación será más o menos compleja. Por ejemplo, la problemática asociada a un servidor web del que existen pocos despliegues es menor que la de un sistema operativo que está ampliamente distribuido.

Además, en el caso de productos tales como los sistemas operativos, se incrementa considerablemente el riesgo asociado y su superficie de exposición. Así, **el mantenimiento de un sistema operativo fuera del ciclo de soporte del fabricante** no solo supone un riesgo para el propio puesto de trabajo, servidor o servicio, sino que **conlleva la exposición a la amenaza para otros activos que están correctamente soportados y mantenidos**.

Los atacantes son conocedores de esta situación y suelen aprovecharla para hacer efectivos sus ataques. Cuando se acerca el fin del ciclo de vida de un producto, especialmente cuando su uso está altamente extendido, los ciberatacantes ponen foco en ello, sabiendo de la debilidad manifiesta a la que se enfrentan las organizaciones:

- Cambio en las infraestructuras.
- Procesos de migración.
- Adaptación de nuevas tecnologías.
- Cambios en los procedimientos.

En muchas ocasiones, estos cambios no son fáciles de implementar y llevan asociado un alto coste en recursos y, desafortunadamente, **se espera excesivamente al fin del ciclo de vida de los productos para tomar decisiones y ejecutar las acciones pertinentes**. Debe considerarse que las fechas de fin de soporte suelen estar prefijadas y es más que factible hacer una planificación con la anticipación adecuada atendiendo a los procedimientos de mantenimiento con los que debe contar toda organización.

Uno de los problemas fundamentales es que, al no existir soporte, todas las vulnerabilidades conocidas que puedan aparecer en un producto no serán corregidas. Por consiguiente, esta debilidad se mantendrá en el tiempo hasta que el producto sea sustituido o actualizado. Adicionalmente, la relevancia de este tipo de vulnerabilidades que no sean corregidas provoca que los atacantes centren sus esfuerzos en desarrollar un código que permita explotarlas y beneficiarse de ellas. **Definitivamente, la inversión necesaria en la actualización o sustitución de estos productos está más que justificada**.

La obsolescencia de estos productos posibilitará la explotación de vulnerabilidades con mayor efectividad y, en consecuencia, que aumente la exposición a amenazas en toda la entidad de forma significativa.

Los fabricantes suelen **extender la duración del soporte de sus productos**, especialmente de los más extensamente implantados. Sin embargo, la aplicación del soporte extendido sólo **puede considerarse como una solución temporal ya que tarde o temprano también finalizará y la problemática seguirá existiendo**.

El **Esquema Nacional de Seguridad (ENS) ofrece** principios básicos, requisitos mínimos y medidas de protección que sirven de ayuda para mitigar el riesgo derivado de la presencia de productos fuera de soporte y por tanto se tratará en este documento.

2 SISTEMAS CON TECNOLOGÍAS FUERA DE SOPORTE: AMENAZAS FRENTE A LA SUPERFICIE DE EXPOSICIÓN

La existencia de tecnología y productos fuera de soporte en los sistemas de la organización puede suponer un riesgo para su seguridad. **Un producto no soportado por su fabricante no experimentará nuevas actualizaciones y los posibles fallos de seguridad que puedan aparecer no serán corregidos,** de forma que contribuirá a incrementar la superficie de exposición a la ciberamenaza.

2.1 AUMENTO DEL RIESGO EN LA SUPERFICIE DE EXPOSICIÓN

La **superficie de exposición viene determinada por los mecanismos de evaluación de las arquitecturas, los accesos, la conectividad, las interconexiones, los procesos, etc.**, de los sistemas de información, permitiendo predecir el potencial ataque y anticiparse a la materialización de las amenazas.

En los productos cuyo soporte ha finalizado, al no generarse actualizaciones de seguridad para corregir las vulnerabilidades que pudieran aparecer, el riesgo sobre la superficie de exposición de las organizaciones aumenta y, como resultado, las posibilidades de éxito ante un potencial ataque.

Las nuevas vulnerabilidades que pudieran aparecer sobre un producto sin soporte no sólo implican que exista riesgo de ataque sobre este, sino que pueden servir como **vector de entrada y método de propagación entre otros servicios que sí están mantenidos y soportados adecuadamente**.

La no existencia de soporte para un producto suele venir asociada con el tiempo de vida de la tecnología. Según van pasando los años, las tecnologías y protocolos que se emplean en los mismos se van quedando obsoletos y cada vez es más necesario generar parches de seguridad para corregir las debilidades publicadas. Por tanto, si en una infraestructura existen productos fuera de soporte, estos serán obsoletos y seguramente harán uso de protocolos y servicios en desuso, tanto para servirlos si se está hablando de tecnologías del lado del servidor como para consumirlos si son tecnologías de cliente.

Esto supondrá un aumento significativo tanto del riesgo al que se expone la entidad al disponer de dichas tecnologías obsoletas en sus infraestructuras como de la probabilidad de que una amenaza se materialice.

2.2 EJEMPLOS DE PROBLEMÁTICAS CON PRODUCTOS FUERA DE SOPORTE

Las amenazas que van asociadas a un producto sin soporte del fabricante son múltiples y deben ser conocidas por la organización al objeto de mitigar los problemas derivados.

Un producto fuera de soporte se corresponde con un producto obsoleto cuyas características son antiguas y, por tanto, pueden aparecer múltiples vulnerabilidades de diferentes categorizaciones que permitirían llevar a cabo diversas acciones maliciosas por parte de un atacante.

Es habitual la ocurrencia de incidentes de seguridad derivados de la explotación de las vulnerabilidades propias de los productos fuera de soporte. Por ejemplo, en los casos en que los servicios expuestos de la organización estén sustentados sobre productos que ya no están soportados por el fabricante, un atacante que haya realizado un proceso de rastreo podrá localizar las debilidades y explotarlas con éxito.

La utilización de productos sin soporte para la navegación por internet o la apertura de adjuntos en correo electrónico con aplicaciones obsoletas y sin las debidas actualizaciones de seguridad también supone un riesgo para la organización.

La materialización de cualquiera de estos incidentes de seguridad puede provocar un impacto en la actividad de la organización e incluso acarrear otras implicaciones, por ejemplo, si llevara asociada el robo o la exposición de datos de carácter personal.

A veces disponer de **una infraestructura externa convenientemente actualizada y unos sistemas de protección perimetral correctamente configurados crea una sensación de falsa seguridad** para los administradores de sistemas, que dejan en un segundo plano los productos sin soporte que pudieran existir en las redes internas. Los atacantes no necesariamente tienen que vulnerar la infraestructura externa para acceder a las redes internas de una organización.

A través de **ataques de ingeniería social**, entre otros, un atacante podría conseguir acceso a la infraestructura y aprovechando las debilidades que pudieran existir en un producto fuera de soporte podría llegar a hacer efectivo su ataque. También son conocidos los ataques por **movimiento lateral**, donde se buscan las debilidades más notables para moverse entre redes o servicios y explotar las capacidades de los atacantes allí donde la organización tenga el flanco más débil.

Un atacante puede permanecer durante mucho tiempo oculto en un servidor obsoleto, esperando el momento adecuado para desencadenar el ataque. Sabe de antemano que, puesto que ese servidor no va a recibir actualizaciones, la capacidad de cambio o

mantenimiento de éste, lo hacen ideal para la fase de persistencia que existe dentro de la fisonomía de un ciberataque.

L**a problemática asociada a la falta de soporte es variada y significativa, tanto para los riesgos originados como para las posibles decisiones y medidas de corrección**.

3 PRODUCTOS FUERA DE SOPORTE Y EL ESQUEMA NACIONAL DE SEGURIDAD

El Esquema Nacional de Seguridad (ENS) ofrece principios básicos, requisitos mínimos y medidas de protección que cabe aplicar cuando se da la circunstancia de la permanencia de productos fuera de soporte.

El principio básico '*Gestión de la seguridad basada en los riesgos*' (art. 6), en su apartado 2 establece que *"La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad…"*.

El principio básico '*Prevención, reacción y recuperación*' (art. 7), en su apartado 1 establece la prevención, además de la detección y corrección, como uno de los medios para conseguir que las amenazas no se materialicen, y en su apartado 2 se refiere a las medidas de prevención, que *"… deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición"*.

Además, el requisito mínimo de '*Integridad y actualización del sistema*' (art. 20), en su apartado 2, indica que *"Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos"*.

Dicho lo anterior, la presencia de productos fuera de soporte obligará a un esfuerzo adicional en ciertas medidas de protección.

3.1 EL ANÁLISIS DE RIESGOS CON PRODUCTOS FUERA DE SOPORTE

La medida *Análisis de riesgos [op.pl.1]* da lugar a una revisión periódica de activos, amenazas, salvaguardas y riesgos que permitirá detectar y señalar posibles productos cuyo soporte ha finalizado o bien tiene una finalización próxima.

La información resultante de la aplicación de esta medida ayudará a identificar, en particular, las medidas que puedan ser necesarias para afrontar los riesgos a que dé lugar la presencia de este tipo de productos.

3.2 MEDIDAS PROCEDIMENTALES

La existencia de productos fuera de soporte requerirá, en particular, un **esfuerzo adicional en medidas** relativas a mantenimiento, configuración, vigilancia y monitorización, entre otras, de los sistemas afectados, de forma complementaria y compensatoria, que deberán ir **acompañadas de los correspondientes procedimientos documentados** para minimizar posibles efectos de error humano o mala praxis.

Cabe reseñar especialmente las siguientes:

- *Mantenimiento [op.exp.4]*
- *Gestión de la configuración [op.exp.3]*
- *Gestión de Cambios [op.exp.5]*

3.3 MEDIDAS TÉCNICAS

La convivencia dentro la misma infraestructura de productos con y sin soporte puede ser el origen de fallos e incompatibilidades en su normal y adecuado funcionamiento. Además, pudiera provocar entre sus administradores una falsa sensación de seguridad. Ciertas medidas del ENS pueden ayudar a mitigar el riesgo:

- Medidas de *Monitorización del sistema* tales como *Detección de intrusión [op.mon.1]*
- Las medidas *Perímetro seguro [mp.com.1]* y *Protección de la confidencialidad [mp.com.2]*, con la implantación de cortafuegos para la protección, separación y control del acceso a la red interna desde el exterior o sus diferentes subredes (*Segregación de redes [mp.com.4]*).
- *Protección frente a código dañino [op.exp.6].* La presencia de productos obsoletos o fuera de soporte impactará en la protección frente a código dañino.
- *Criptografía [mp.si.2]* o *protección de claves criptográficas [op.exp.11]*. Aquí pueden darse dos (2) problemáticas: la derivada de mantener algoritmos o protocolos débiles y obsoletos, y la presencia productos que no puedan manejar sistemas de criptografía adecuados en base a condiciones actuales de protección.
- *Aceptación y puesta en servicio [mp.sw.2]*. Considerar en los procesos de puesta en servicio de nuevas tecnologías que éstas no sean obsoletas de por sí, o que en un plazo razonable de tiempo no vayan a quedar fuera de soporte por parte del fabricante.
- *Cifrado [mp.info.3]*. Caben las mismas consideraciones que en el caso de la criptografía.
- *Firma electrónica [mp.info.4]*. Igualmente aplican las mismas consideraciones que en criptografía.

- En relación con la *Protección de las comunicaciones*, medidas *Protección de la confidencialidad [mp.com.2]* y *Protección de la autenticidad y de la integridad [mp.com.3]*, pudiera haber impacto en el uso de productos VPN[1] cuya seguridad se vea mermada por la falta de soporte y la obsolescencia.
- La *Protección de los servicios [mp.s]*, en general, requiere atención especial, pues servicios tales como el correo electrónico o las aplicaciones web, entre otros, constituyen flancos particularmente expuestos a ataques.

Todas estas medidas se habrán de revisar siempre que se dé la circunstancia de existencia de activos fuera de soporte u obsoletos.

4 ORIENTACIÓN PARA LA TOMA DE DECISIÓN CON PRODUCTOS FUERA DE SOPORTE

Como resultado de la evolución continua de la tecnología, la problemática de los productos fuera de soporte es un reto que da lugar a la necesidad de adoptar determinadas decisiones.

En este apartado se tratan diferentes posibilidades que pueden servir como apoyo, orientando a posteriori las particularidades que puede ofrecer cada una de las opciones.

4.1 OPCIÓN 1. IMPLEMENTACIÓN DE SISTEMAS CLOUD

Las tecnologías basadas en la nube se han hecho muy populares y se ha normalizado su uso. Aunque su inicio supuso una revolución y un cierto rechazo por parte de las entidades, su constante evolución, así como las ventajas que aporta, constituye una opción más que interesante para que las organizaciones puedan plantearse el despliegue de nuevos servicios o actualizar los que ya se encuentren obsoletos.

Las soluciones compatibles con tecnologías *cloud* ofrecen ventajas tanto funcionales como en su administración que hacen que la migración a este tipo de soluciones haya pasado a ser una de las opciones para resolver la problemática de los productos fuera de soporte.

Los servicios *cloud* suelen estar dotados por defecto de funciones de seguridad o, si no, permiten su integración con soluciones altamente populares. Por ejemplo, a título ilustrativo, no se entiende una solución de correo electrónico en un entorno *cloud*, sin que el proveedor proporcione por defecto:

- Evolución y actualización de la solución para la protección frente a vulnerabilidades conocidas.
- Solución *antispam* y *antiphishing*.

[1] Virtual Private Network.

- Protección frente a código dañino.
- Protección frente a ataques de denegación de servicio.
- Pasarelas seguras de correo sobre TLS (*Transport Layer Security*).
- Sistemas avanzados de registro de actividad, análisis de buzones, retención de correos ante problemas legales, protección de información, etc.

Debido a la variedad de proveedores de servicios *cloud* existente, la organización debe llevar a cabo un análisis de los mismos, previo a la migración o despliegue de una nueva solución, para evitar problemas de compatibilidades con las infraestructuras de origen y destino.

En las soluciones *cloud*, el *hardware* y, dependiendo de la solución también el *software* y los componentes de los que depende la infraestructura, son propiedad del proveedor de los servicios. Es este proveedor quien pasa a responsabilizarse de su mantenimiento y su gestión, liberando de esa tarea a los clientes siempre y cuando no se haya internalizado el servicio *Cloud*.

Además, los proveedores de servicios *cloud*, para proporcionar una mayor fiabilidad a sus clientes, ofrecen facilidades de cara a configurar los servicios migrados a la nube con tolerancia a fallos, alta disponibilidad y capacidad de crecimiento sostenible.

Dentro de las diferentes posibilidades que proporcionan los sistemas *cloud*, cada organización elegirá la solución que mejor cumpla con sus necesidades y se adapte a su entorno. Existen diferentes opciones que ofrecen los proveedores en relación con las tecnologías *cloud computing*, especialmente para adaptarlas a las necesidades de cada entidad:

- *Software* como servicio. SaaS.
- Plataforma como servicio. PaaS.
- Infraestructura como servicio. IaaS.

Cada una de ellas proporciona una serie de características en las cuales la organización debe dedicar más o menos esfuerzo, pero a la vez se encuentra más o menos limitado. Así, por ejemplo, los servicios SaaS requieren de un menor coste administrativo, pero son menos flexibles en cuanto a opciones que los servicios en modalidad IaaS.

Los proveedores de servicios *cloud* tienen en general una política de pago por uso, es decir, que sus clientes sólo pagan por el uso que hagan de los diferentes recursos ofrecidos. Dentro de este modelo, dependiendo del tipo de servicio contratado, los clientes pueden escoger, en relación con el consumo de servicio, entre tres (3) tipos de nube:

- Pública. Compartir el *hardware* existente en la plataforma del proveedor con otros clientes.

- Privada. Reservar *hardware* para su uso en exclusividad internalizando principalmente el servicio.
- Híbrida. Ambas soluciones anteriores no son excluyentes, de manera que se puede conectar las soluciones de la nube privada con las hospedadas en la nube pública.

Cada una de ellas ofrece diferentes posibilidades en relación con los siguientes elementos:

- Control de la información sensible y protección en los accesos.
- Flexibilidad para aprovechar los recursos adicionales que ofrecen las tecnologías *cloud* cuando se necesiten.
- Facilidad para la transición de servicio y control de la carga de trabajo.
- Rentabilidad para escalar los entornos en función de las necesidades.

Los principales proveedores de servicios de nube, en general, cumplen con los estándares y las normativas principales de seguridad de la información tales como el ENS. Sin embargo, esto no exime que haya que realizar las preceptivas configuraciones y la aplicación efectiva de la política de seguridad corporativa.

Para mayor información sobre servicios en la nube y seguridad véanse las guías *CCN-STIC 823 Servicios en la nube*, *CCN-STIC 886 Perfil de cumplimiento específico de Cloud Privados* y otras guías relativas a servicios cloud específicos.

4.2 OPCIÓN 2. ACTUALIZACIÓN DE SISTEMAS CON TECNOLOGÍAS FUERA DE SOPORTE

Cabe la posibilidad de que existan organizaciones que, debido a las características de su entorno, los servicios que ofrezcan o la tipología de los datos que manejen no contemplen la posibilidad de migrar al *cloud* los sistemas cuyo soporte hayan finalizado. En esta situación la organización debe proceder a actualizar todas las tecnologías que se encuentren fuera de soporte.

Para llevar a cabo esta labor, se debe evaluar cuántos sistemas se encuentran en este estado y generar un plan de trabajo para llevar a cabo las actualizaciones necesarias teniendo en cuenta factores como la disponibilidad de dichos sistemas, las compatibilidades y dependencias con otras tecnologías de la organización y la posibilidad de retornar a la situación inicial en caso de existir algún fallo en el proceso.

Se recomienda seleccionar **sistemas que se encuentren en entornos controlados o cuya falta de disponibilidad no afecte de manera crítica a la organización para comenzar las labores de actualización**. Una vez actualizados estos sistemas y habiendo comprobado que todas las tecnologías que dependen de estos sistemas funcionan correctamente, se puede actualizar el resto de los sistemas definidos en el plan de trabajo.

Esta opción debe valorarse ya que con el paso de tiempo el soporte de los productos actualizados volverá a finalizar, por lo que la organización debe seguir gestionando y manteniendo el ciclo de vida de los productos para evitar que éstos se queden sin soporte a lo largo del tiempo.

Esta opción **es lógica para puestos de trabajo y determinados servicios exclusivamente internos, pero debe valorarse si es lo más adecuado, teniendo en consideración las capacidades de la nube**, especialmente para la prestación de servicios públicos o que se sabe que demandan una alta escalabilidad.

Las ventajas de actualizar los productos sin soporte son:

- **Control de la infraestructura y los productos**. La organización tendrá el control en todo momento de su infraestructura y los productos que residan en ella.
- **No existen problemas en la integración**. No es necesario realizar cambios en la infraestructura una vez que se actualicen los productos.
- **Información protegida en escenarios de información sensible**. Los datos de la organización se seguirán manteniendo en la infraestructura interna.

Las desventajas de esta solución son:

- **Gestión y mantenimiento**. Las organizaciones deben encargarse de continuar manteniendo y gestionando los productos.
- **Crecimiento de las necesidades**. Las nuevas tecnologías cada vez requieren un *hardware* con mejores y mayores prestaciones, lo que puede conllevar la necesidad de adquirir nuevos servidores o la actualización de los ya existentes.

  Los espacios físicos de los CPD[2] fueron diseñados bajo unas ciertas premisas, con determinadas características y cargas de *hardware* concretos, con una serie de limitaciones físicas de almacenamiento. Por ejemplo, con el auge del teletrabajo, muchas organizaciones que han querido internalizar todo el servicio se han encontrado con problemas de capacidad física en sus CPD para soportar más servidores que permitieran ofrecer las funcionales adecuadas.
- **Problemas de compatibilidad**. Es posible que al actualizar un producto existan problemas de compatibilidad con otras tecnologías ya existentes en la infraestructura.
- **Con el paso del tiempo** el producto actualizado volverá a perder el soporte teniendo que **volver a realizar la misma operativa**.

[2] Centro de Proceso de Datos.

4.3 OPCIÓN 3. CONTRATACIÓN DE SERVICIOS DE SOPORTE EXTENDIDO

En determinadas ocasiones, por motivos de continuidad de negocio y/o disponibilidad de servicio, las organizaciones no contemplan a corto plazo la migración de sus productos a la nube y tampoco pueden actualizar o sustituir ciertos productos sin soporte de sus infraestructuras. Algunos fabricantes son conocedores de esta situación y ofrecen la posibilidad de contratar un soporte extendido para alguno de sus productos.

Esta debe ser la última opción y siempre debe enfocarse como una solución temporal mientras se implementan algunas de las soluciones anteriormente descritas.

El soporte extendido, en la mayoría de los fabricantes, sólo incluye actualizaciones y parches de seguridad. No incluye nuevas actualizaciones, desarrollos o diseños que no tengan relación con la seguridad.

En algunos casos, para productos cuya demanda está muy extendida, los fabricantes pueden proporcionar este soporte de manera gratuita. Un ejemplo es el soporte extendido que Microsoft proporciona a los usuarios de Windows 7 bajo ciertos condicionantes: sólo en el caso de llevar esos Windows 7 a escritorios virtuales en Microsoft Azure. Pero ha de tenerse en cuenta que, en la mayoría de los casos, este tipo de soporte extendido tiene un coste.

El soporte extendido también tiene una fecha de finalización, por lo que no debe considerarse como una solución permanente, sino que se debe complementar con otras medidas.

La contratación de un soporte extendido es una solución que pueden proporcionar algunos fabricantes.

Sus principales ventajas son:

- Proporciona una solución temporal mientras **se implementan otras opciones de remediación**.
- **No es necesario realizar cambios** en la infraestructura existente.

Las desventajas principales son:

- Se trata de una **medida temporal y costosa** para las organizaciones.
- **A medio plazo deberán acometerse otras medidas** como la migración o cambio del producto o sistema.
- Indica que la organización **no ha llevado a cabo planes de mantenimiento adecuados**.

4.4 OPCIÓN 4. MANTENIMIENTO DE TECNOLOGÍAS SIN SOPORTE POR CONSIDERACIONES DE SERVICIO O ECONÓMICAS

En los casos, en los que por motivos de continuidad de negocio/servicio o por motivos de inversión económica, no sea posible implementar alguna de las soluciones anteriormente expuestas y sea necesario mantener los productos sin soporte, **se deben aplicar medidas compensatorias y complementarias de vigilancia** teniendo en cuenta siempre el riesgo que supone tener tecnologías fuera de soporte en la infraestructura de las organizaciones.

4.4.1 RIESGOS QUE ASUME LA ORGANIZACIÓN

Al mantener productos fuera de soporte en la infraestructura se asumen riesgos en el corto y medio plazo. Éstos se manifiestan a través de **diferentes problemas de seguridad que pudieran aparecer en un producto obsoleto por razón de la exposición a la explotación de vulnerabilidades, la obsolescencia de protocolos o la debilidad de algoritmos**.

Un atacante podría llevar a cabo las siguientes acciones, entre otras:

- Toma de control de la infraestructura o de servicios concretos.
- Extraer, modificar o eliminar información sensible de la organización.
- Conducir ataques de denegación de servicio.
- Suplantar identidades.
- Utilizar a una organización para realizar ataques efectivos contra otras enmascarando sus acciones.
- Propagar código dañino cuyos efectos pueden ir desde el cifrado de información pidiendo un rescate para descifrarla (*ransomware*) hasta la fuga de información sensible.

4.4.2 MEDIDAS COMPENSATORIAS Y COMPLEMENTARIAS DE VIGILANCIA

Entre las posibles siguientes medidas compensatorias o complementarias caben las que siguen.

- **Situar estos productos en redes aisladas** cuyo acceso esté lo más restringido posible. De esta manera se reducirán los riesgos frente a propagación de *malware*, movimientos laterales y *pivoting*[3]. Además, este aislamiento servirá también como medida de protección frente al robo de información. Este aspecto debe ser muy determinante ya que uno de los motivos por los cuales se pueden llegar a mantener estos productos es la criticidad de los datos que manejan.

[3] método para acceder a un segundo equipo a través de otro ya atacado.

- Realizar una **correcta segregación de las redes en las que existan productos fuera de soporte**, implementando en ellas sistemas de detección y prevención de intrusos: IDS (*Intrusion Detection System*) e IPS (*Intrusion Prevention System*) respectivamente, y filtrado de las comunicaciones con una correcta configuración de los *firewalls* de red.
- **Configurar correctamente los sistemas de autenticación** para las aplicaciones y servicios que estén accesibles a través de estas redes. Se incluirá la obligación de utilizar contraseñas robustas, de actualizarlas periódicamente y en caso de considerarse necesario la implementación de múltiple factor de autenticación (MFA).
- Además, debido al riesgo elevado que existe en dichas redes, se deben **implementar sistemas de monitorización que permitan vigilar y trazar** todo el tráfico de entrada y salida a las mismas.
- Adicionalmente, para tener el **control y medir la evolución de la superficie de exposición**, se recomienda el uso de herramientas que permitan realizar el seguimiento del nivel de peligrosidad al que se expone la organización y así poder precisar las medidas oportunas, tanto de índole técnico como procedimental. Estas herramientas deben **facilitar la gestión y el control de las vulnerabilidades que puedan aparecer en los productos** que se van a mantener sin soporte del fabricante.

Además, como se ha apuntado más arriba será necesario reforzar las medidas de *Gestión de la configuración [op.exp.3]*, *Mantenimiento [op.exp.4]* y *Gestión de cambios [op.exp.5]*.

En adición a lo anteriormente expuesto, se exigirá un **mayor esfuerzo relacionado con las tareas de monitorización de los sistemas afectados** por la falta de soporte que implica un mayor esfuerzo en la vigilancia de la red.

Las medidas procedimentales apuntadas previamente se complementarán con medidas tales como la medida *Detección de intrusión* [op.mon.1] con la implantación de dispositivos IDS e IPS con los análisis de IoC (indicadores de compromiso) específicos para tecnologías fuera de soporte.

Igualmente, las medidas *Perímetro seguro* [mp.com.1] y *Protección de la confidencialidad* [mp.com.2], con la implantación de cortafuegos para la protección, separación y control del acceso a la red interna desde el exterior o sus diferentes subredes (*Segregación de redes* [mp.com.4]).

Es precisamente la *Segregación de redes* [mp.com.4] una de las principales medidas técnicas que contribuyen a la reducción de las amenazas que afectan a la superficie de exposición de los diferentes productos fuera de soporte. Se debe valorar incluso el uso de equipos aduana o frontera que serán los responsables de autorizar el acceso a dichos

productos fuera de soporte dentro de la subred aislada del exterior (internet), hacen efectiva dicha reducción o la implantación de sistemas tipo diodo para limitar los flujos de información.

La medida *Protección frente a código dañino* [op.exp.6] es una de las más importantes medidas técnicas que complementa a las ya descritas. Esta medida de detección es la que, mediante la implantación de herramientas, monitoriza y bloquea vectores de ataque cuyo objetivo es el acceso ilegítimo a la infraestructura de la organización en la que se almacena y procesa la información. Se debe valorar emplear tecnologías específicas para la protección de servicios fuera de soporte, diversificar las soluciones empleadas por la organización para cubrir un mayor espectro de problemas o bien activar medidas más efectivas como la detección de anomalías o sistemas EDR (*Endpoint Detection and Response*).

Para los productos sin soporte relacionados con los servicios prestados vía web, se tendrá en cuenta la medida *Protección de servicios y aplicaciones web* [mp.s.2], de cara a especificar los diferentes tipos de ataque que pueden sufrir estos subsistemas debido a sus características particulares, y los diferentes métodos de detección e identificación, como son los análisis de vulnerabilidades, así como las pruebas de penetración (cajas blanca, gris y negra).

Por último, la periodicidad de la revisión de las medidas de marco operacional indicadas (*Gestión de la configuración* [op.exp.3], *Mantenimiento* [op.exp.4], *Gestión de cambios* [op.exp.5] y *Protección frente a código dañino* [op.exp.6]), así como de la medida *Protección de servicios y aplicaciones web* [mp.s.2], aportará un mayor control del estado de los sistemas o productos fuera de soporte, posibilitando la anticipación frente a posibles incidentes de seguridad.

Se debe **valorar el aumento de los mecanismos de vigilancia**, mediante:

- Incremento de la protección de autenticación.
- Mayor control de los accesos remotos y análisis de tráfico (origen y destino).
- Incremento en las condiciones de protección (bastionado) de clientes, servidores y servicios.
- Registros de acceso de actividad y correlación a través de soluciones SIEM[4] para los servicios obsoletos y su relación con otros sistemas.
- Implantación de protección de la información mediante tecnología de control de derechos (IRM)[5].

[4] Sistema de Gestión de Eventos e Información de Seguridad.
[5] Solución de protección centrada en lo datos, que permite que la información corporativa viaje protegida y bajo control en todo momento.

Como bien es sabido, ninguna medida procedimental o técnica de seguridad de las medidas preventivas anteriormente expuestas es infalible. En caso de la materialización de una amenaza que sea originada por el uso de productos fuera de soporte, se requerirá la definición y aplicación de un proceso de gestión de incidentes (*Gestión de incidentes* [op.exp.7]), medida de índole reactivo, con un nivel de madurez adecuado para minimizar sus consecuencias.

El mantenimiento de los productos fuera de soporte **sólo debe considerarse cuando no se puedan implementar ninguna de las otras opciones anteriormente citadas**.

Su principal ventaja es:

- Proporciona una solución en los casos en los que no sea posible implementar cualquiera de las soluciones anteriores por motivos de continuidad de negocio o inversión en tecnología altamente costosa.

Las desventajas de esta solución son múltiples:

- **Aumento del riesgo y las amenazas en la superficie de exposición**. La organización debe asumir los riesgos asociados a mantener estos productos.
- **Coste**. Es necesario realizar un gran desembolso para aplicar medidas compensatorias y complementarias de vigilancia necesarias para reducir el riesgo.
- **Tecnología obsoleta**. Al no actualizar los productos, se seguirá trabajando con tecnologías antiguas que no contarán con los últimos avances funcionales y de seguridad en los propósitos que desempeñen.
- Es necesario **implementar medidas compensatorias y complementarias de vigilancia** para reducir los riesgos.

5 CONCLUSIONES

Habida cuenta de lo recogido en el presente documento, se pueden determinar las siguientes conclusiones:

- La **existencia de productos fuera de soporte u obsoletos en una organización supone un aumento del riesgo** puesto que facilita a un posible atacante aprovechar las debilidades de tales productos.
- Cuanto mayor sea la obsolescencia de un producto o tecnología, mayores serán los riesgos a los que se enfrenta la entidad.
- **El Esquema Nacional de Seguridad** ofrece principios básicos, requisitos mínimos y medidas de protección que pueden ayudar a mitigar el riesgo de la presencia de productos fuera de soporte u obsoletos.
- Disponer de productos obsoletos en los escenarios corporativos TIC, implicará la **revisión de la política de seguridad, la reevaluación del Análisis de Riesgos o la**

adaptación de procedimientos y medidas técnicas para disminuir los problemas de seguridad derivados de esta casuística.

- Existen **diferentes opciones que las organizaciones deben evaluar** cuando se enfrentan al fin del ciclo de vida de productos, especialmente en lo relativo a los servicios que proporciona la organización.
- En referencia a los servicios, las entidades deben **valorar positivamente el empleo de tecnologías *cloud***, por los beneficios que ésta reporta.
- Por el contrario, y aunque pueda parecer una opción cómoda y en apariencia sostenible, **contratar soportes extendidos de productos a los fabricantes, no debe considerarse como la mejor opción**. En general, resulta una solución altamente costosa y requiere la aplicación de medidas complementarias de protección, así como la puesta en marcha de procedimientos operacionales adecuados.
- Únicamente cuando las características del servicio no permitan otra alternativa, se asumirá mantener productos obsoletos en la infraestructura. Por ejemplo, la adquisición de un *hardware* o *software* de investigación de alto coste hace años, cuyo valor para la organización es innegable y la inversión para su actualización resulta inviable.

  En este sentido **mantener este *hardware* o *software*, aunque no esté soportado por el fabricante, es un imponderable**. No obstante, la organización deberá aplicar **medidas compensatorias y complementarias de vigilancia** para limitar efectos negativos en materia de seguridad, tanto para dicho sistema como para el resto de los sistemas que sí se encuentren en un correcto estado de soporte.