LIBRO ELECTRÓNICO

# Las bases de la ciberseguridad

Cómo la seguridad por capas puede ayudarle a proteger sus clientes y garantizar sus beneficios

*A medida que las empresas se enfrentan a un número de ciberataques más elevado que nunca, se espera que los proveedores de servicios gestionados (MSP) proporcionen un nivel de seguridad básico a sus clientes. Aunque "básico" ha significado durante mucho tiempo el uso de un antivirus, en la actualidad no es suficiente. Se requiere una estrategia de seguridad por capas, que combine varios servicios de seguridad esenciales en una única plataforma integrada que proporcione una protección completa. Es justo en este punto donde los MSP pueden proteger sus beneficios.*

## POR QUÉ LA SEGURIDAD ES MÁS IMPORTANTE QUE NUNCA PARA LOS PROVEEDORES DE SERVICIOS GESTIONADOS

*Si una empresa sufre un ataque de ransomware y pierde datos financieros o información esencial de sus clientes , ¿quién se lleva la culpa? Independiente de que sea justo o no, suele ser el proveedor de servicios gestionados (MSP) el que la asume.*

¿Por qué? Porque, a medida que ciberataques como el ransomware son cada vez más habituales, la seguridad se convierte en una prioridad esencial para la mayoría de empresas. Los costosos ataques y las pérdidas de información aparecen con mucha frecuencia en las noticias y las empresas asumen que su asesor de TI de confianza proporciona un nivel de seguridad básico en sus servicios. Independientemente de que el MSP suministre esta seguridad, el resultado es el mismo: acciones de respuesta y mitigación que requieren mucho tiempo y que afectan a los beneficios del MSP, sobre todo a aquellos que trabajan en el marco de contratos con tarifas fijas.

Solo tenemos que examinar, por ejemplo, un estudio de 2017, en el que se indica que se requiere una media de 12 horas para hacer frente a un ataque de ransomware[1].

La mejor estrategia de la que dispone un MSP para evitar estos problemas es ofrecer un servicio de protección y seguridad esencial como parte de su oferta de servicios de TI gestionados. De esta forma, puede contribuir a la protección de sus clientes frente a las amenazas más frecuentes e incluso contribuir al crecimiento de su negocio, al destacar frente a la competencia.

### AMENAZAS DIVERSAS REQUIEREN VARIAS CAPAS DE SEGURIDAD

En la actualidad, las empresas se enfrentan a un número de riesgos de TI más elevado que nunca, entre los que se incluye el ransomware, accesos no autorizados, pérdidas de datos, ataques de denegación de servicio distribuido y espionaje corporativo. Asimismo, existen muchos puntos de entrada a través de los cuales pueden iniciarse estos ataques: tráfico web y de correo electrónico, unidades USB, inicios de sesión no seguros, dispositivos como smartphones y portátiles, aplicaciones y datos (tanto en reposo como en tránsito).

A pesar de lo que muchos proveedores de seguridad afirman, no existe una única "solución mágica" que pueda protegerle frente a una amplia gama de amenazas. Para proteger de verdad a sus clientes, los MSP deben ir más allá de los antivirus e implementar una estrategia de defensa en profundidad y por capas, que permite combinar varios controles y herramientas de seguridad para defender el sistema de TI. La clave radica en la redundancia que forma parte de esta estrategia: si falla un control de seguridad o si se supera, el resto de defensas superpuestas debe estar ahí para mitigar la amenaza.

*Piense en los diferentes niveles de seguridad que la gente aplica para proteger sus hogares. Por ejemplo, tienen una valla en su jardín, cierran las puertas, disponen de una alarma y guardan sus posesiones más valiosas en una caja fuerte. Si todo esto falla, siempre pueden recurrir a su seguro para sustituir lo que se ha perdido.*

1 *"The 2017 Endpoint Protection Ransomware Effectiveness Report," KnowBe4. Último acceso: junio de 2018.*

Piense en los diferentes niveles de seguridad que la gente aplica para proteger sus hogares. Por ejemplo, tienen una valla en su jardín, cierran las puertas, disponen de una alarma y guardan sus posesiones más valiosas en una caja fuerte. Si todo esto falla, siempre pueden recurrir a su seguro para sustituir lo que se ha perdido.

Así funciona la seguridad por capas, y es este mismo enfoque el que debemos aplicar en el ámbito de las TI.

## LAS BASES DE LA SEGURIDAD DE LAS TI

Los MSP creen que la integración de los servicios de seguridad en sus ofertas de servicios de TI deberían comenzar por los siguientes elementos básicos de seguridad:



### GESTIÓN DE REVISIONES

Muchos accesos no autorizados se producen cuando un atacante saca partido a elementos del sistema o del software no actualizados. Los MSP deben asegurarse de que todos los dispositivos que administran se encuentren actualizados con las revisiones de software más recientes. Sin embargo, cuanto mayor es el número de clientes que debe gestionarse, más difícil es controlar que todo esté al día. El software de gestión de revisiones ofrece una visibilidad completa sobre el estado de estas, gracias a funciones de automatización y programación que ofrecen un control individualizado sobre las políticas de revisiones.



### ANTIVIRUS AUTOGESTIONADO

La forma en la que un MSP gestiona su antivirus es tan importante como que este se encuentre implementado. Las mejores soluciones antivirus protegen frente al malware conocido y al nuevo (mediante una combinación de protección tradicional basada en firmas a la que se suman sofisticadas comprobaciones heurísticas y análisis de comportamiento), al mismo tiempo que proporcionan un elevado nivel de flexibilidad mediante políticas de cuarentena personalizables. Los antivirus integrados (o autogestionados) también ofrecen a los MSP un único panel desde el que pueden simplificar las implementaciones masivas en sitios y servidores, programar análisis automatizados en los periodos en los que no afectan a los usuarios finales, etc.



### PROTECCIÓN WEB

Es muy frecuente que los ataques de phishing, las descargas ocultas y otros ataques basados en la Web se produzcan cuando un usuario accede de forma inconsciente a un sitio malicioso. Los MSP necesitan un sistema que les permita bloquear las solicitudes de URL maliciosas para evitar las conexiones a dominios vinculados con atacantes. El software de protección web lleva a cabo esta labor, al mismo tiempo que permite a los MSP establecer sus propias políticas de filtrado de contenido, listas negras de sitios web, políticas de navegación y mucho más.

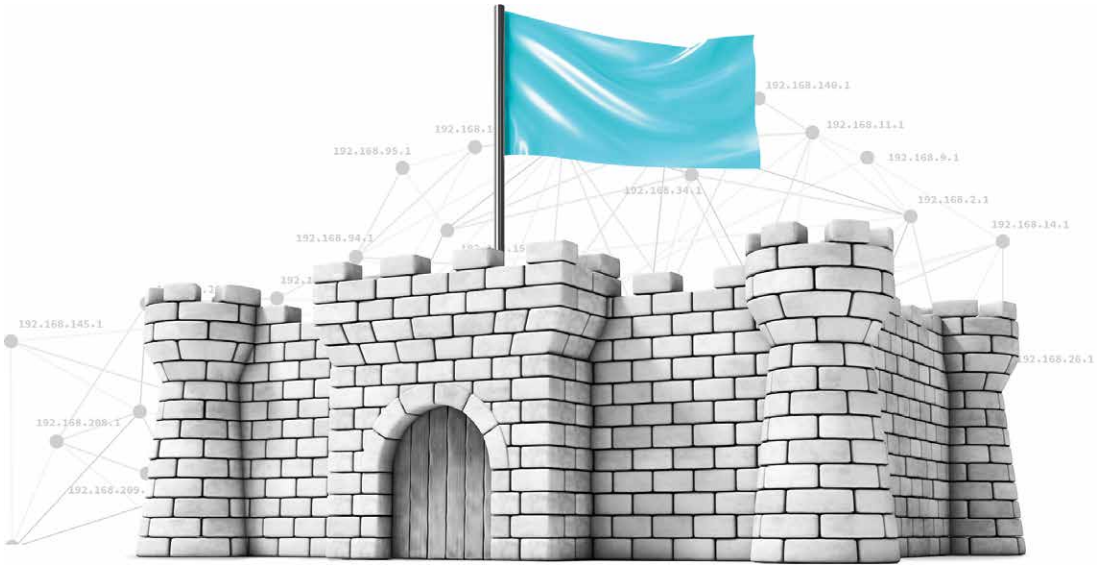
## FILTRADO DEL CORREO ELECTRÓNICO

La mayor parte de las amenazas de seguridad están vinculadas al correo electrónico. Mediante el análisis de los mensajes entrantes y salientes para detectar posibles adjuntos, scripts, dominios, URL y cadenas de texto maliciosos, el software de filtrado del correo electrónico facilita la tarea de proteger a los clientes frente al correo no deseado, los ataques de phishing y el malware. También ofrece a los MSP un control absoluto sobre las listas negras, las listas blancas y las políticas de cuarentena.

## COPIA DE SEGURIDAD

Las copias de seguridad son como los seguros: no siempre son necesarias, pero, cuando lo son, pueden salvarte la vida. Una solución de copia de seguridad basada en la nube y de recuperación después de una catástrofe es la mejor defensa posible frente a la mayoría de ataques de ransomware, al hacer posible que las empresas vuelvan a trabajar con rapidez, al permitir restaurar de forma rápida y sencilla los archivos corruptos o cifrados. Como mínimo, los MSP deben ofrecer una solución para realizar copias de seguridad de los documentos de sus clientes. Si gestionan servidores, también deben considerar realizar copias de seguridad de estos sistemas.

Lo ideal es que estos servicios estén integrados en todos los paquetes ofrecidos por el MSP. De esta forma, pueden garantizar que todos sus clientes disfruten de un nivel de protección básico.



## SEGURIDAD POR CAPAS EN ACCIÓN

Para ilustrar el motivo por el que la seguridad por capas es tan importante para la seguridad, piense en las diferentes formas en las que el ransomware puede acceder a la red de una organización[2]:



**73 %**
**Adjuntos de correo electrónico**



**54 %**
**Phishing mediante correo electrónico**



**28 %**
**Usuarios que visitan sitios web maliciosos o comprometidos**

El correo electrónico y la navegación web son, con diferencia, los puntos de inicio más habituales para una infección por ransomware. En la mayoría de los casos, los usuarios finales acceden de forma no intencionada a un sitio web comprometido o malicioso. Normalmente, suelen llegar a estos a través de un enlace o adjunto de aspecto legítimo que los engaña para que hagan clic o los abran.

*La información que se encuentra expuesta a un mayor grado de riesgo por los ataques de ransomware incluye los datos financieros (62%) y la información sobre clientes (61 %).*

Del mismo modo que los ataques de ransomware pueden acceder a la red de diferentes maneras, estos pueden detectarse de muchas formas. De hecho, la mayoría se detectan mediante herramientas de seguridad en los terminales, puertas de enlace web y de correo electrónico o sistemas de detección de intrusiones (por ejemplo, cortafuegos de red):



**83 %**
**Herramientas antimalware/antivirus/ de seguridad en los terminales**



**64 %**
**Puertas de enlace web y de correo electrónico**



**46 %**
**Sistemas de detección de intrusiones**

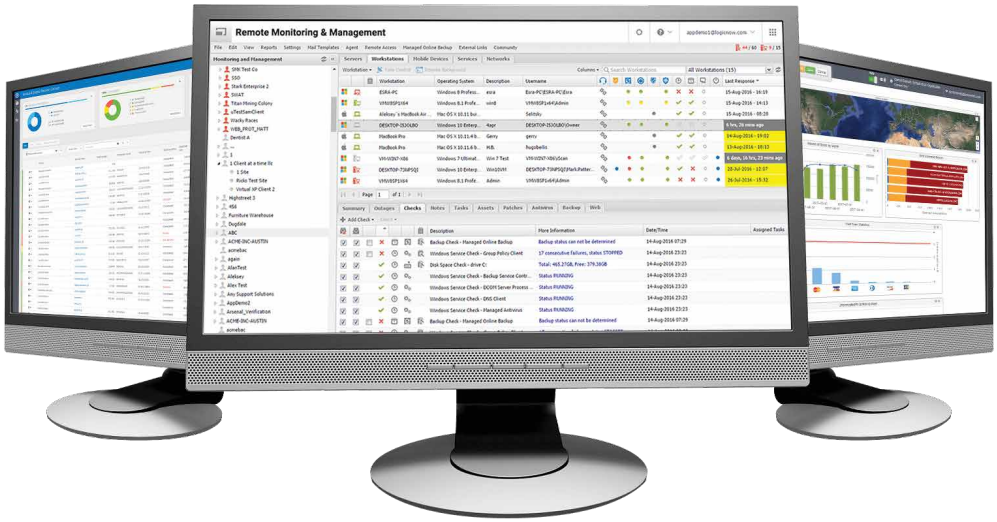
Si el cliente de un MSP solo confía en un antivirus, uno de cada cinco ataques de ransomware superarán este sistema de seguridad. Sin embargo, si se utilizan varios controles de seguridad superpuestos, incluso aunque uno supere el antivirus y acceda a la red, podrá seguir siendo detenido cuando intente pasar de un dispositivo a otro o cuando intente conectar con su servidor de control malicioso.

En la seguridad por capas, cada componente está diseñado para complementar al resto (e incluso compensar los huecos existentes) con el fin de detener las amenazas de seguridad avanzadas. La gestión de revisiones permite mantener el software y los sistemas operativos actualizados con las revisiones de seguridad más recientes para evitar que los atacantes saquen partido a las vulnerabilidades. Los antivirus detectan y bloquean un gran número de amenazas conocidas. Los sistemas de filtrado web y de correo electrónico sitúan en cuarentena los mensajes sospechosos e interrumpen la comunicación con los sitios de "mando y control". Además, las copias de seguridad de los datos hacen que la recuperación sea muy sencilla en caso de pérdida inesperada. De hecho, si se cuenta con un sistema de copia de seguridad implementado, el 54 % de las empresas puede recuperarse de un ataque de ransomware en 24 horas[2].

2 *Ransomware: 2017 Report, Bitdefender, Cybersecurity Insiders, Information Security Community on LinkedIn, Crowd Research Partners. Último acceso: junio de 2018.*

## SOLARWINDS OFRECE UN ENFOQUE SIMPLIFICADO PARA LA ESTRATEGIA DE SEGURIDAD POR CAPAS

*Implementar una estrategia de seguridad por capas no tiene que ser complejo ni costoso.*




A diferencia de lo que sucede con los productos de seguridad independientes, que pueden requerir experiencia específica en cada campo y consolas independientes, el sistema de seguridad básico de seguridad de ADM Cloud se encuentra completamente integrado en una única consola de administración.

A través de un panel fácil de usar, los MSP pueden asegurarse de que sus políticas de seguridad estén definidas y que se apliquen de forma coherente en todos los dispositivos que gestionan, incluidos los servidores. De esta forma, pueden disfrutar de las ventajas que les ofrece un panel único con el que pueden configurar y automatizar políticas de forma rápida y sencilla para aplicación de revisiones, antivirus, protección web, filtrado de correo electrónico, copias de seguridad y mucho más. Así, se agiliza la prestación del servicio y se aumenta la rentabilidad sin tener que incrementar la cantidad de esfuerzo o experiencia necesarios.

En algunos casos, estos elementos de seguridad esencial pueden activarse desde dentro de la plataforma de administración y supervisión remotas del MSP. En otros, tienen que adquirirse y activarse por separado. En cualquier caso, con SolarWinds es posible gestionarlos y automatizarlos de forma rápida y sencilla a través de un panel único. De este modo, los MSP pueden integrar la seguridad como componente esencial de sus paquetes de TI básicos (o, si lo prefieren, posicionar estos elementos como complementos en un paquete de bajo coste tarificado por dispositivo) y proporcionar a sus clientes la máxima tranquilidad mediante una oferta sencilla, eficiente y eficaz.

*Esto hace posible que los MSP integren la seguridad como un componente esencial de sus paquetes de TI básicos y así proporcionar a sus clientes la máxima tranquilidad a través de una oferta de seguridad sencilla, eficiente y eficaz.*

## UNA SITUACIÓN EN LA QUE TODOS GANAN

*Al adoptar la estrategia de defensa en profundidad y seguridad por capas y convertir las características de seguridad esenciales en parte de su oferta de servicios de TI gestionados, los MSP pueden satisfacer sus expectativas en materia de seguridad de TI.*

Los clientes de los MSP están tranquilos al saber que están expuestos a un menor riesgo de interrupción de su actividad asociadas a las amenazas oportunistas más habituales. Al contar con un cliente bien protegido, los técnicos del MSP tienen que dedicar menos tiempo a los problemas de seguridad rutinaria y a responder a un número menor de ataques. Cuando se cuenta con controles de seguridad básicos automatizados y gestionables con facilidad, los técnicos pueden ofrecer soporte técnico a un mayor número de clientes, así como centrarse en tareas de mayor valor que contribuyan a los objetivos a largo plazo de la empresa. Esto ofrece a los MSP la oportunidad de incrementar el tamaño de sus cuentas, ampliar los servicios facturables y fortalecer las relaciones con sus clientes. A medida que el MSP obtiene más conocimientos y experiencia en materia de seguridad, puede ofrecer servicios de seguridad más avanzados a sus clientes, lo que les permitirá conseguir más ingresos regulares.