Cisco 2016
Informe anual de seguridad

Resumen ejecutivo

Los profesionales de seguridad deben repensar sus estrategias de defensa.

Los atacantes y los defensores están desarrollando tecnologías y tácticas que crecen en sofisticación. Por su parte, los actores maliciosos están creando infraestructuras internas (back-end) sólidas con las que lanzar y respaldar sus campañas. Los delincuentes en línea están perfeccionando las técnicas para quitarles dinero a las víctimas y evitar ser detectados incluso si continúan robando datos y propiedad intelectual.

El Informe anual de seguridad 2016 de Cisco –que presenta ideas, perspectivas y la investigación de Cisco Security Research– pone de relieve los desafíos que deben hacer frente los defensores para detectar y bloquear a los atacantes que emplean un arsenal de herramientas frondoso y cambiante. En el informe también se incluye la investigación de expertos externos, como Level 3 Threat Research Labs, para arrojar más luz sobre las tendencias de amenazas actuales.

Analizamos en detalle los datos recabados por los investigadores de Cisco para mostrar los cambios con el tiempo, ofrecer perspectivas sobre el significado de estos datos y explicar cómo los profesionales de seguridad deben responder a las amenazas.

En este informe, presentamos y analizamos lo siguiente:

INTELIGENCIA DE AMENAZAS

En esta sección se analizan algunas de las tendencias de ciberseguridad más impactantes que nuestros investigadores identificaron, además de actualizaciones sobre vectores de ataque web, métodos de ataque web y vulnerabilidades. También incluye una mirada más amplia sobre amenazas crecientes como el ransomware. A fin de elaborar el análisis de las tendencias observadas en 2015, Cisco Security Research usó un conjunto global de datos de telemetría.

PERSPECTIVAS DEL SECTOR

En esta sección se analizan las tendencias de seguridad que afectan a las empresas, incluidos el uso creciente del cifrado y los potenciales riesgos de seguridad que presenta. Observamos las debilidades en la forma en que las pymes (SMB) están protegiendo sus redes. Y presentamos la investigación realizada en empresas que dependen de software desactualizado, no compatible o que está en el final de su vida útil para respaldar su infraestructura de TI.

ESTUDIO COMPARATIVO SOBRE CAPACIDADES DE SEGURIDAD

En esta sección se describen los resultados del segundo Estudio comparativo sobre capacidades de seguridad de Cisco, centrado en la percepción de los profesionales de seguridad acerca del estado de la seguridad en sus organizaciones. Al comparar los resultados de la encuesta de 2015 con los de 2014, Cisco descubrió que los directores generales de seguridad (CSO) y los administradores de operaciones de seguridad (SecOps) se sienten menos confiados en cuanto a poder frustrar ataques o que su infraestructura de seguridad esté actualizada. Sin embargo, la encuesta también indica que las empresas están intensificando la capacitación y otros procesos de seguridad en un intento por fortalecer sus redes. Los resultados del estudio son exclusivos del Informe anual de seguridad 2016 de Cisco.

UNA MIRADA HACIA ADELANTE

En esta sección se ofrece una mirada sobre el panorama geopolítico que afecta la seguridad. Analizamos los resultados de dos estudios de Cisco: uno en el que se examinan las inquietudes de los ejecutivos de ciberseguridad y otro que se centra en la percepción de los responsables de las decisiones de TI sobre los riesgos de seguridad y la confiabilidad. También ofrecemos una actualización acerca de nuestro progreso en la reducción del tiempo de detección (TTD) y destacamos el valor de migrar a una arquitectura de defensa ante amenazas integrada como medio para combatir las amenazas.

Contenido

Principales acontecimientos y descubrimientos

Principales acontecimientos y descubrimientos

Los delincuentes cibernéticos (ciberdelincuentes) han perfeccionado sus infraestructuras internas (back-end) para realizar ataques en formas que mejoran la eficacia y las ganancias.

- Con la ayuda de Level 3 Threat Research Labs y la cooperación del proveedor de alojamiento Limestone Networks, Cisco identificó y neutralizó la operación más grande del kit de ataque Angler en los Estados Unidos, que afectaba a 90 000 víctimas por día y generaba decenas de millones de dólares al año para los artífices de las amenazas por detrás de la campaña.
- SSHPsychos (Group 93), uno de los botnets de ataque de denegación de servicio distribuido (DDoS) más grandes jamás observado por los investigadores de Cisco, fue debilitado considerablemente gracias a los esfuerzos combinados de Cisco y Level 3 Threat Research Labs. Como el caso de estudio Angler antes mencionado, este éxito apunta al valor de la colaboración en el sector para combatir a los atacantes.
- Las extensiones de navegador maliciosas son un problema generalizado y pueden ser una fuente importante de filtración de datos para las empresas. Calculamos que más del 85% de las organizaciones estudiadas son afectadas por extensiones de navegador maliciosas.
- Botnets conocidos como Bedep, Gamarue y Miuref representaron la mayor parte de la actividad de comando y control mediante botnets que afectaba a un grupo de organizaciones que analizamos en julio de 2015.
- El análisis de malware validado como “malo conocido” de Cisco determinó que la mayor parte del malware (91,3%) usa el servicio de nombre de dominio (DNS) para realizar campañas. Mediante una investigación retrospectiva de consultas de DNS, Cisco descubrió que en las redes de clientes se estaban usando solucionadores de DNS “no autorizados”. Los clientes no estaban al tanto de que sus empleados estaban usando los solucionadores como parte de su infraestructura de DNS.
- Las vulnerabilidades de Adobe Flash siguen siendo populares entre los ciberdelincuentes. Sin embargo, los proveedores de software están reduciendo el riesgo de que los usuarios se expongan a malware a través de la tecnología Flash.
- Al observar las tendencias de 2015, nuestros investigadores sugieren que el tráfico cifrado HTTPS ha llegado a un punto de inflexión: pronto se convertirá en la forma dominante de tráfico de Internet. Si bien el cifrado puede proteger a los consumidores, también puede poner en riesgo la eficacia de los productos de seguridad, lo que dificulta el seguimiento de las amenazas para la comunidad de seguridad. Sumado al desafío, algunos tipos de malware pueden iniciar comunicaciones cifradas a través de un conjunto diverso de puertos.
- Los actores maliciosos están usando sitios web comprometidos creados con la popular plataforma de desarrollo web WordPress para sus actividades delictivas. Allí pueden organizar los recursos de servidores y evadir la detección.

- La infraestructura obsoleta está creciendo y deja a las organizaciones cada vez más vulnerables al riesgo. Analizamos 115 000 dispositivos de Cisco® en Internet y descubrimos que el 92% de los dispositivos de la muestra estaba ejecutando software con vulnerabilidades conocidas. Además, el 31% de los dispositivos de Cisco en el campo incluidos en nuestro análisis están en la etapa "fin de venta" y el 8%, en el "fin de vida útil".
- En 2015, los ejecutivos de seguridad mostraron un menor grado de confianza en sus herramientas y procesos de seguridad que en 2014, según el Estudio comparativo sobre capacidades de seguridad 2015 de Cisco. Por ejemplo, en 2015, el 59% de las organizaciones indicó que su infraestructura de seguridad estaba "muy actualizada". En 2014, el 64% dijo lo mismo. Sin embargo, sus crecientes preocupaciones de seguridad las están motivando a mejorar sus defensas.
- El estudio comparativo muestra que las pymes usan menos defensas que las grandes empresas. Por ejemplo, en 2015, el 48% de las pymes dijo que usaba seguridad web, en comparación con el 59% en 2014. Y el 29% afirmó que usaba herramientas de configuración y revisión en 2015, en comparación con el 39% en 2014. Tales debilidades pueden poner a los clientes empresariales de las pymes en riesgo, ya que los atacantes pueden violar más fácilmente sus redes.
- Desde mayo de 2015, Cisco redujo la mediana del tiempo de detección (TTD) de las amenazas conocidas en nuestras redes a unas 17 horas, es decir, menos de un día. Esto supera ampliamente el cálculo actual de TTD del sector, que es 100 a 200 días.

Sin desviarse de su meta: Para los ciberdelincuentes modernos, hacer dinero es fundamental

Sin desviarse de su meta: Para los ciberdelincuentes modernos, hacer dinero es fundamental

En el pasado, muchos delincuentes en línea se escondían en las sombras de Internet. Para evitar ser detectados solo hacían breves incursiones en las redes empresariales para lanzar sus ataques. Actualmente, algunos ciberdelincuentes envalentonados están aprovechando recursos en línea legítimos. Socavan la capacidad del servidor, roban datos y exigen rescates a las víctimas en línea cuya información tienen secuestrada.

Estas campañas son un escalamiento trascendente en la guerra entre defensores y atacantes. Si los atacantes encuentran más lugares en línea donde operar, su impacto puede crecer exponencialmente.

En este informe, los investigadores de seguridad de Cisco destacan las tácticas que usan los artífices de las amenazas para crear una infraestructura resistente con el fin de realizar campañas más fuertes y eficaces. Los atacantes siguen adoptando métodos más eficaces para aumentar sus ganancias y muchos están prestando especial atención al aprovechamiento de los recursos de servidores.

La explosión de ransomware (consulte la **página 10**) es un claro ejemplo. El ransomware les ofrece a los delincuentes una manera sencilla de extraer más dinero directamente a los usuarios. Cuando los atacantes establecen las campañas que ponen en riesgo a decenas de miles de usuarios por día con pocas interrupciones o ninguna, la “paga” por sus esfuerzos puede ser asombrosa. Además de desarrollar mejores formas de rentabilizar sus campañas, los atacantes están usurpando recursos legítimos como base de operaciones.

Ahora, los creadores de algunas de las variantes de ransomware y los desarrolladores de otros ataques están derivando el tráfico a sitios web de WordPress hackeados como una forma de evitar la detección y usar espacio de servidor (consulte la **página 33**). Y los responsables de SSHPsychos, uno de los botnets más grandes jamás visto por los investigadores de Cisco, operaban en redes estándar con poca interferencia hasta que el esfuerzo de eliminación combinado de Cisco y Level 3 Threat Research Labs persuadió a los proveedores de servicios para que bloqueen el tráfico al creador del botnet.

Inteligencia de amenazas

Inteligencia de amenazas

Cisco ha recabado y analizado un conjunto global de datos de telemetría para este informe. Las investigaciones y los análisis continuos realizados en torno a las amenazas descubiertas, como tráfico de malware, pueden proporcionar información sobre el posible comportamiento delictivo a futuro y ayudar en la detección de amenazas.

Casos destacados

La colaboración en el sector permite que Cisco neutralice la campaña de gran alcance y rentabilidad de los kits de ataque y el ransomware

El kit de ataque Angler es uno de los más grandes y eficaces del mercado. Se lo ha vinculado con diversas campañas de ransomware y publicidad maliciosa de alto perfil. Y ha sido un factor importante en la explosión general de la actividad de ransomware que nuestros investigadores de amenazas han estado supervisando de cerca en los últimos años. Los malhechores usan ransomware para cifrar los archivos de los usuarios y proporcionan la clave de descifrado solo después de que los usuarios pagan un "rescate", generalmente, de entre USD 300 a USD 500.

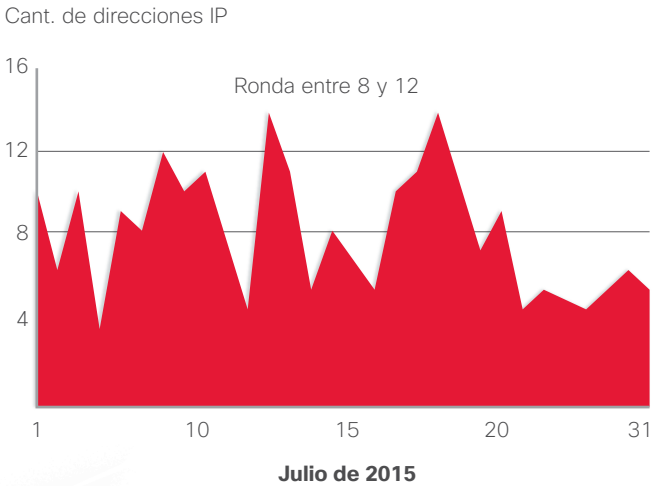
Como se explica en el Informe semestral de seguridad 2015 de Cisco, las criptomonedas como bitcoin y las redes de anonimato como Tor permiten que los atacantes ingresen en el mercado de malware de manera fácil y comiencen a generar ingresos rápidamente. El aumento de la popularidad del ransomware puede asociarse a dos ventajas principales: representa una operación de bajo mantenimiento para los artífices de amenazas y ofrece una forma rápida de rentabilización porque los usuarios les pagan a atacantes directamente en criptomonedas.

Mediante la investigación de Angler y de las tendencias afines de ransomware, Cisco determinó que algunos operadores del kit de ataque estaban usando un porcentaje exorbitante de servidores proxy mundiales para el kit Angler que estaban en servidores operados por Limestone Networks. Este uso del servidor es un claro ejemplo de otra tendencia que nuestros investigadores han estado observando recientemente en la economía informal: los artífices de amenazas están combinando recursos legítimos y maliciosos para realizar sus campañas.

En este caso, la infraestructura IP que respaldaba a Angler no era muy grande. Generalmente, la cantidad diaria ronda en 8 a 12 sistemas activos. La mayoría estuvo activo durante un solo día. En la Figura 1, se muestra la cantidad de direcciones IP únicas que Cisco observó en julio de 2015.

Cisco descubrió que, básicamente, los operadores de Angler pasaban secuencialmente de una dirección IP a otra para ocultar la actividad de amenazas y evitar cualquier interrupción de su proceso de enriquecimiento.

Figura 1. Cantidad de direcciones IP de Angler a la fecha, julio de 2015



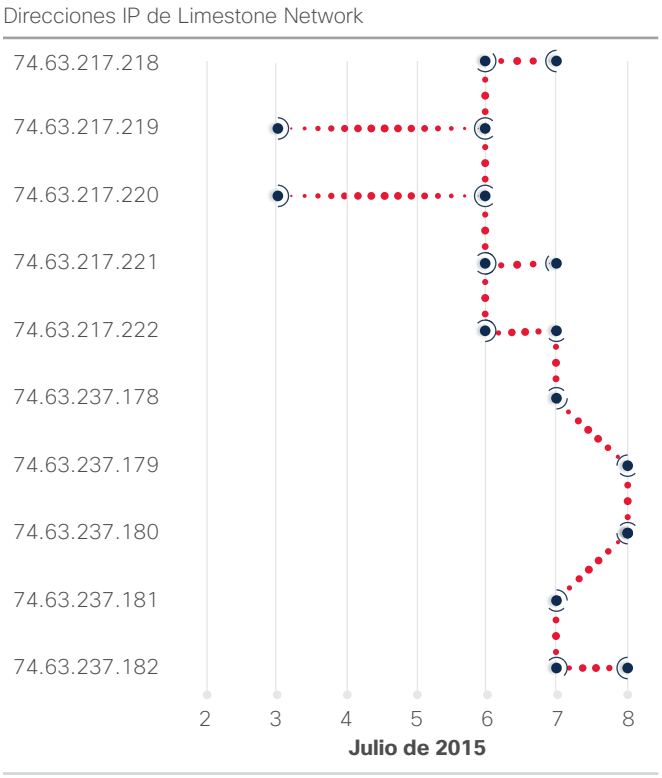
Fuente: Cisco Security Research

Como se ilustra en la Figura 2, Angler comienza con una dirección IP (en el ejemplo, 74.63.217.218). A medida que el sistema afecta a los usuarios y genera "ruido" que los defensores comienzan a detectar, los atacantes cambian a una dirección IP adyacente (74.63.217.219). Esta actividad continúa a través de bloques casi contiguos de espacio IP de un solo proveedor de alojamiento.

Cisco analizó la información IP para identificar los números de sistema autónomo (ASN) y los proveedores asociados con las direcciones IP. Determinamos que la mayoría del tráfico relacionado con Angler provenía de servidores operados por dos proveedores de alojamiento legítimos: Limestone Networks y Hetzner (Figura 3). Representaban casi el 75% del volumen de tráfico total del mes de julio.

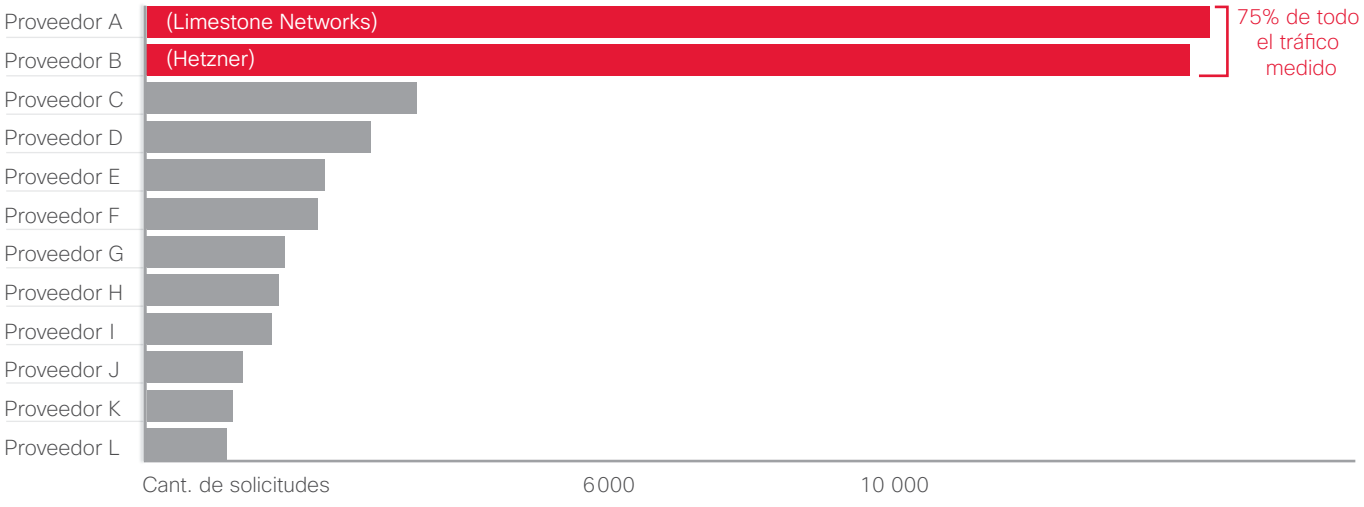
Cisco se comunicó primero con Limestone Networks, que, aparentemente, alojaba la porción global más grande de Angler. Limestone agradeció la oportunidad de colaborar. Las empresas habían estado lidiando con excesivas cancelaciones de pagos con tarjeta de crédito todos los meses porque los atacantes usaban nombres y tarjetas de crédito fraudulentas para comprar lotes aleatorios de sus servidores valuados en miles de dólares.

Figura 2. Baja infraestructura de IP que admite Angler



Fuente: Cisco Security Research

Figura 3. Solicitudes HTTP con Angler por proveedor, julio de 2015



Fuente: Cisco Security Research

El enfoque de los atacantes de comprar los servidores dificultaba asociar la actividad fraudulenta a un solo actor. Por ejemplo, un malhechor, tal vez, podía comprar tres o cuatro servidores en un solo día, y usar un nombre y una tarjeta de crédito diferentes para adquirir tres o cuatro servidores al día siguiente. De esta manera, en esencia, podía "rodar" de una dirección IP a la siguiente cuando los defensores identificaban los servidores comprometidos y los ponían fuera de línea.

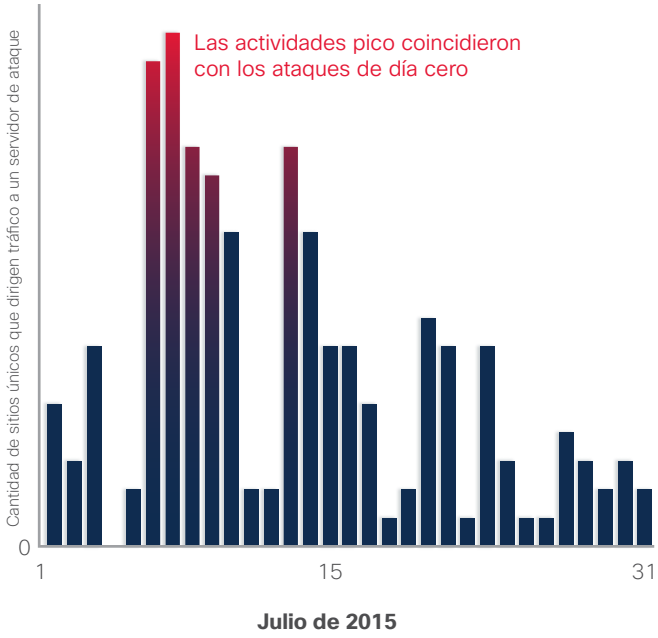
Para investigar esta actividad, Cisco obtuvo ayuda de Level 3 Threat Research Labs y de OpenDNS, una empresa de Cisco. Level 3 Threat Research Labs pudo brindar una mayor perspectiva global de la amenaza, lo que proporcionó a Cisco la capacidad de ver en mayor profundidad el alcance y la trascendencia de esta en su punto máximo. Por su parte, OpenDNS proporcionó una mirada única de la actividad del dominio asociada con la amenaza, lo que brindó a Cisco una comprensión más exhaustiva de cómo los atacantes estaban incorporando técnicas como ***domain shadowing*** (camuflaje de dominio).

Luego, los investigadores de amenazas de Cisco observaron, específicamente, cómo los usuarios daban con Angler y, posteriormente, recibían cargas maliciosas. Los investigadores detectaron que los usuarios eran redirigidos al kit de ataque Angler a través de publicidad maliciosa incluida en sitios web populares. Los anuncios falsos eran colocados en cientos de sitios importantes de noticias, bienes raíces y cultura popular. Estos tipos de sitio comúnmente se conocen en la comunidad de seguridad como sitios "buenos conocidos".

Además, los investigadores de amenazas de Cisco encontraron incontables ejemplos de sitios web pequeños y aparentemente aleatorios que hacían el mismo tipo de redireccionamiento, incluido el obituario de una persona en un periódico rural pequeño en los Estados Unidos. Es muy probable que esta última estrategia se diseñara para dirigirse a personas mayores. En general, es más probable que esta población use navegadores web predeterminados, como Microsoft Internet Explorer, y es menos probable que esté al tanto de la necesidad de revisar regularmente las vulnerabilidades de Adobe Flash.

Otro aspecto notable de esta operación de Angler era el volumen de sitios de referencia únicos y la baja frecuencia con la que se los usaba (Figura 4). Encontramos más de 15 000 sitios únicos que redirigían a las personas al kit de ataque Angler, de los cuales el 99,8% se usaba menos de 10 veces. Por lo tanto, la mayoría de los sitios de referencia estaban activos solo durante un breve lapso y se quitaban después de afectar a unos cuantos usuarios. En nuestro análisis de julio de 2015, notamos que los picos de actividad coincidieron con varios ataques de día cero de Hacking Team (CVE-2015-5119, CVE-2015-5122).[1]

Figura 4. Sitios de referencia únicos por día, julio de 2015

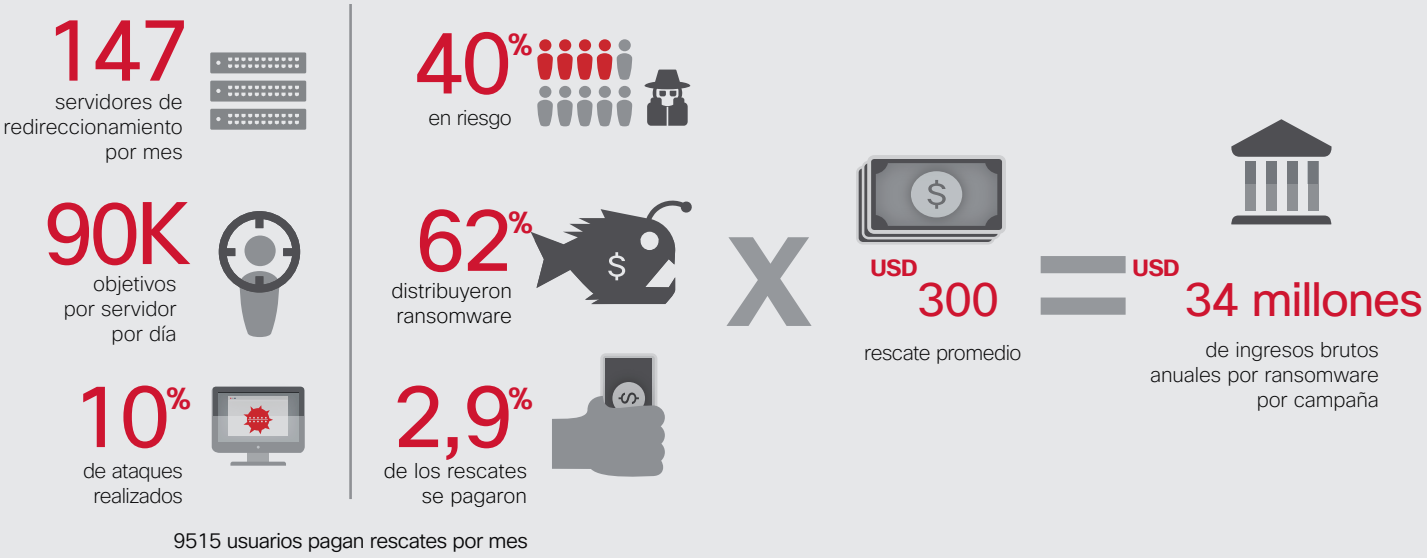


Fuente: Cisco Security Research

Cisco determinó que aproximadamente el 60% de las cargas dañinas de Angler distribuidas mediante esta operación específica introducían algún tipo de variante de ransomware, en la mayoría de los casos, Cryptowall 3.0. Otros tipos de cargas dañinas incluyen Bedep, un descargador de malware que se usa comúnmente para instalar malware de campañas de fraude mediante pago por clic. (Consulte "Las infecciones de navegadores se expanden y son una fuente importante de filtración de datos", **página 16**). Ambos tipos de malware están diseñados para que los atacantes extraigan mucho dinero a los usuarios en riesgo en forma rápida y con un nivel de esfuerzo bajo o nulo.

[1] "Adobe Patches Hacking Team's Flash Player Zero-Day" (Adobe aplica correcciones para prevenir los ataques de día cero a Flash Player de Hacking Team), de Eduard Kovacs, *SecurityWeek*, 8 de julio de 2015: **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day**.

Ingresos de Angler



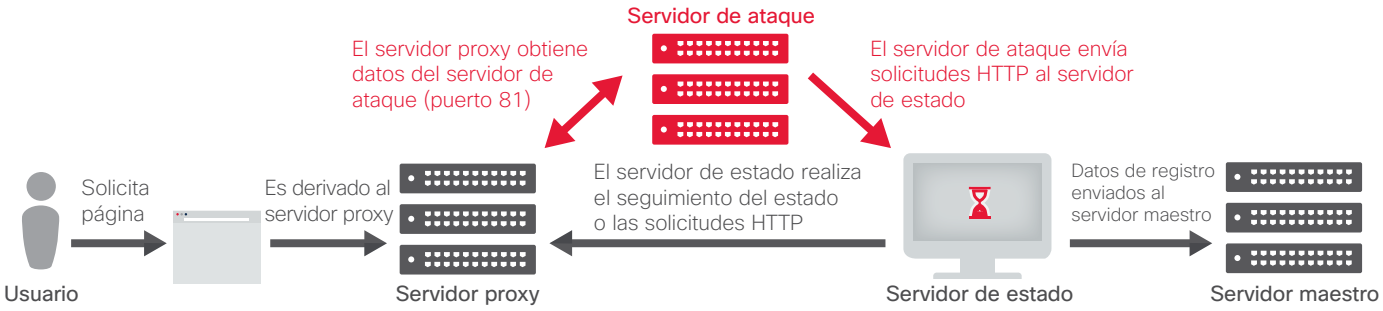
Fuente: Cisco Security Research

Según las investigaciones de Cisco, el principal actor responsable de alrededor de la mitad de la actividad del kit de ataque Angler en esta campaña en particular afectó a hasta 90 000 víctimas por día. Según nuestros cálculos, la campaña les dejaba a los atacantes una ganancia neta de más de USD 30 millones al año.

COMPARTIR

Probablemente, la red de Hetzner tuvo una tasa de éxito similar. Esto significa que el artífice de amenazas detrás de la operación que involucró a los servidores de Limestone Networks and Hetzner fue responsable de la mitad de toda la actividad global de Angler durante el análisis de Cisco. Los investigadores de Cisco calculan que esta operación fue capaz de generar ingresos brutos de USD 60 millones por año.

Figura 5. Infraestructura interna (back-end) de Angler



Fuente: Cisco Security Research

Cisco también descubrió que, en realidad, los servidores a los que los usuarios estaban conectados no alojaban ninguna de las actividades maliciosas de Angler. Servían como conductos. Los usuarios recibían la cadena de redireccionamiento y enviaban una solicitud GET para una página de acceso, que accedía al servidor proxy. El servidor proxy enrutaba el tráfico a un servidor de ataque en un país diferente, en un proveedor diferente. En nuestra investigación, descubrimos que un único servidor de ataque estaba asociado con diversos servidores proxy. (Consulte la Figura 5).

Cisco identificó un servidor de estado que administraba tareas como el monitoreo de estado. Cada servidor proxy único que el servidor de estado supervisaba tenía un par de URL únicas. Si la ruta era consultada, el servidor de estado devolvía un mensaje de código de estado HTTP "204". Los atacantes podían identificar en forma exclusiva cada servidor proxy y asegurarse de que no solo estuviera en funcionamiento, sino también que los defensores no lo hubieran manipulado. Con la otra URL, los atacantes podían recopilar los registros del servidor proxy y determinar el nivel de eficacia de la red.

La colaboración en el sector fue un componente fundamental en la capacidad de Cisco para investigar la actividad del kit de ataque Angler. En última instancia, permitió detener los redireccionamientos a los servidores proxy con Angler en un proveedor de servicios estadounidense y concientizar acerca de una operación de delito cibernético altamente sofisticada que estaba afectando a miles de usuarios todos los días.

Cisco trabajó estrechamente con Limestone Networks para identificar los nuevos servidores puestos en línea y controlarlos de cerca para asegurarse de que fuesen neutralizados. Poco después, los atacantes se alejaron de Limestone Networks y la actividad de Angler disminuyó globalmente.

Para obtener más información sobre cómo Cisco interrumpió un importante flujo de ingresos internacional generado por el kit de ataque Angler, lea la entrada del blog sobre seguridad de Cisco "**Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually from Ransomware Alone**" (Enfoque sobre amenazas: Cisco Talos frustra acceso a kit de ataque internacional masivo que genera USD 60 millones anuales solo por ransomware).

Los esfuerzos coordinados del sector ayudan a inutilizar uno de los botnets DDoS más grandes de Internet

Con frecuencia, las tecnologías integradas de defensa ante amenazas pueden detener ataques importantes antes de que afecten las redes empresariales. Sin embargo, en muchos casos, impedir un ataque potencialmente masivo requiere no solo defensas tecnológicas, sino también coordinación entre los proveedores de servicios, los proveedores de seguridad y los grupos del sector.

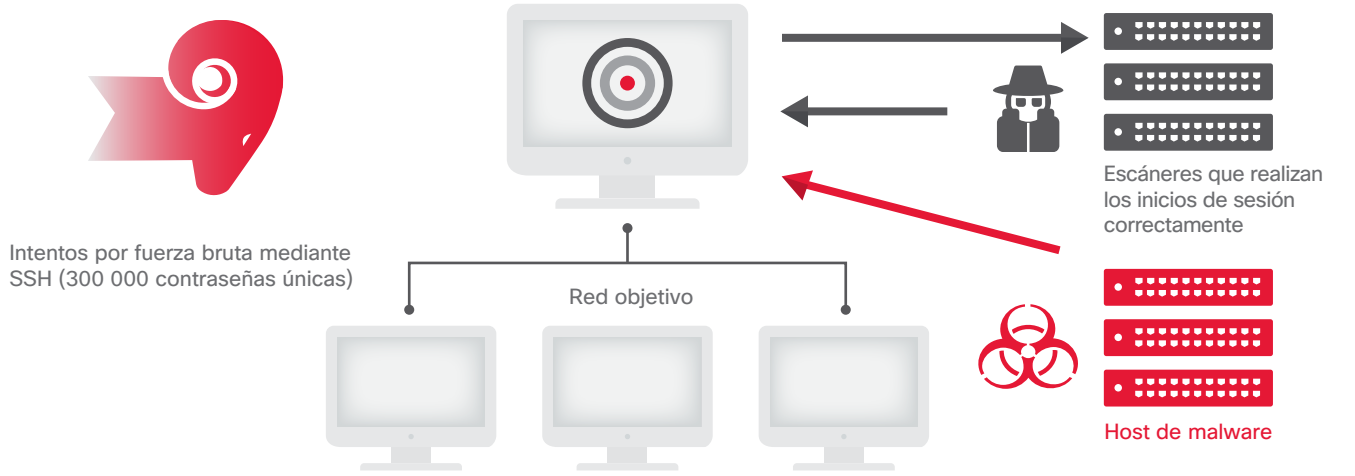
A medida que los delincuentes toman cada vez más en serio la rentabilización de sus actividades, el sector tecnológico debe hacer un mejor trabajo de asociación para anular las campañas delictivas. SSHPsychos (también denominado Group 93), uno de los botnets DDoS más grandes jamás observado por los investigadores de Cisco, fue debilitado en gran parte después de la colaboración de Cisco con Level 3 Threat Research Labs.

AMENAZA ÚNICA

La red de DDoS de SSHPsychos es una amenaza única por varios motivos. Dado que detalla decenas de miles de equipos distribuidos en Internet, tiene el poder de lanzar un ataque de denegación de servicio distribuido (DDoS) que no puede abordarse por dispositivo individual. En este caso, el botnet se creó mediante ataques de fuerza bruta que involucraban tráfico con Secure Shell (SSH) (Figura 6). El protocolo SSH se usa para posibilitar comunicaciones seguras, y suele usarse para la administración remota de sistemas. A veces, SSHPsychos representaba más del 35% de todo el tráfico SSH global de Internet (Figura 7), según el análisis de Cisco y Level 3.

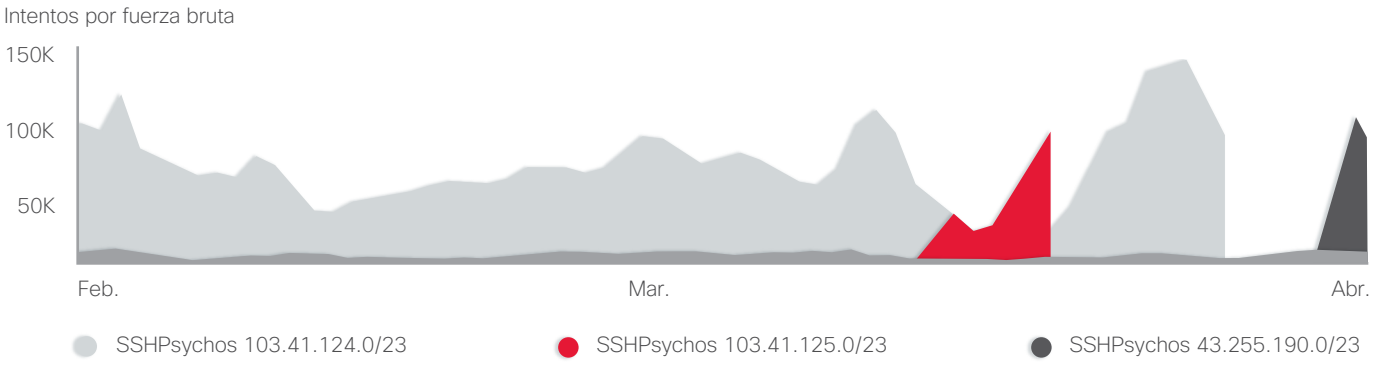
SSHPsychos funciona en dos países: China y los Estados Unidos. Los intentos de inicio de sesión por fuerza bruta, con 300 000 contraseñas exclusivas, procedían de un proveedor de alojamiento ubicado en China. Cuando los atacantes podían iniciar sesión tras adivinar la contraseña raíz correcta, los ataques de fuerza bruta cesaban. Veinticuatro horas más tarde, los atacantes iniciaban sesión desde una dirección IP estadounidense e instalaban un rootkit DDoS en la máquina afectada. Claramente, esto era una táctica para reducir la sospecha de los administradores de red. Los objetivos del botnet variaban, pero, en muchos casos, parecían ser grandes proveedores de servicios de Internet (ISP).

Figura 6. SSHPsychos usa ataques de fuerza bruta



Fuente: Cisco Security Research

Figura 7. En su pico máximo, SSHPsychos representó el 35% del tráfico mundial de Internet



Fuente: Cisco Security Research

COLABORACIÓN CON EXPERTOS EN SEGURIDAD

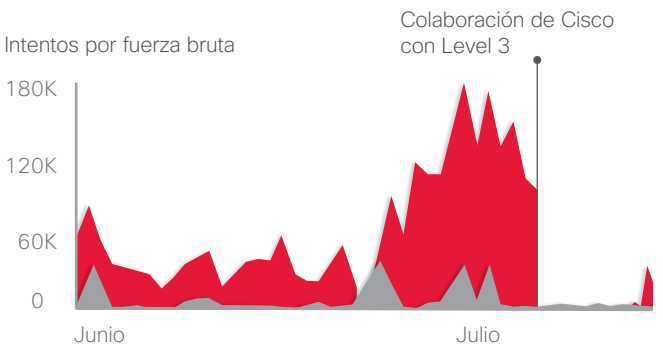
Dada la escala de la red de DDoS, nuestros investigadores creían que el daño sería difícil de contener. Era crucial trabajar junto con una organización que pudiera eliminar el grupo de fuerza bruta de Internet de manera eficaz. Sin embargo, los proveedores de redes troncales muestran reticencia a filtrar el contenido de sus clientes.

Cisco consultó a Level 3 Threat Research Labs. Level 3 analizó el tráfico en el ***netblock***, o rango de direcciones IP, donde se pensaba que podía residir SSHPsychos (103.41.124.0/23). Confirmó que en dicha dirección no se originaba ni se recibía ningún tráfico legítimo. Enrutó silenciosamente el tráfico de red dentro de sus propias redes. Luego se comunicó con los proveedores de servicios de los dominios relevantes para solicitarles que eliminaran el tráfico de la red.

Los resultados de esta iniciativa se observaron de inmediato (Figura 8). Casi no se detectó nueva actividad en la red original. Sin embargo, una nueva red en el netblock 43.255.190.0/23 mostró un gran volumen de tráfico de ataques de fuerza bruta mediante SSH. Tenía el mismo comportamiento asociado con SSHPsychos. Después de este nuevo surgimiento de tráfico del tipo de SSHPsychos, Cisco y Level 3 decidieron tomar medidas contra 103.41.124.0/23 y el nuevo netblock 43.255.190.0/23.

Neutralizar los netblocks usados por SSHPsychos no desactivó la red de DDoS en forma permanente. Sin embargo, ciertamente retrasó la capacidad de sus creadores para ejecutar sus operaciones y evitó que SSHPsychos se expandiera a nuevos equipos, al menos temporalmente.

Figura 8. El tráfico de SSHPsychos disminuye considerablemente después de la intervención



Fuente: Cisco Security Research

A medida que los ciberdelincuentes desarrollan grandes redes de ataque, el sector de seguridad debe explorar formas de colaboración cuando se enfrenta a una amenaza como SSHPsychos. Los proveedores de dominio de nivel superior, los ISP, los proveedores de alojamiento, los solucionadores de DNS y los proveedores de seguridad ya no pueden quedarse al margen cuando los delincuentes en línea lanzan sus ataques en redes diseñadas para transportar solo tráfico legítimo. En otras palabras, cuando los delincuentes distribuyen tráfico malicioso en lo que más o menos se considera " a simple vista", el sector debe eliminar las rutas maliciosas a estas redes legítimas.

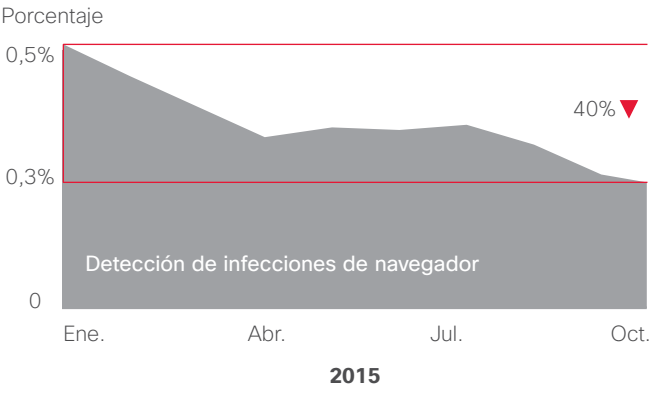
Para obtener más información sobre la respuesta de Cisco and Level 3 Threat Research Labs a la amenaza de SSHPsychos, lea la entrada del blog sobre seguridad de Cisco "**Threat Spotlight: SSHPsychos**" (Enfoque sobre amenazas: SSHPsychos).

Las infecciones de navegadores se expanden y son una fuente importante de filtración de datos

A menudo, los equipos de seguridad ven los complementos de navegador como una amenaza de poca gravedad. Sin embargo, deben establecer su supervisión con una prioridad más alta para poder identificar y solucionar rápidamente estos tipos de infecciones.

El motivo de la urgencia: nuestra investigación indica que las infecciones de navegador son mucho más frecuentes de lo que muchas organizaciones puedan creer. De enero a octubre de 2015, examinamos 26 familias de complementos de navegador maliciosos (Figura 9). Al mirar el patrón de infecciones de navegador durante estos meses, la cantidad de infecciones parecía estar en un descenso general.

Figura 9. Infecciones de navegadores, de enero a octubre de 2015



Fuente: Cisco Security Research

Sin embargo, este patrón es engañoso. El volumen creciente de tráfico HTTPS durante dichos meses no permitió identificar los indicadores de riesgo generalmente asociados con las 26 familias que examinamos, dado que la información de URL no podía verse por estar cifrada. (Para obtener más información sobre el cifrado y los desafíos que representa para los defensores, consulte "Cifrado: Una tendencia creciente y un desafío para los defensores", **página 30**).

Las extensiones de navegador maliciosas pueden robar información y pueden ser una fuente importante de filtración de datos. Cada vez que un usuario abre una página web nueva con un navegador afectado, las extensiones de navegador maliciosas recopilan datos. Exfiltran más que los detalles básicos acerca de cada página web interna o externa que visita el usuario. También recopilan información altamente confidencial integrada en la URL. Esta información puede incluir credenciales de usuario, datos de clientes, y detalles sobre la infraestructura y las API internas de una organización.

Las extensiones de navegador maliciosas multipropósito se distribuyen mediante adware o paquetes de software. Están diseñadas para obtener ingresos explotando a los usuarios de diversas maneras. En un navegador infectado, pueden guiar a los usuarios para que hagan clic en publicidad maliciosa, como anuncios publicitarios o ventanas emergentes. También pueden distribuir malware tentando a los usuarios a hacer clic en un enlace afectado o a descargar un archivo infectado incluido en una publicidad maliciosa. Además, pueden secuestrar las solicitudes de navegador de los usuarios e inyectar páginas web maliciosas en las páginas de resultados de los motores de búsqueda.

Considerando las 45 empresas de nuestra muestra, determinamos que, todos los meses, más del 85% de las organizaciones eran afectadas por extensiones de navegador maliciosas, un resultado que pone de relieve la escala masiva de estas operaciones. Dado que, a menudo, los navegadores infectados se consideran una amenaza relativamente menor, pueden pasar inadvertidos o quedar sin resolver durante días o incluso más, lo que les da a los atacantes más tiempo y la oportunidad de llevar a cabo sus campañas (consulte "Tiempo de detección: La carrera para seguir acortándolo", **página 60**).

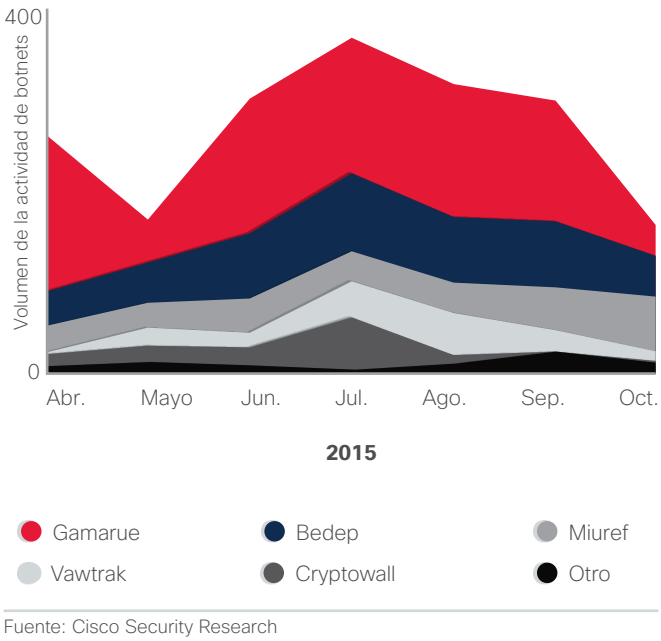
Por consiguiente, sugerimos que vale la pena que los equipos de seguridad dediquen tiempo y recursos a la supervisión de este riesgo y que consideren un aumento del uso de la automatización para priorizar las amenazas.

Comando y control mediante botnets: Una descripción general global

Los botnets son redes de computadoras infectadas con malware. Los atacantes pueden controlarlas en grupo y ordenarles que realicen una tarea específica, como enviar correo electrónico no deseado o iniciar un ataque DDoS. Han estado creciendo en tamaño y en cantidad por años. Para comprender mejor el panorama actual de amenazas a escala global, analizamos las redes de 121 empresas de abril a octubre de 2015 en busca de pruebas de uno o más de los ocho botnets comúnmente vistos. Los datos se normalizaron para proporcionar una descripción general de la actividad de los botnets (Figura 10).

Descubrimos que, durante este período, Gamarue –un programa de interceptación de información modular multipropósito, de unos cuantos años– era la amenaza más común de comando y control.

Figura 10. Crecimiento de las amenazas individuales (proporción de usuarios infectados)



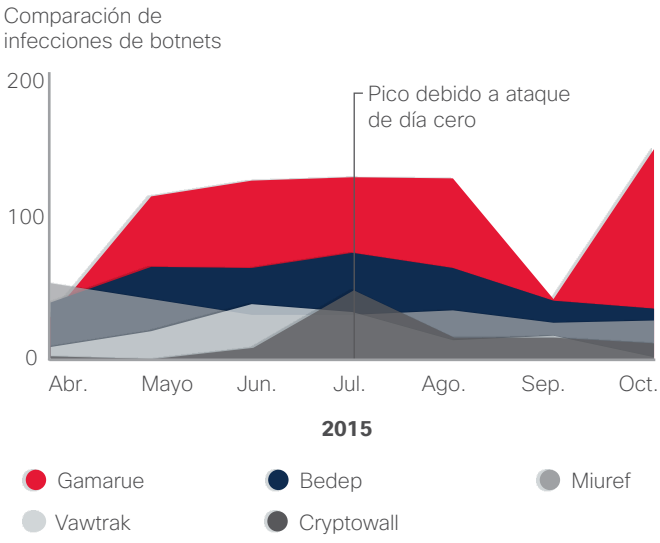
Fuente: Cisco Security Research

En julio, se identificó un pico significativo en la cantidad de infecciones que involucraban el ransomware Cryptowall 3.0. Esta actividad se atribuye en gran medida al kit de ataque Angler, que se conoce por distribuir la carga dañina de Cryptowall. Según se indicó en el Informe semestral de seguridad 2015 de Cisco, los autores de Angler y de otros kits de ataque han sido rápidos en atacar "brechas de revisión" con Adobe Flash, el tiempo entre el lanzamiento de una actualización de Adobe y el momento en que el usuario realmente aplica la actualización.[2] Los investigadores de amenazas de Cisco atribuyen el pico de julio de 2015 al ataque de día cero de Flash CVE-2015-5119 que se expuso como parte de las fugas de Hacking Team.[3]

El kit de ataque Angler también distribuye el troyano Bedep, que se usa para realizar campañas de fraude mediante pago por clic. Durante julio, también se observó un pico leve en la predominancia de esa amenaza (Figura 11).

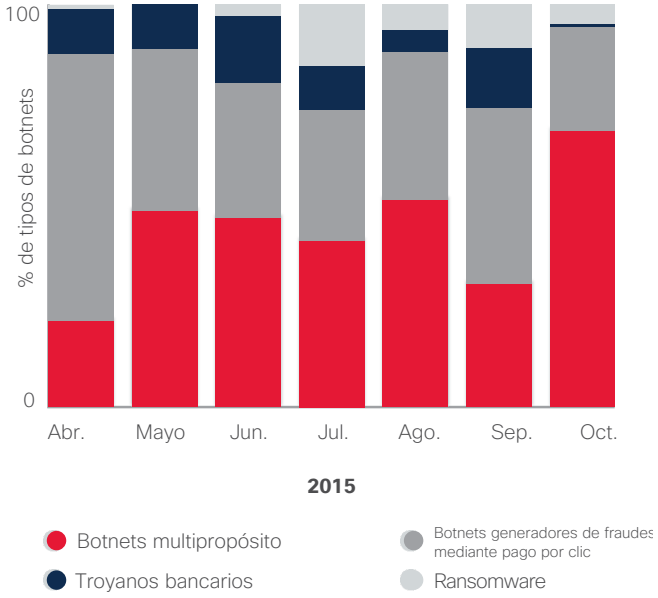
En forma conjunta, Bedep, Gamarue y Miuref (otro troyano y secuestrador de navegador que puede realizar fraudes mediante pago por clic) representaron más del 65% de la actividad de comando y control mediante botnets en la base de usuarios que analizamos.

Figura 11. Cobertura mensual de amenazas, según la cantidad de usuarios infectados



Fuente: Cisco Security Research

Figura 12. Cobertura mensual de amenazas, según la categorías de amenazas



Fuente: Cisco Security Research

El porcentaje de las infecciones de Bedep se mantuvo relativamente estable durante el período analizado. Sin embargo, se observó una disminución notable de las infecciones de Miuref. Atribuimos esto al aumento del tráfico HTTPS, que ayudó a ocultar los indicadores de riesgo de Miuref.

En la Tabla 12, se muestran los tipos de botnets responsables de la mayoría de las infecciones en el plazo bajo control. Los botnets multipropósito como Gamarue y Sality guiaban el paquete, seguidos de los botnets generadores de fraudes mediante pago por clic. Los troyanos bancarios ocupaban el tercer lugar, lo que muestra que, si bien es antiguo, este tipo de amenaza sigue siendo generalizada.

[2] Informe semestral de seguridad 2015 de Cisco: **http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html**.
[3] "Adobe Patches Hacking Team's Flash Player Zero-Day" (Adobe aplica correcciones para prevenir los ataques de día cero a Flash Player de Hacking Team), de Eduard Kovacs, *SecurityWeek*, 8 de julio de 2015: **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day.**

El punto ciego de DNS: Ataques mediante DNS para lograr comando y control

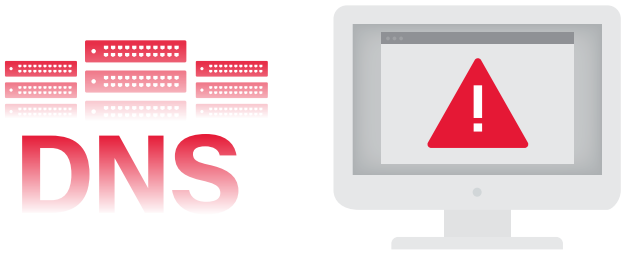
El análisis de malware validado como “malo conocido” de Cisco determinó que la mayor parte del malware (91,3%) usa el servicio de nombre de dominio de una de estas tres formas:

- Para obtener comando y control
- Para exfiltrar datos
- Para redireccionar el tráfico

Para llegar a este porcentaje, tomamos todos los comportamientos de muestra de una gran variedad de sandboxes que poseemos. El malware que se determinó que no usaba DNS de ninguna manera, o que solo lo usaba para realizar “verificaciones de estado” de Internet, se eliminó de la muestra para el análisis. El malware restante usaba DNS para conectarse a sitios validados como malos o considerados sospechosos.

Pese a la dependencia de los delincuentes en DNS para impulsar sus campañas de malware, pocas empresas monitorean DNS por motivos de seguridad (o ni siquiera lo hacen). Esta falta de supervisión convierte a DNS en una vía ideal para los atacantes. Según una encuesta reciente que realizamos (consulte la Figura 13), el 68% de los profesionales de seguridad informa que sus organizaciones no supervisan las amenazas de DNS recursivo. (Los servidores de nombres DNS recursivos proporcionan las direcciones IP de los nombres de dominio previstos a los hosts solicitantes).

Figura 13. Supervisión de amenazas de DNS recursivo



Fuente: Cisco Security Research

¿Por qué DNS es un punto ciego de seguridad para muchas organizaciones? Un motivo principal es que los equipos de seguridad y expertos en DNS generalmente trabajan en grupos de TI diferentes dentro de la empresa y no interactúan con frecuencia.

No obstante, deberían hacerlo. La supervisión de DNS es esencial para identificar y contener las infecciones de malware que ya están usando DNS para una de las tres actividades antes mencionadas. También es un primer paso importante en la asignación de otros componentes que pueden usarse para investigar aún más un ataque, desde determinar el tipo de infraestructura que respalda un ataque hasta encontrar su fuente.

La supervisión de DNS, sin embargo, implica más que la colaboración entre el equipo de seguridad y el equipo de DNS. Requiere hacer coincidir la experiencia y la tecnología correctas para el análisis de correlación. (Si desea más información, consulte “La colaboración en el sector permite que Cisco neutralice la campaña de gran alcance y rentabilidad de los kits de ataque y el ransomware” en la **página 10** para averiguar cómo OpenDNS ayudó a Cisco a adquirir más visibilidad de dominio respecto de las IP que el kit de ataque Angler estaba usando).

ANÁLISIS RETROSPECTIVO DE DNS

La investigación retrospectiva de Cisco de consultas de DNS y el subsiguiente tráfico de TCP y UDP identifica varias fuentes de malware. Esto incluye servidores de comando y control, sitios web y puntos de distribución. La investigación retrospectiva también detecta contenido de gran amenaza mediante la inteligencia proporcionada por listas de amenazas, informes de amenazas de la comunidad, tendencias observadas en riesgos cibernéticos y el conocimiento de las vulnerabilidades exclusivas del sector de un cliente.

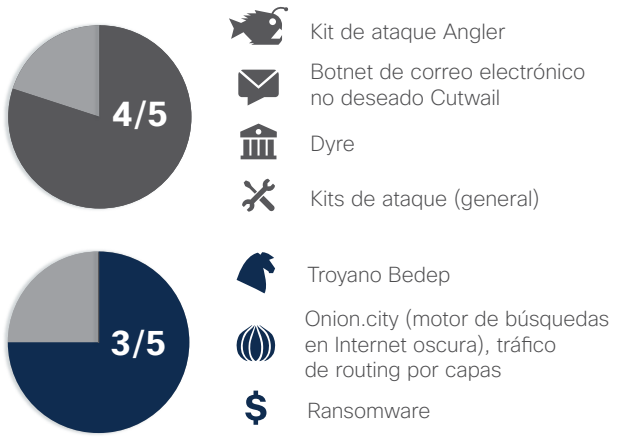
Nuestros informes retrospectivos permiten identificar intentos de exfiltración de datos de ocurrencia “baja y lenta” que están comúnmente asociados al comportamiento de amenazas persistentes avanzadas (APT) y que, en muchos casos, no pueden capturarse con las tecnologías tradicionales de detección de amenazas. El objetivo de este análisis es identificar anomalías en la gran cantidad de tráfico de comunicación saliente. Este enfoque “de adentro hacia afuera” permite detectar posibles riesgos de datos y actividad de red perjudicial que, de otra forma, probablemente serían pasados por alto.

Así es cómo hemos detectado que en las redes de clientes se estaban usando solucionadores de DNS "no autorizados". Los clientes no estaban al tanto de que sus empleados estaban usando los solucionadores como parte de su infraestructura de DNS. La falta de administración y supervisión activas del uso de solucionadores de DNS puede conllevar comportamiento malicioso como envenenamiento de caché DNS y redireccionamiento de DNS.

Además de detectar e identificar solucionadores de DNS "no autorizados", la investigación retrospectiva también ha descubierto los siguientes problemas en las redes de clientes:

- Espacio de direcciones del cliente encontrado en correo electrónico no deseado de terceros y listas de malware bloqueados
- Espacio de direcciones del cliente qué actúa como baliza de los conocidos servidores de comando y control Zeus y Palevo
- Campañas de malware activas, como CTB-Locker, Angler y DarkHotel
- Actividad sospechosa, incluido el uso de Tor, reenvío automático de correo electrónico y conversión de documentos en línea
- Tunelización generalizada de DNS a dominios registrados en China
- "Typosquatting" (error tipográfico deliberado) de DNS[4]
- Clientes internos que saltean la infraestructura de confianza de DNS del cliente

Después de analizar una muestra selecta de clientes de inteligencia de amenazas personalizada de Cisco de diversos mercados verticales, también encontramos los siguientes tipos de malware en el porcentaje respectivo del total de clientes examinado:



[4] Typosquatting es el acto de registrar un nombre de dominio que es similar a un nombre de dominio existente; es la estrategia que usan los atacantes para focalizarse en usuarios que, involuntariamente, escriben mal los nombres de dominio previstos.

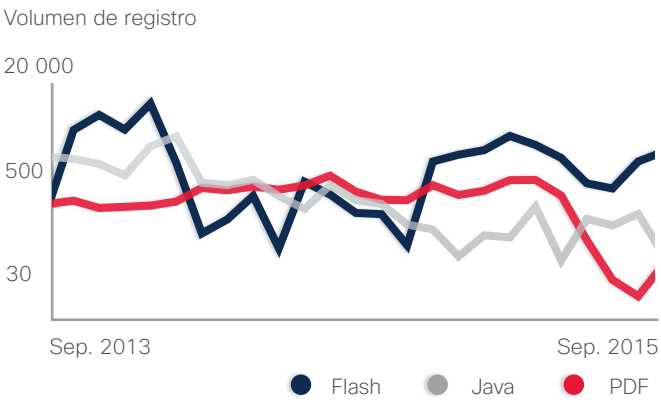
Análisis de inteligencia de amenazas

Vectores de ataque web

ADOBE FLASH: UNA HERRAMIENTA OBSOLETA, TARDE O TEMPRANO

Pese a que el volumen general de Flash ha disminuido en el último año (consulte la siguiente sección, **"Tendencias del contenido de Adobe Flash y PDF"**), sigue siendo una herramienta favorita entre los desarrolladores de kits de ataque. De hecho, en 2015, no hubo una tendencia clara de aumento o descenso del malware basado en Flash (Figura 14). Probablemente, el malware relacionado con Flash siga siendo un vector de ataque principal durante un tiempo: cabe mencionar que los autores del kit de ataque Angler apuntan en gran medida a las vulnerabilidades de Flash.

Figura 14. Porción de vectores de ataque, comparación de dos (2) años



Fuente: Cisco Security Research

La presión del sector para eliminar Adobe Flash de la experiencia de navegación está conduciendo a una disminución de la cantidad de contenido Flash en la Web (consulte la sección siguiente, **"Tendencias del contenido de Adobe Flash y PDF"**). Esto es similar a lo que se viene viendo con el contenido Java en los últimos años y lo que, a su vez, ha dado lugar a una constante tendencia descendente en el volumen de malware de Java (de hecho, los autores de Angler ya ni siquiera se molestan en incluir ataques de Java). Mientras tanto, el volumen de malware de PDF se ha mantenido bastante constante.

Microsoft Silverlight también se redujo como vector de ataque, porque muchos proveedores han dejado de admitir la API que usa Silverlight para integración en los navegadores. Muchas empresas se están alejando de Silverlight y están adoptando las tecnologías basadas en HTML5. Microsoft ha indicado que no hay una nueva versión de Silverlight en el horizonte y, actualmente, solo está lanzando actualizaciones relacionadas con la seguridad.

TENDENCIAS DEL CONTENIDO DE ADOBE FLASH Y PDF

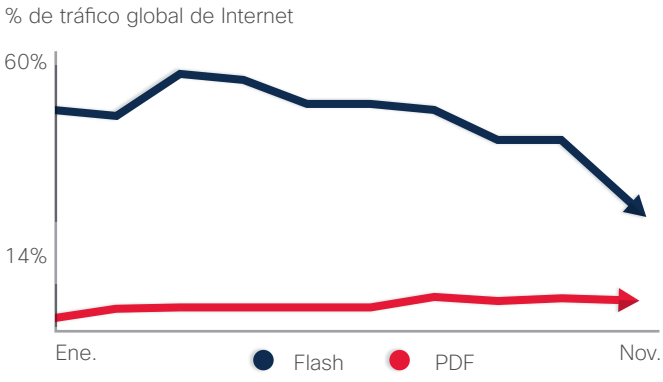
Los investigadores de Cisco han estado observando una disminución general en la cantidad de contenido de Adobe Flash en la Web (Figura 15). Las acciones recientes de Amazon, Google y otras grandes empresas en el espacio de Internet son un factor de la disminución del contenido Flash. Estas empresas dejaron de aceptar la publicidad web que usa Flash o la bloquean.

Por su parte, el contenido de PDF se mantuvo bastante estable durante el último año y, probablemente, así siga. Sin embargo, hace tiempo que dejó de ser un vector de ataque web importante.

Es probable que, ahora que Adobe anunció que eliminará Flash gradualmente, la disminución del contenido de Flash continúe, incluso, se acelere.[5] No obstante, posiblemente pase tiempo antes de que el contenido de Flash desaparezca. Flash está integrado en navegadores como Google Chrome, Microsoft Internet Explorer y Microsoft Edge, y aún se usa ampliamente en el contenido web, incluido el contenido de video y juegos.

Sin embargo, en los próximos años, a medida que se adopten nuevas tecnologías (como HTML5 y las plataformas móviles), la tendencia a largo plazo de vectores de ataque web como Java, Flash, y Silverlight será cada vez más clara. Con el tiempo, serán menos frecuentes. Por lo tanto, probablemente sean vectores mucho menos atractivos para los atacantes orientados a las ganancias que se centran en vectores que les permiten poner en riesgo a grandes poblaciones de usuarios y generar ingresos rápidamente.

Figura 15. Porcentaje del tráfico total para Flash y PDF

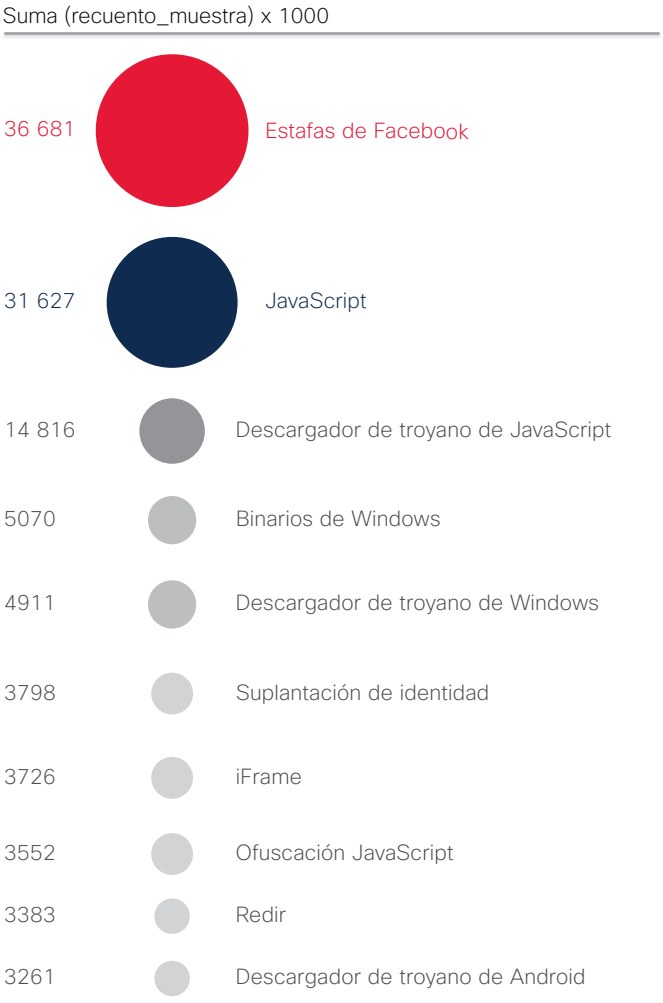


Fuente: Cisco Security Research

Métodos de ataque web

En las Figuras 16 y 17 se muestran los distintos tipos de malware que usan los adversarios para acceder a las redes de las organizaciones. En la Figura 16, se ilustra el malware que se ve con mayor frecuencia: adware, spyware, redireccionadores maliciosos, ataques de iFrame y suplantación de identidad.

Figura 16. Malware más comúnmente observado



Fuente: Cisco Security Research

[5] "Adobe News: Flash, HTML5 and Open Web Standards" (Adobe News: Flash, HTML5 y estándares de web abiertos), Adobe, 30 de noviembre de 2015: **http://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html.**

La Figura 16 puede verse básicamente como una recopilación de los tipos de malware que usan los delincuentes para obtener el acceso inicial. Son los métodos comprobados y más rentables para poner en riesgo a grandes grupos de usuarios con relativa facilidad. Los ataques de JavaScript y las estafas de Facebook (ingeniería social) fueron los métodos de ataque que se usaron con mayor frecuencia, según nuestra investigación.

En la figura 17, se muestra el malware de menor volumen. Tenga en cuenta que un "volumen más bajo" no significa "menos eficaz". De acuerdo con Cisco Security Research, el malware de menor volumen puede representar amenazas emergentes o campañas altamente focalizadas.

Muchas de estas técnicas más sofisticadas están diseñadas para extraer tanto valor como sea posible de los usuarios en riesgo. Roban datos de alto valor o secuestran los activos digitales de los usuarios para exigir un rescate.

Por lo tanto, al monitorear el malware web, no es suficiente enfocarse solo en los tipos de amenazas más comúnmente observadas. Debería considerarse el espectro de ataques completo.

Figura 17. Muestra de malware de bajo volumen observado

Fuente: Cisco Security Research

Actualizaciones de amenazas

LISTA DE LAS PRINCIPALES VULNERABILIDADES DE ADOBE FLASH

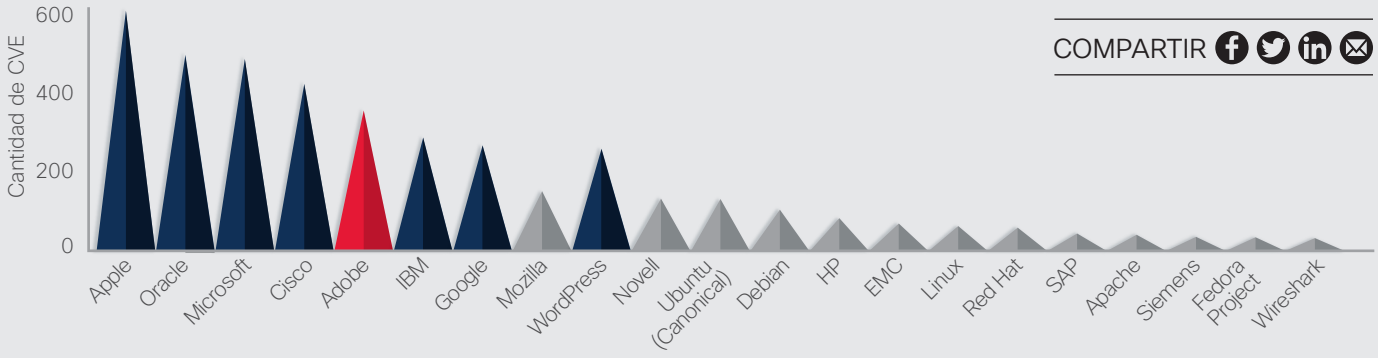
La plataforma de Adobe Flash ha sido un vector de amenazas popular para los delincuentes durante varios años. Las vulnerabilidades de Flash aún aparecen con frecuencia en listas de alertas de extrema urgencia. En 2015, la buena noticia fue que los proveedores de productos en los que comúnmente ocurrían estos ataques, como los navegadores web, reconocieron esta debilidad y ahora están tomando medidas para recortarles las oportunidades a los atacantes.

En 2016, lo más probable es que los delincuentes centren sus ataques en los usuarios de Adobe Flash. Algunas de estas vulnerabilidades Flash tienen ataques disponibles en línea públicamente o a la venta como parte de kits de ataque. (Como se mencionó en la **página 21**, el volumen de contenido relacionado con Flash disminuyó, pero Flash sigue siendo un vector de ataque principal).

Si consideramos las tácticas usadas para reducir el impacto de Java –otro vector común de ataque–, muchos navegadores web bloquean o aíslan Flash mediante sandboxes como una forma de proteger a los usuarios. Si bien este es un desarrollo positivo, es importante recordar que los atacantes aún tendrán éxito en el lanzamiento de ataques durante algún tiempo. Tal vez los usuarios no actualicen sus navegadores según sea necesario, y los delincuentes seguirán lanzando ataques dirigidos a las versiones antiguas de software de navegador.

Sin embargo, los investigadores de Cisco creen que las protecciones que ahora están incorporadas en algunos de los navegadores web y sistemas operativos de uso general reducirán la dependencia de Flash por parte de los delincuentes. Dado que los atacantes en línea se centran en lograr los mejores resultados posibles (por ejemplo, alta rentabilidad) con la mayor eficacia, dedicarán escasos esfuerzos a los ataques menos propensos a ofrecer un retorno de la inversión.

Figura 18. Cantidad total de CVE por proveedor



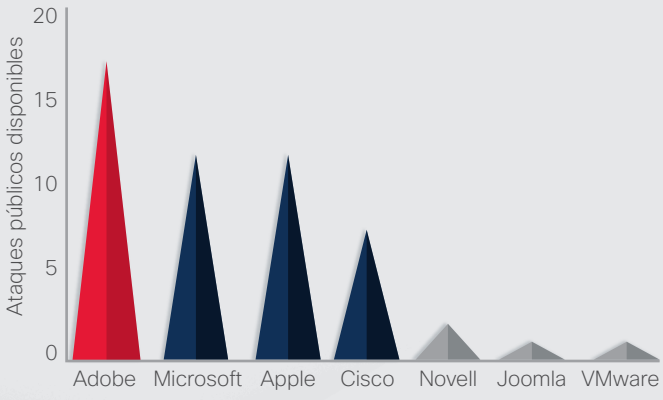
Fuente: Cisco Security Research, Base de Datos de Vulnerabilidades de los Estados Unidos (National Vulnerability Database, NVD)

En el gráfico anterior se muestra la cantidad total de vulnerabilidades y exposiciones comunes (CVE) publicadas en 2015 por proveedor. Nótese que Adobe no es tan destacado en este gráfico como en el gráfico de la derecha, que muestra las vulnerabilidades para las que hay ataques disponibles.

Además, WordPress muestra solo 12 vulnerabilidades para 2015 para su propio producto. Las 240 vulnerabilidades adicionales provienen de complementos y scripts creados por colaboradores externos.

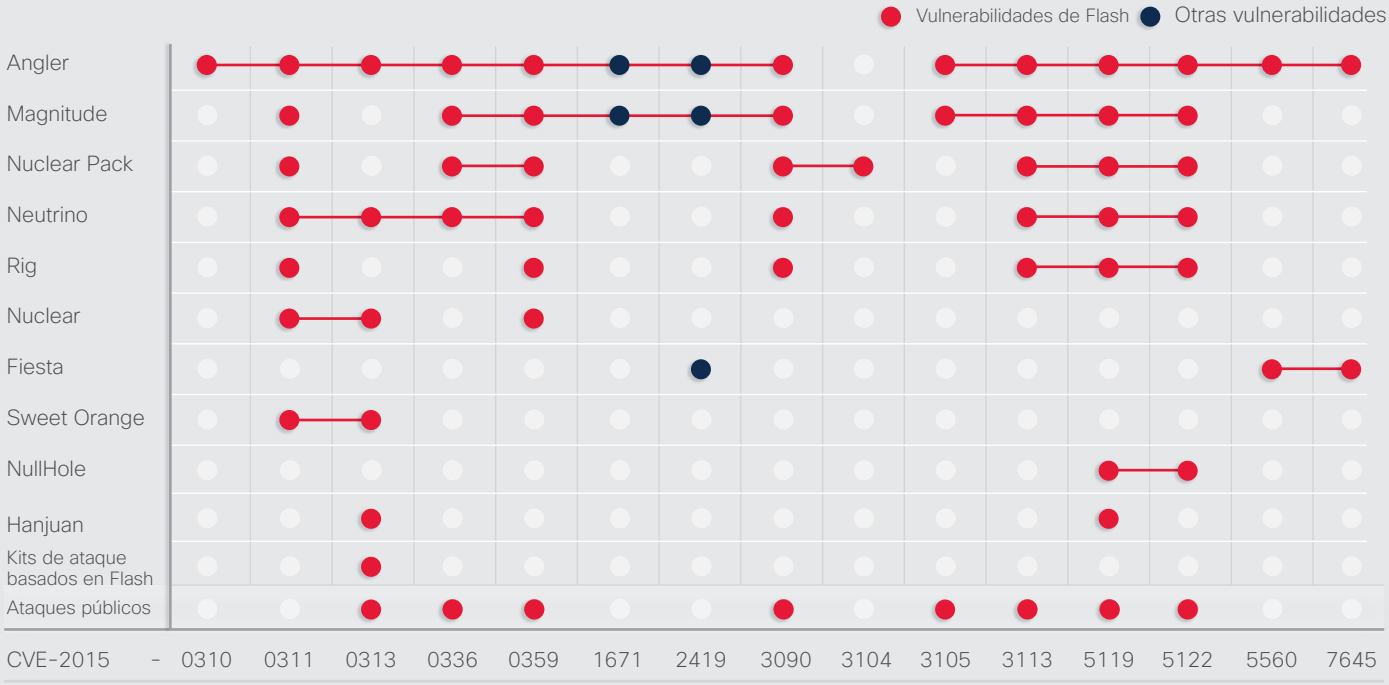
Como se observa en la Figura 20, las listas de vulnerabilidades y ataques relacionados pueden brindar orientación a los profesionales de seguridad. Estos pueden administrar y priorizar las vulnerabilidades de alto riesgo y más comunes, y revisarlas más rápidamente que a las vulnerabilidades de bajo riesgo. Visite el sitio web CVE Details **(https://www.cvedetails.com/top-50-products.php)** para obtener más información sobre las CVE por proveedor.

Figura 19. Cantidad de ataques públicos disponibles por vulnerabilidad del proveedor



Fuente: Cisco Security Research, Metasploit, base de datos de ataques

Figura 20. Vulnerabilidades comunes



Fuente: Cisco Security Research

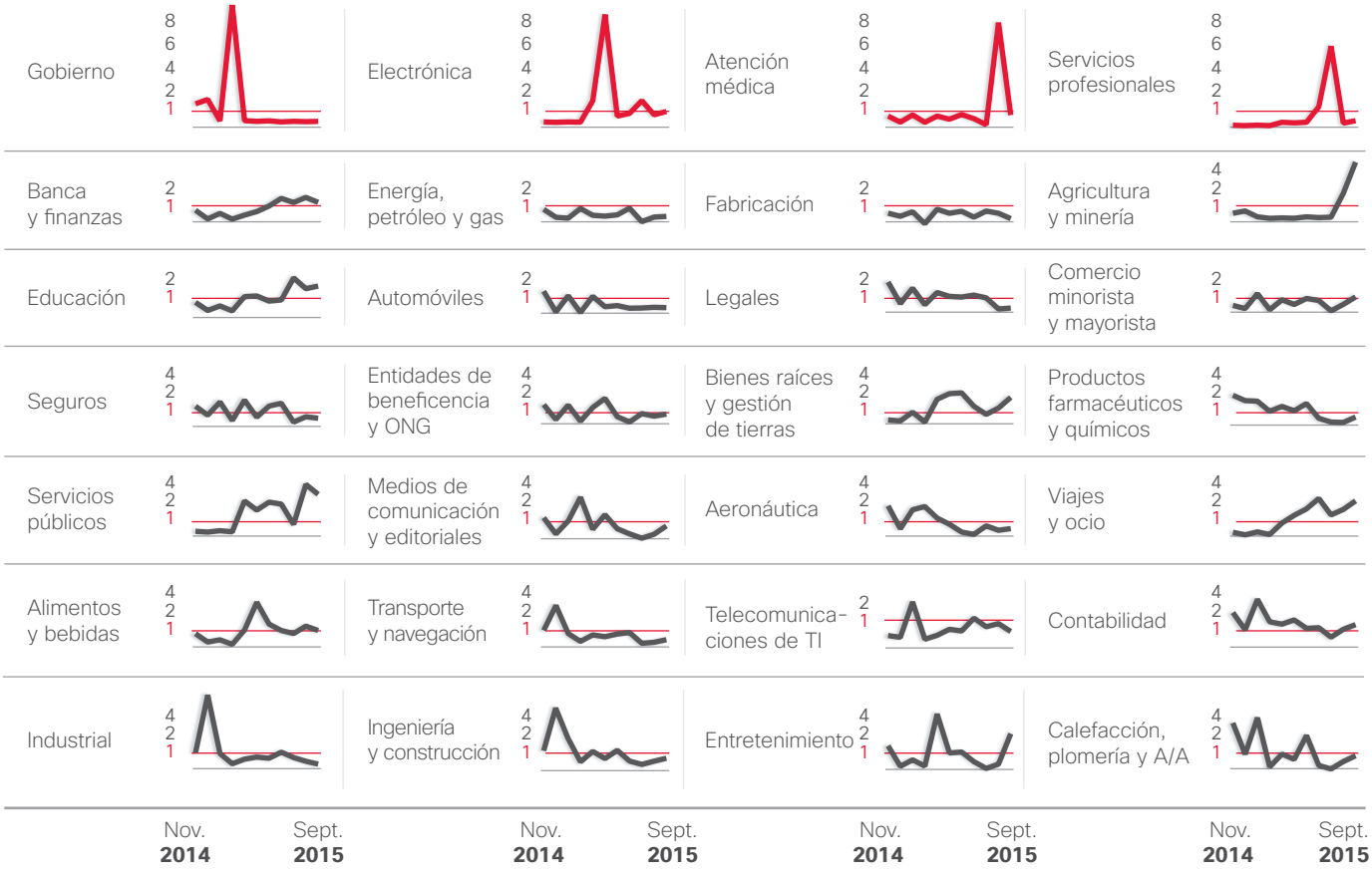
En la Figura 20, se muestran vulnerabilidades de alto riesgo y se indica si la vulnerabilidad es parte de un kit de ataque realizado por encargo (consulte la línea “Kits de ataque basados en Flash”) o tiene ataques de público conocimiento (consulte la línea “Ataques públicos”). Las vulnerabilidades para las que hay ataques funcionales representan una alta prioridad de revisión. Esta lista se puede usar para ayudar a los profesionales de seguridad a priorizar sus actividades de revisión y corrección. La existencia de un ataque para un producto dado –públicamente o dentro de un kit de ataque– no indica necesariamente que estén ocurriendo ataques.

Riesgo de hallazgos de malware en mercados verticales

Para realizar el seguimiento de mercados de alto riesgo en busca de hallazgos de malware, examinamos los volúmenes relativos del tráfico de ataque ("tasas de bloqueo") y del tráfico "normal" o esperado.

En la Tabla 21 se muestran las 28 industrias principales y su actividad de bloqueo relativa como una proporción del tráfico de red normal. Una proporción de 1.0 significa que el número de bloqueos es proporcional al volumen del tráfico observado. Cualquier proporción por encima de 1.0 representa tasas de bloqueo superiores a lo esperado y cualquier proporción por debajo de 1.0 representa tasas de bloqueo inferiores a lo esperado.

Figura 21. Tasas de bloqueo mensuales de mercados verticales, de noviembre de 2014 a septiembre de 2015

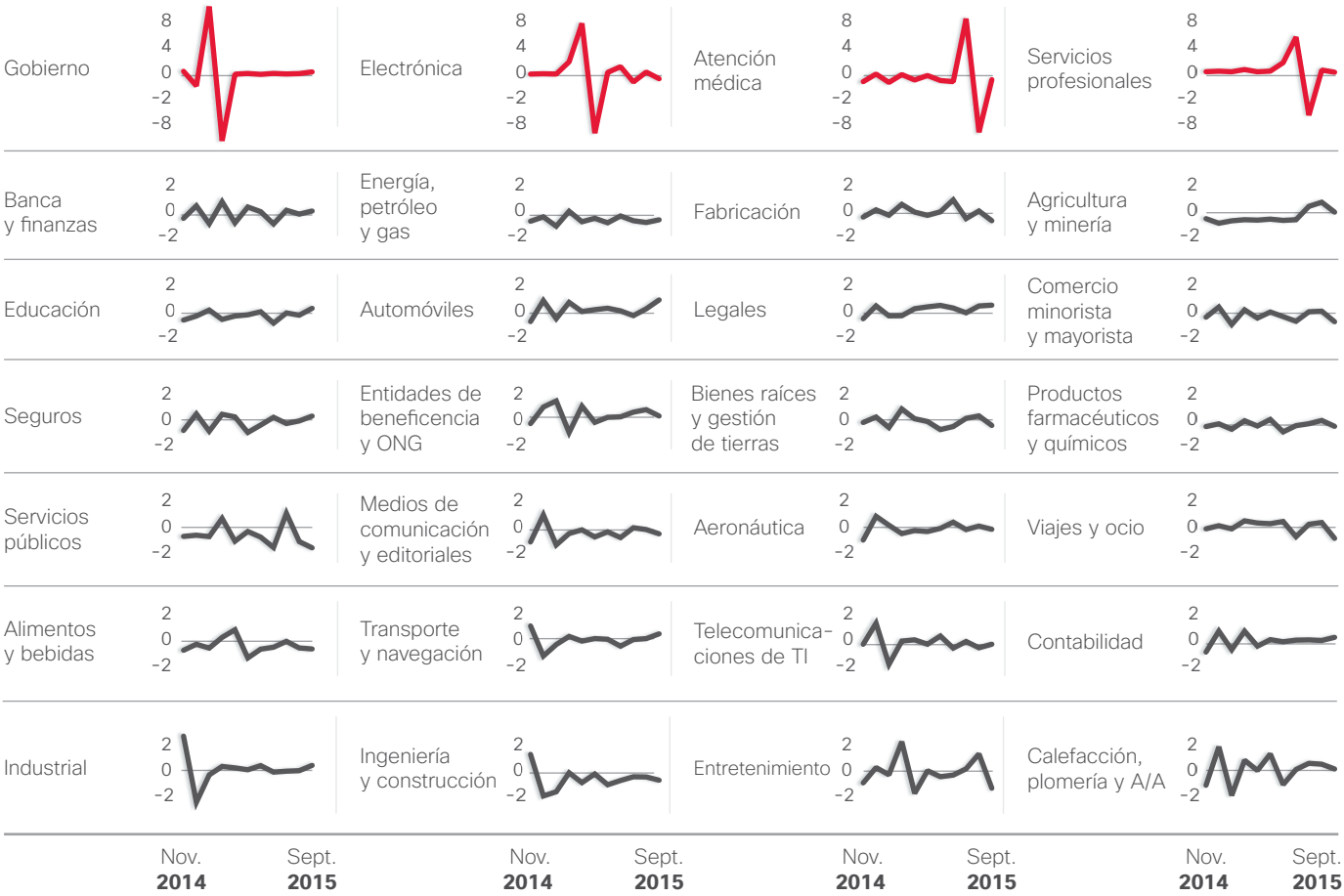


Fuente: Cisco Security Research

En la Figura 22, se muestra cómo el enfoque de los atacantes en mercados verticales específicos puede ser fugaz. (El cero no representa ningún cambio neto). De enero a marzo de 2015, el gobierno fue el mercado vertical con la actividad de tasa de bloqueo más alta. De marzo a mayo, fue el sector de la electrónica. En pleno verano, la mayor parte de los bloqueos ocurrió en el área de los servicios profesionales. Y en el otoño de 2015, los servicios de salud ocupaban el primer puesto de todos los mercados verticales en la cantidad de tasas de bloqueo.

Según nuestra investigación, los cuatro mercados verticales con la mayor parte de la actividad de bloqueo en 2015 fueron objetivo de ataques relacionados con troyanos. El mercado vertical del gobierno también debió enfrentar un gran número de ataques de inyección PHP, en tanto que el sector de servicios profesionales fue asolado con una gran cantidad de ataques de iFrame.

Figura 22. Tasas de bloqueo relativas de mercados verticales, comparación mes a mes



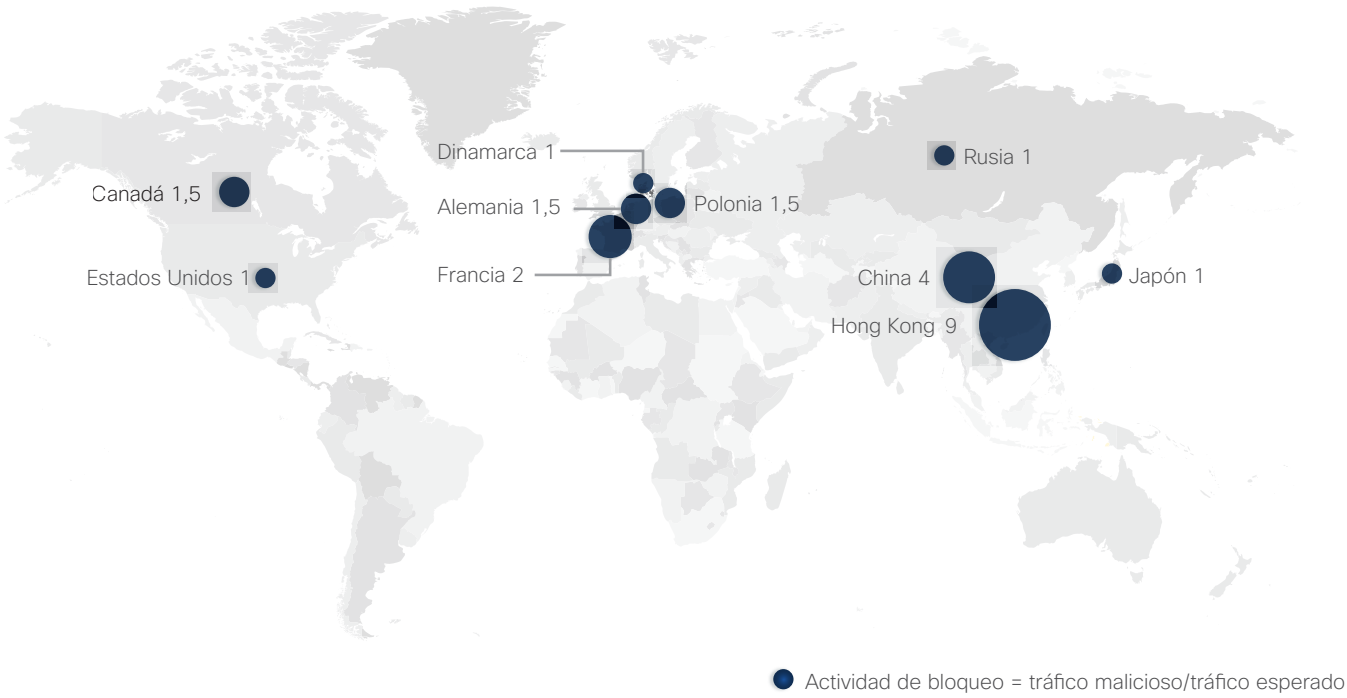
Fuente: Cisco Security Research

Actividad de bloqueo web: Descripción general geográfica

También examinamos dónde se origina la actividad de bloqueo basada en malware por país o región, como se observa en la Figura 23. Los países para el estudio se seleccionaron según el volumen de tráfico de Internet. Un valor de "proporción de bloqueo" de 1.0 indica que el número de bloqueos observados es proporcional al tamaño de la red.

Los países y las regiones con actividad de bloqueo que consideramos superior a lo normal probablemente tengan muchos servidores web y hosts con vulnerabilidades no corregidas en sus redes. Los actores maliciosos no respetan las fronteras de los países y alojarán malware donde sea más eficaz.

Figura 23. Bloqueos web por país o región



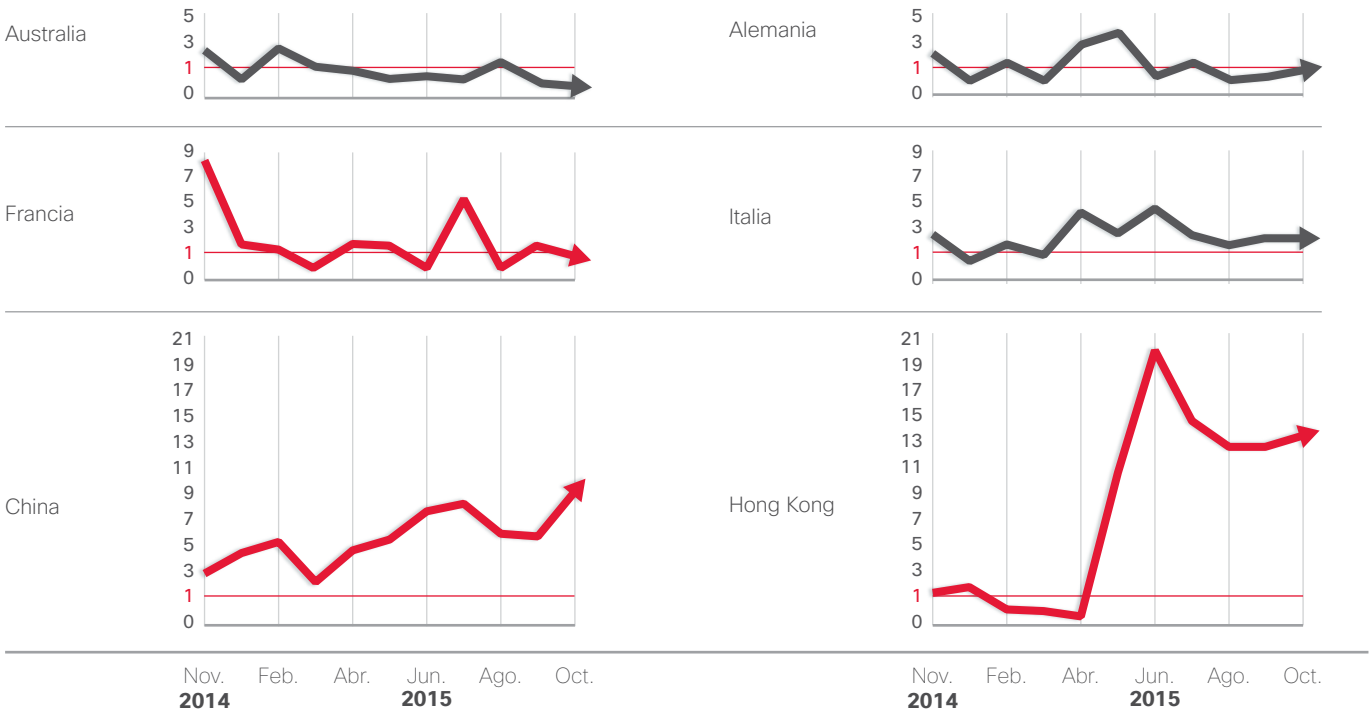
Fuente: Cisco Security Research

Una presencia en redes grandes y comercialmente viables que administran un alto volumen de Internet es otro factor para que la actividad de bloqueo sea alta, razón por la cual Hong Kong encabeza nuestra lista.

En la Figura 24, donde se muestra una comparación mes a mes de los bloqueos web por país o región desde noviembre de 2014 hasta octubre de 2015, se ofrece cierto contexto adicional para estas clasificaciones.

Nótese que Hong Kong tuvo una actividad de bloqueo web más alta de lo normal en la primavera de 2015, al igual que Francia. Desde entonces, ambos países han experimentado una disminución considerable en la actividad de bloqueo web; sin embargo, debido a que las tasas de actividad más altas a principios de este año estuvieron muy por encima de la referencia, la disminución reciente en la actividad aún deja a Hong Kong situado bastante más arriba para fin de año. El pico en la actividad de bloqueo en Francia volvió a los niveles normales en el verano.

Figura 24. Bloqueos web por país o región, mes a mes, de noviembre de 2014 a octubre de 2015



Fuente: Cisco Security Research

Perspectiva del sector

Perspectivas del sector

Cisco proporciona investigación y análisis de tendencias y prácticas de seguridad. Paradójicamente, algunas de estas pueden dificultar la capacidad de los defensores para realizar un seguimiento de las amenazas y poner a las organizaciones y a los usuarios individuales en un mayor riesgo de peligro y ataque.

Cifrado: una tendencia creciente, y un desafío para los defensores

El cifrado tiene sentido. Las empresas necesitan proteger la propiedad intelectual y otros datos confidenciales, los anunciantes desean preservar la integridad del contenido de sus anuncios y de sus análisis de back-end, y los negocios están prestando especial interés a la protección de la privacidad de sus clientes.

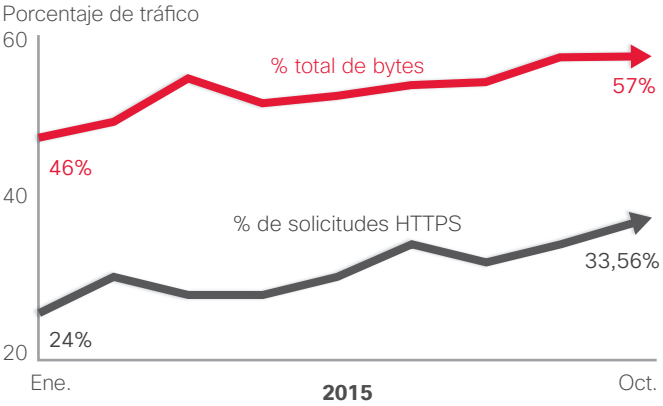
Pero el cifrado también plantea problemas de seguridad para las organizaciones, incluida una falsa sensación de seguridad. Las organizaciones mejoraron mucho el cifrado de datos cuando estos se transmiten entre entidades, pero los datos almacenados a menudo quedan desprotegidos. Muchas de las vulnerabilidades más importantes que se produjeron en los últimos años aprovecharon los datos sin cifrar almacenados en el centro de datos y en otros sistemas internos. Para los atacantes, esto es como seguir un camión de suministro seguro a un depósito abierto.

También es importante que las organizaciones comprendan que el cifrado integral puede disminuir la eficacia de algunos productos de seguridad. El cifrado oculta los indicadores de riesgo que se utilizan para identificar la actividad maliciosa y realizar un seguimiento de esta.

Pero no hay excusa para dejar datos confidenciales sin cifrar. Las herramientas de seguridad y sus operadores deben adaptarse a este nuevo y desafiante mundo. Para ello, deben recopilar encabezados y otras partes no cifradas del flujo de datos, sumadas a otras fuentes de información contextual a fin de analizar el tráfico cifrado. Las herramientas que dependen de la visibilidad de la carga útil, como la captura completa de paquetes, son cada vez menos eficaces. Ejecutar Cisco NetFlow y otros análisis basados en metadatos es actualmente indispensable.

Al observar las tendencias de 2015, nuestros investigadores sugieren que el tráfico cifrado, en particular HTTPS, alcanzó un punto crítico. Aunque aún no abarca la mayoría de las transacciones, pronto se convertirá en la forma predominante de tráfico en Internet. De hecho, en nuestra investigación se muestra que ya representa sistemáticamente más del 50% de bytes transferidos (Figura 25) debido a la sobrecarga de HTTPS y a un mayor contenido que se envía a través HTTPS, como las transferencias a sitios de almacenamiento de archivos.

Figura 25. Porcentajes de SSL



Fuente: Cisco Security Research

Para cualquier transacción web, se envían (salientes) y se reciben (entrantes) varios bytes. Las transacciones HTTPS tienen mayores solicitudes salientes que las solicitudes salientes del protocolo HTTP (aproximadamente 2000 bytes adicionales). Sin embargo, las solicitudes entrantes de HTTPS también tienen una sobrecarga, pero estas se vuelven menos importantes con mayores respuestas.

Al combinar los bytes entrantes con los salientes en una transacción web, podemos determinar el porcentaje total de todos los bytes involucrados en la transacción web que se cifran mediante HTTPS. Debido al aumento del tráfico HTTPS y la sobrecarga adicional, determinamos que los bytes HTTPS representaron el 57% de todo el tráfico web en octubre de 2015 (Figura 25), un valor superior al 46% registrado en enero.

Mediante el análisis de tráfico web, también determinamos que las solicitudes HTTPS han aumentado de forma gradual, pero considerablemente, desde enero de 2015. Como se muestra en la Figura 25, el 24% de las solicitudes de enero utilizaron el protocolo HTTPS; el resto de ellas utilizó el protocolo HTTP.

En octubre, el 33,56% de las solicitudes observadas eran HTTPS. Además, descubrimos que el porcentaje de bytes entrantes de HTTPS aumentó. Este fue el caso durante todo el año. A medida que la cantidad de tráfico mediante HTTPS aumenta, se requiere más ancho de banda. Se requieren 5 Kbps adicionales por transacción.

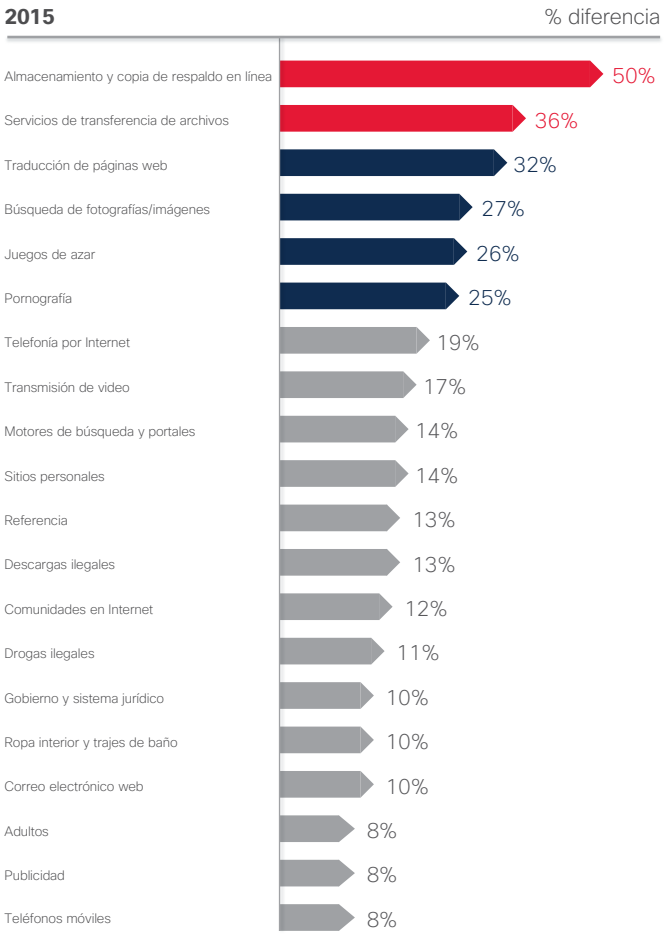
Atribuimos el aumento general del tráfico web cifrado principalmente a estos factores:

- Un tráfico más móvil de las aplicaciones, que cifran intrínsecamente.
- Más solicitudes de descarga de video cifrado por parte de los usuarios.
- Más solicitudes de servidores de almacenamiento y respaldo con "datos confidenciales almacenados", que los atacantes están ansiosos de aprovechar.

De hecho, en la Figura 26 se muestra que las solicitudes HTTPS de almacenamiento y recursos de respaldo en línea aumentaron un 50% desde principios de 2015. Los servicios de transferencia de archivos también aumentaron considerablemente durante el mismo período: un 36%.

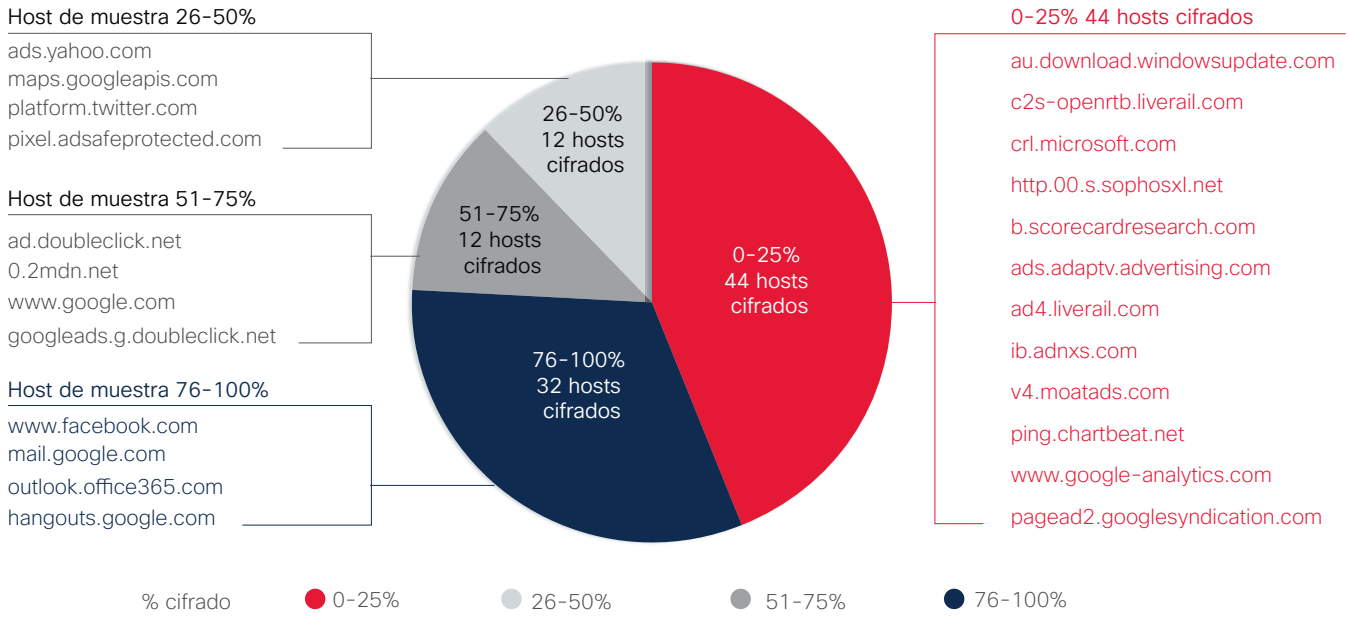
Finalmente, hay una mayor actividad de cifrado tanto en la cantidad de transacciones cifradas como en la cantidad de bytes cifrados por transacción. Cada uno posee sus propios beneficios y sus propios riesgos potenciales, lo que lleva a la necesidad de contar con una defensa ante amenazas integrada que ayude a aumentar la visibilidad.

Figura 26. Solicitudes HTTPS: Cambios más importantes de enero a septiembre de 2015



Fuente: Cisco Security Research

Figura 27. Hosts principales que cifran tráfico HTTPS



Fuente: Cisco Security Research

Al observar los dominios principales por solicitudes (Figura 27), podemos notar que muchas de las páginas principales de contenido de Google y Facebook están cifradas. Por lo general, solo el 10% del tráfico de publicidad de estas está cifrado.

Independientemente de los desafíos, el cifrado de datos es un requisito en el panorama actual de amenazas. Los atacantes son muy expertos en evitar el control de acceso para que los usuarios dejen la información crítica desprotegida en cualquier etapa del almacenamiento o de la transferencia.

Por eso, es esencial que los equipos de seguridad supervisen los patrones de tráfico web para asegurarse de que las solicitudes HTTPS no provengan de ubicaciones sospechas ni se dirijan a estas. Una pequeña advertencia: no busque tráfico cifrado en un conjunto predefinido de puertos. Como se analiza en la siguiente sección, en nuestra investigación se muestra que el malware posiblemente inicie comunicaciones cifradas en un conjunto diverso de puertos.

EL FACTOR DE LA ENTROPÍA

Una alta entropía es un buen indicio de transferencias o comunicación de archivos cifrados o comprimidos.[6] La buena noticia para los equipos de seguridad es que la entropía es relativamente fácil de supervisar porque no requiere conocimientos de los protocolos criptográficos subyacentes.

Durante un período de 3 meses que comenzó el 1 de junio de 2015, los investigadores de Cisco especializados en seguridad observaron 7 480 178 flujos enviados desde 598 138 muestras de malware con una "puntuación de la amenaza: 100". Hubo 958 851 flujos de alta entropía durante este período, lo que equivale a un 12,82%.

También identificamos 917 052 flujos en el protocolo Transport Layer Security (TLS) (un 12,26%). Además, 8419 flujos de TLS eran de un puerto distinto a 443, el puerto predeterminado para un HTTP seguro. Algunos de los puertos que el malware observado utilizaba para comunicarse eran los puertos 21, 53, 80, y 500.

A medida que el nivel de tráfico de Internet cifrado continúe aumentando, será cada vez más importante que las organizaciones adopten una arquitectura de defensa ante amenazas integrada (consulte "Seis principios de defensa ante amenazas integrada", **página 62**). Las soluciones puntuales no son eficaces para identificar posibles amenazas en el tráfico cifrado. Las plataformas de seguridad integrada proporcionan a los equipos de seguridad mayor visibilidad con respecto a lo que sucede en los dispositivos o las redes. Gracias a esto, pueden identificar más fácilmente los patrones sospechosos de actividad.

[6] Entropía: En informática, la entropía (falta de orden o de previsibilidad) es la aleatoriedad recopilada por un sistema operativo o una aplicación para su uso en la criptografía o para otros usos que requieran datos aleatorios.

El avance hacia el cifrado: Datos de casos

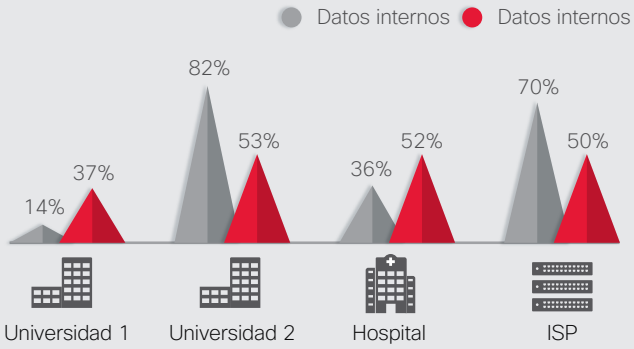
Lancope, una empresa de Cisco, estudió las tasas de cifrado tanto para el tráfico interno como el de Internet en tres sectores empresariales (dos universidades, un hospital y un proveedor de servicios de Internet [ISP] todos con sede en Estados Unidos).

En una de las universidades, Lancope descubrió que casi todo el tráfico interno estaba cifrado (el 82%). Además, el 53% del tráfico de Internet de la universidad estaba cifrado. Estos resultados están a la par con las tendencias que Lancope observó en otros sectores.

Solo el 36% de los datos internos del hospital estaba cifrado. Sin embargo, más de la mitad (el 52%) del tráfico de Internet estaba cifrado.

En el principal ISP, el 70% del tráfico interno y el 50% del tráfico de Internet estaban cifrados.

El estudio de Lancope cuenta la historia de la adopción generalizada del cifrado de datos en movimiento en diferentes sectores. Cisco sugiere que ahora se debería aplicar un enfoque similar al cifrado de datos almacenados para limitar los efectos de los riesgos que corre una organización.



Fuente: Laboratorios de investigación de amenazas de Lancope

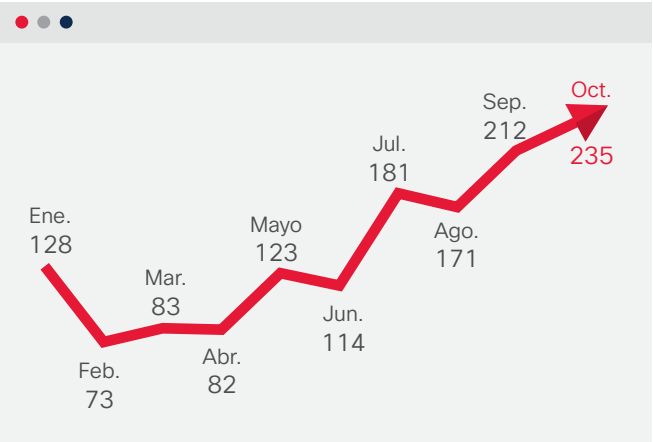
Los delincuentes en línea aumentan la actividad de los servidores en WordPress

Como se analizó en la introducción de este informe, los delincuentes en línea buscan continuamente métodos para agregar eficacia y ahorro de costos a sus operaciones, junto con nuevas formas de evadir la detección. Cada vez más, los ciberdelicuentes están encontrando esta eficacia en sitios web creados con WordPress, la conocida plataforma de desarrollo de sitios web y blogs. En los sitios WordPress, los atacantes pueden controlar el flujo continuo de servidores comprometidos para crear una infraestructura que respalde el ransomware, el fraude bancario o los ataques de suplantación de identidad. En Internet hay una gran cantidad de sitios abandonados creados con WordPress que no reciben mantenimiento desde una perspectiva de seguridad. A medida que emergen nuevos problemas de seguridad, estos sitios a menudo se ven comprometidos y se suelen incorporar en campañas de ataques.

Mediante el análisis de los sistemas utilizados para admitir el ransomware y otros malware, los investigadores de Cisco especializados en seguridad descubrieron que muchos delincuentes en línea están cambiando de la actividad en línea a los servidores comprometidos de WordPress. El número de dominios de WordPress utilizados por los delincuentes aumentó un 221% entre febrero y octubre de 2015 (consulte la Figura 28).

Los investigadores de Cisco creen que este cambio de lugar se produjo por una serie de razones. Cuando el ransomware utiliza otras herramientas para comunicar claves de cifrado y otra información de comando y control, se pueden detectar o bloquear esas comunicaciones, lo que impide que el proceso de cifrado se complete. Sin embargo, las comunicaciones que transmiten claves de cifrado a través de servidores comprometidos de WordPress pueden parecer normales, lo que aumenta las posibilidades de que se realice el cifrado de archivos. Es decir, los sitios WordPress actúan como agentes de retransmisión.

Figura 28. Cantidad de dominios de WordPress utilizados por los creadores de malware



Fuente: Cisco Security Research

Para evitar las desventajas de otras tecnologías, los delincuentes recurrieron a WordPress, que usan para alojar cargas útiles de malware y servidores de comando y control. Los sitios WordPress ofrecen varias ventajas. Por ejemplo, los numerosos sitios abandonados brindan a los delincuentes más oportunidades para poner en riesgo los sitios con protecciones de seguridad poco seguras.

El riesgo de usar sistemas afectados para ejecutar una operación de malware es que se puede quitar uno de los servidores hackeados cuando se detecta el riesgo. Si esto sucede en el medio de una campaña, es posible que el descargador de malware no pueda recuperar su carga útil o que el malware no pueda comunicarse con sus servidores de comando y control. Los investigadores de Cisco especializados en seguridad observaron que el malware superó esto mediante el uso de más de un servidor de WordPress. Cisco incluso descubrió listas de servidores comprometidos de WordPress almacenados en sitios de uso compartido de datos, como Pastebin.

El malware utilizaba estas listas para encontrar servidores de comando y control en funcionamiento, lo que permitía que el malware funcionara incluso si un servidor comprometido fallaba. Los investigadores también identificaron descargadores de malware que tenían una lista de sitios WordPress que almacenaban cargas útiles. Si un sitio de descarga no funcionaba, el malware iba al siguiente y descargaba cargas útiles maliciosas del servidor de WordPress en funcionamiento.

Los sitios WordPress comprometidos a menudo no funcionaban con la última versión de WordPress, contaban con contraseñas de administrador no seguras y utilizaban complementos a los que les faltaban parches de seguridad.

Estas vulnerabilidades permitían a los atacantes apropiarse de los servidores de WordPress y usarlos como infraestructura de malware (consulte la Figura 29).

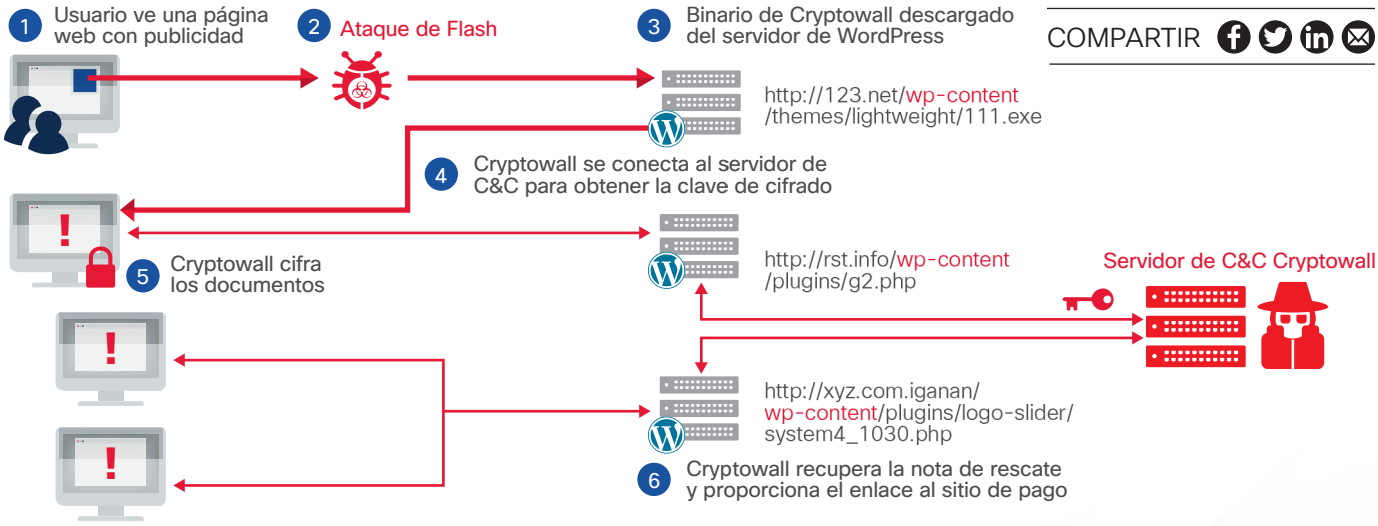
Los investigadores de Cisco han identificado algunos de los tipos de archivo y de software alojados con frecuencia en sitios WordPress comprometidos:

- Archivos ejecutables que son cargas útiles para los kits de ataque.
- Archivos de configuración de malware, como Dridex y Dyre.
- Código proxy que transmite comunicación de comando y control para ocultar la infraestructura de comando y control.
- Sitios web de suplantación de identidad para recopilar nombres de usuario y contraseñas.
- Scripts HTML que redireccionan el tráfico a los servidores de los kits de ataque.

Además, los investigadores de Cisco identificaron diversas familias de malware que utilizan sitios WordPress comprometidos para la infraestructura:

- Infostealer Dridex
- Programa de interceptación de contraseñas Pony
- Ransomware TeslaCrypt
- Ransomware Cryptowall 3.0
- Ransomware TorrentLocker
- Botnet de correo no deseado Andromeda
- Instalador troyano de malware Bartallex
- Infostealer Necurs
- Páginas de inicio de sesión falsas

Figura 29. Cómo se ven afectados los sitios WordPress



Fuente: Cisco Security Research

Los profesionales de seguridad preocupados por los riesgos que el sitio WordPress alojado por delincuentes plantea deben buscar una tecnología de seguridad web que examine el contenido proveniente de sitios creados con WordPress. Dicho tráfico podría considerarse inusual si la red descarga programas de sitios WordPress en lugar de solo sitios web e imágenes (aunque los sitios WordPress pueden alojar programas legítimos también).

Infraestructura obsoleta: un problema con de 10 años de gestación

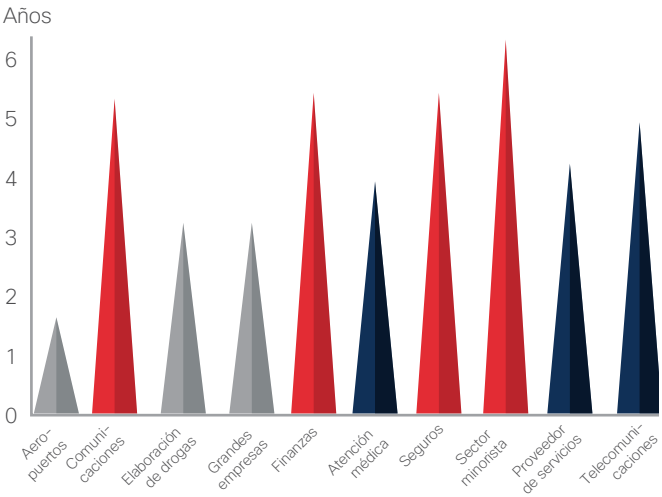
Todas las empresas de hoy son empresas de TI en cierta medida, porque dependen de su infraestructura de TI y TO (tecnología operativa) para estar conectadas, digitalizadas y tener éxito. Esto significa que necesitan dar prioridad a la seguridad de TI. Sin embargo, muchas organizaciones se basan en infraestructuras de red creadas a partir de componentes obsoletos, desactualizados, que ejecutan sistemas operativos vulnerables y no tienen capacidad de recuperación informática (ciberresiliencia).

Recientemente, analizamos 115 000 dispositivos Cisco en Internet y en entornos de clientes como una forma de llamar la atención sobre los riesgos de seguridad que plantean la infraestructura obsoleta y la falta de atención a los parches de vulnerabilidades.

En nuestra muestra de un día, identificamos 115 000 dispositivos mediante el análisis de Internet y luego observamos los dispositivos "desde fuera hacia dentro" (desde la perspectiva de Internet a la de la empresa). Mediante nuestro escaneo y análisis, descubrimos que 106 000 de los 115 000 dispositivos tenían vulnerabilidades conocidas en el software que ejecutaban. Esto significa que, de nuestra muestra, el 92% de los dispositivos Cisco en Internet es susceptible a vulnerabilidades conocidas.

Cisco también detectó que la versión de software que esos dispositivos ejecutaban tenía 26 vulnerabilidades, en promedio. Además, descubrimos que muchas organizaciones ejecutaban software desactualizados en sus infraestructuras de red (Figura 30). Encontramos que algunos clientes de los sectores financiero, de servicios de salud y de comercio minorista utilizan versiones de nuestro software de más de 6 años.

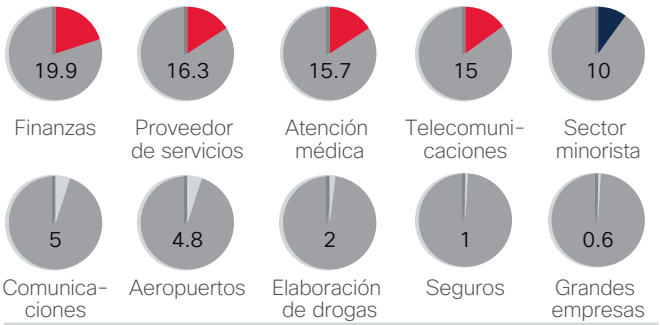
Figura 30. Edad promedio del software en años



Fuente: Cisco Security Research

También descubrimos que muchos de los dispositivos de infraestructura analizados habían alcanzado el último día de soporte (LDoS), lo que significa que no se pueden actualizar ni proteger (Figura 31). Estos dispositivos ni siquiera reciben parches para las vulnerabilidades conocidas, por lo que no reciben información sobre amenazas nuevas. Se ha informado a los clientes de este problema.

Figura 31. Porcentaje de LDoS de los dispositivos de infraestructura



Fuente: Cisco Security Research

Para obtener más información sobre este tema, lea las entradas del blog sobre seguridad de Cisco:

"Seguridad de TI: Cuando se sobrestima la madurez"

"Evolución de los ataques en los dispositivos Cisco IOS"

"SYNful Knock: Detección y mitigación de ataques a software Cisco IOS"

Además, el 8% de los 115 000 dispositivos analizados en nuestra muestra ha alcanzado su etapa de fin de vida útil, y otro 31% alcanzará el fin de soporte dentro de uno a cuatro años.

Una infraestructura de TI desactualizada y obsoleta constituye una vulnerabilidad para las organizaciones. A medida que avanzamos a Internet de las cosas (IdC) e Internet de todo (IdT), se torna cada vez más importante que las empresas se aseguren de contar con una infraestructura de red segura para que, de este modo, se garantice la integridad de los datos y las comunicaciones que atraviesan la red. Esto es fundamental para el éxito de IdT emergente.

Muchos clientes de Cisco desarrollaron sus infraestructuras de red hace una década. En ese entonces, muchas empresas simplemente no tuvieron en cuenta el hecho de que dependerían completamente de esa infraestructura. Tampoco previeron que la infraestructura se convertiría en un objetivo principal para los atacantes.

Las organizaciones suelen evitar hacer actualizaciones de infraestructura porque son costosas y requieren tiempo de inactividad de la red. En algunos casos, una simple actualización no bastará. Algunos productos son tan antiguos que no se pueden actualizar a fin de incorporar las últimas soluciones de seguridad necesarias para proteger a la empresa.

Solo estos hechos expresan la criticidad de mantener la infraestructura. Las organizaciones deben planificar actualizaciones periódicas y reconocer el valor de controlar sus infraestructuras críticas de forma proactiva, antes de que lo haga un adversario.

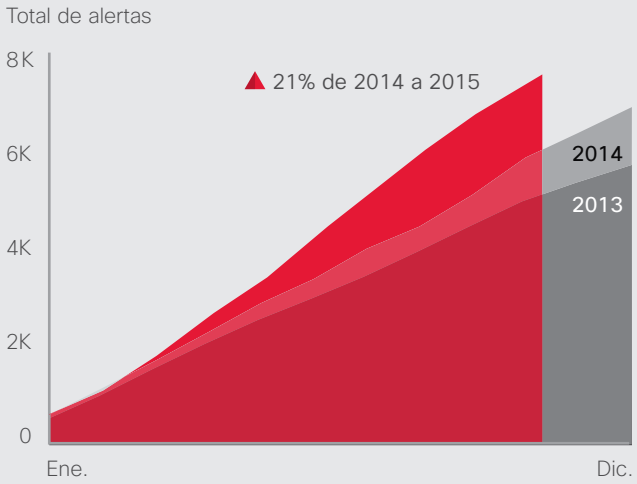
Los totales de alertas acumuladas demuestran un creciente compromiso con la administración de vulnerabilidades

La dependencia de la infraestructura obsoleta abre la puerta a los atacantes. Sin embargo, el aumento de alertas acumuladas, que incluyen vulnerabilidades de productos en soluciones de código abierto y patentadas, es una señal positiva de que el sector tecnológico está prestando especial atención a eliminar las oportunidades para los atacantes.

Los totales de alertas acumuladas aumentaron un 21% de 2014 a 2015. De julio a septiembre de 2015, el aumento fue notablemente alto. Este aumento puede atribuirse en gran parte a importantes actualizaciones de software de proveedores, como Microsoft y Apple, porque las actualizaciones de productos producen más informes de vulnerabilidades de software.

Los principales proveedores de software ahora lanzan revisiones y actualizaciones en mayor volumen y son más transparentes en esta actividad. El creciente volumen es uno de los principales motores de las organizaciones que automatizan la administración de vulnerabilidades mediante el uso de plataformas de inteligencia de seguridad y administración que ayudan a administrar el volumen del inventario de software y del sistema, las vulnerabilidades y la información sobre amenazas. Estos sistemas e interfaces de programación de aplicaciones (API) permiten una administración de la seguridad más eficiente, oportuna y eficaz en organizaciones grandes y pequeñas.

Figura 32. Alertas acumulativas totales anuales



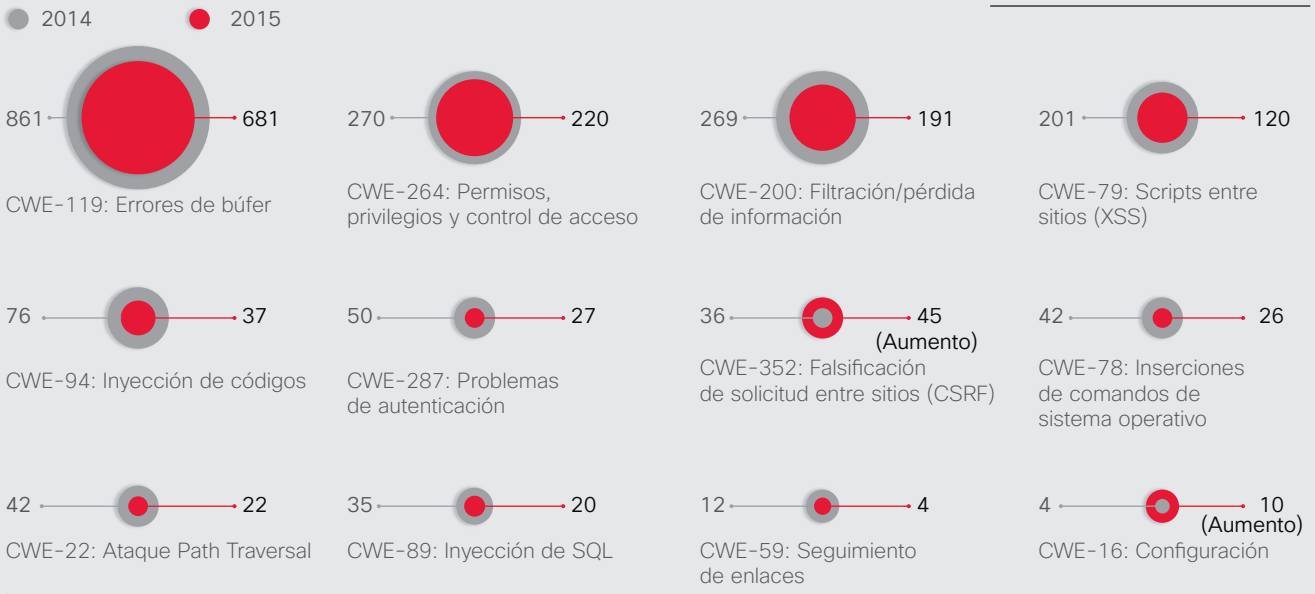
Fuente: Cisco Security Research

Categorías de amenazas: Disminución de los errores de búfer, filtraciones de información y divulgaciones

En el examen de categorías comunes de vulnerabilidades, las vulnerabilidades de scripts entre sitios (XSS) se redujeron un 47% de 2014 a 2015 (Figura 33). La reducción puede deberse a una mayor atención prestada a la prueba de vulnerabilidades. Los proveedores se han vuelto más expertos en identificar estas vulnerabilidades específicas y en solucionarlas antes de que sus productos se lancen al mercado.

Las vulnerabilidades de la filtración o divulgación de la información se redujeron un 15% en 2015. Estas vulnerabilidades implican divulgaciones no voluntarias a partes que no tienen acceso explícito. Los proveedores están más atentos a los controles que permiten o rechazan el acceso a los datos, lo que hace que esta vulnerabilidad común ocurra con menos frecuencia.

Figura 33. Cantidad de vulnerabilidades en categorías comunes



Fuente: Cisco Security Research

¿Las pymes constituyen un eslabón débil de la seguridad empresarial?

Las pequeñas y medianas empresas (pymes) desempeñan un papel importante en las economías nacionales. Cuando sus clientes les confían datos, las pymes también asumen la responsabilidad de proteger esta información contra atacantes en línea. Sin embargo, como se detalla en el Estudio comparativo sobre capacidades de seguridad 2015 de Cisco (consulte la **página 41**), las pymes muestran indicios de que sus defensas contra atacantes son más débiles de las que sus desafíos exigen. A su vez, estas debilidades pueden poner en riesgo a los clientes de las pymes. Los atacantes que pueden violar la red de una pyme también pueden encontrar una vía hacia una red empresarial.

Según los resultados del Estudio comparativo sobre capacidades de seguridad 2014 de Cisco, las pymes utilizan menos procesos para analizar riesgos y menos herramientas de defensa ante amenazas en comparación con el año pasado. Por ejemplo, el 48% de las pymes declaró haber utilizado seguridad web en 2015; el 59% afirmó que lo hizo en 2014. Solo el 29% afirmó que utilizó herramientas de configuración y revisión en 2015, en comparación con el 39% en 2014.

Además, casi una cuarta parte de los encuestados de las pymes que no tienen un ejecutivo a cargo de la seguridad no cree que sus empresas sean objetivos de gran valor para los delincuentes en línea. Esta convicción insinúa que hay un exceso de confianza en la capacidad de la empresa para frustrar los sofisticados ataques en línea de hoy, o, lo que es más probable, que esta nunca será atacada.

ES MENOS PROBABLE QUE LAS PYMES UTILICEN LOS EQUIPOS DE RESPUESTA ANTE LOS INCIDENTES

En muchos casos, es menos probable que las pymes tengan equipos de respuesta ante incidentes y de inteligencia de amenazas que las corporaciones. Esto puede deberse a restricciones de presupuesto: los encuestados indicaron problemas relacionados con el presupuesto como uno de los obstáculos más grandes para adoptar procesos y tecnología de seguridad avanzados. El 72% de las corporaciones (aquellas con más de 1000 empleados) cuenta con ambos equipos, en comparación con el 67% de las empresas con menos de 500 empleados.

Las pymes también utilizan menos procesos para analizar riesgos, eliminar las causas de un incidente y restaurar sistemas a los niveles previos al incidente (Figura 35).

Por ejemplo, el 53% de las empresas con más de 10 000 empleados utiliza el análisis del flujo de red para analizar los sistemas afectados, en comparación con el 43% de las empresas con menos de 500 empleados. El 60% de las empresas con más de 10 000 empleados revisa y actualiza las aplicaciones consideradas vulnerables, en comparación con el 51% de las empresas con menos de 500 empleados.

El uso de ciertas defensas ante amenazas por parte de las pymes parece estar disminuyendo. Por ejemplo, en 2014, el 52% de las pymes utilizó seguridad móvil, pero solo el 42% lo hizo en 2015. Además, en 2014, el 48% de las pymes utilizó el escaneo de vulnerabilidades, en comparación con el 40% en 2015 (consulte la Figura 36).

Figura 34. Principales obstáculos de las pymes

¿Cuál de las siguientes opciones considera que pueden ser los obstáculos más grandes para adoptar procesos y tecnología de seguridad avanzada?

Tamaño de la empresa	250-499	500-999	1000-9999	10,000+
Restricciones de presupuesto	40%	39%	39%	41%
Problemas de compatibilidad con sistemas antiguos	34%	30%	32%	34%
Prioridades contrapuestas	25%	25%	24%	24%

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 36. Disminución de las defensas de las pymes en 2015

¿Cuáles de los siguientes tipos de defensas contra amenaza de seguridad usa actualmente su organización, si es que usa algún tipo?

	2014	2015
Seguridad móvil	52%	42%
Tecnología inalámbrica protegida	51%	41%
Análisis de vulnerabilidades	48%	40%
VPN	46%	36%
Administración de información y eventos de seguridad (SIEM)	42%	35%
Pruebas de penetración	38%	32%
Informática forense de red	41%	29%
Revisión y configuración	39%	29%
Informática forense de terminales	31%	23%

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 35. Las pymes utilizan menos procesos de seguridad que las corporaciones

¿Cuáles de estos procesos usa su organización para analizar los sistemas comprometidos, si es que usa algún proceso?

Tamaño de la empresa	250-499	500-999	1000-9999	10,000+
Informática forense de memorias	36%	36%	35%	34%
Análisis del flujo de red	43%	47%	52%	53%
Análisis de registros/eventos correlacionados	34%	34%	40%	42%
Equipos de análisis/respuesta a incidentes externos (o de terceros)	40%	32%	34%	39%
Análisis de registros de sistemas	47%	51%	55%	59%
Análisis de registros	43%	47%	52%	53%
Detección de indicadores de riesgo (IOC)	31%	34%	37%	36%

¿Qué procesos usa su organización para restaurar los sistemas afectados a los niveles operativos anteriores al incidente?

Revisión y actualización de aplicaciones consideradas vulnerables	51%	53%	57%	60%
Implementación de detecciones y controles nuevos o adicionales	49%	55%	57%	61%

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

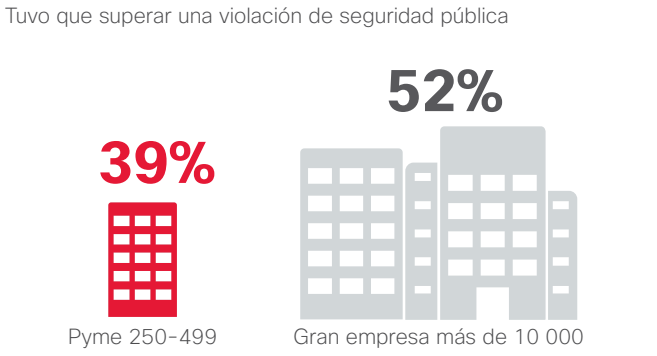
¿Por qué resulta importante el hecho de que las pymes suelan usar menos defensas que las grandes empresas? En un entorno de seguridad donde los atacantes desarrollan tácticas más sofisticadas para acceder a redes y mantenerse inadvertidos, ninguna empresa puede dejar sus redes desprotegidas ni posponer la aplicación de procesos que puedan ofrecer conocimientos sobre cómo se produjo un riesgo para poder evitarlo en el futuro.

Además, es posible que las pymes no se den cuenta de que sus propias vulnerabilidades se traducen en riesgos para los clientes de corporaciones y sus redes. Los delincuentes actuales a menudo obtienen acceso a una red como medio para encontrar un punto de ingreso en otra red más lucrativa, y las pymes pueden ser el punto de partida de ese ataque.

MENOS POSIBILIDADES DE HABER EXPERIMENTADO VIOLACIONES PÚBLICAS DE DATOS

Las pymes tienen menos posibilidades que las corporaciones de haber enfrentado una violación a la seguridad pública, probablemente debido a sus superficies más pequeñas desde la perspectiva de una red. Mientras que el 52% de las empresas con más de 10 000 empleados administró las consecuencias de una violación a la seguridad pública, solo el 39% de las empresas con menos de 500 empleados lo hizo.

Figura 37. Las pymes informan menos violaciones públicas

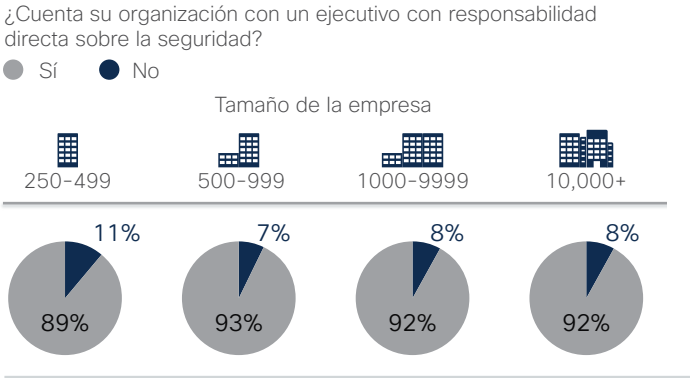


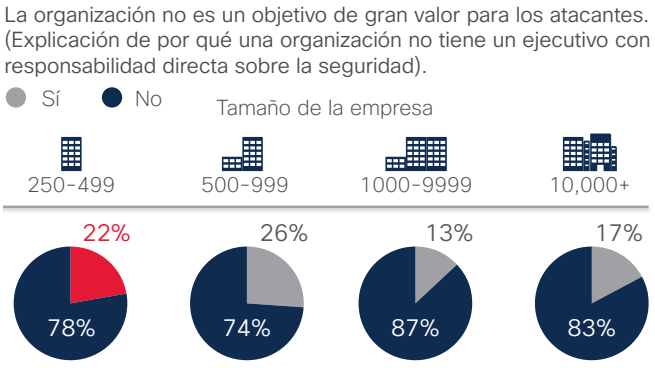
Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

COMPARTIR

Las violaciones a la seguridad pública son claramente disruptivas y perjudiciales para una empresa, pero ofrecen un beneficio: alientan a las empresas a centrarse con más detenimiento en proteger su seguridad y considerar la posibilidad de fortalecerla. Los datos de la encuesta de Cisco (consulte la **página 74**) indican que cuando las corporaciones sufren una violación pública de datos, actualizan considerablemente la tecnología de seguridad e implementan procesos más eficaces.

Figura 38. Las pymes no se perciben como objetivos de gran valor





Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

La visión de las pymes de sus empresas como objetivos de ciberdelincuentes puede demostrar una brecha en su percepción sobre el panorama de las amenazas. Como se explicó anteriormente en la Figura 38, el 22% de las empresas con menos de 500 empleados dijo que no tiene un ejecutivo con responsabilidad y rendición de cuentas directas para la seguridad porque no se ven como objetivos de gran valor.

ES más PROBABLE QUE LAS PYMES SUBCONTRATEN FUNCIONES DE SEGURIDAD EN 2015

Si bien en la encuesta se muestra que, en líneas generales, hay más pymes que subcontratan funciones de seguridad, en general, es menos probable que subcontraten determinados servicios, como asesoramiento y consultoría, en comparación con las corporaciones. Por ejemplo, el 55% de las corporaciones subcontrata servicios de asesoramiento y consultoría, en comparación con el 46% de las empresas con menos de 500 empleados. El 56% de las corporaciones subcontrata tareas de auditoría de seguridad, en comparación con el 42% de las empresas con menos de 500 empleados (consulte la Figura 39).

Sin embargo, en 2015, una mayor cantidad de pymes están subcontratando al menos algunos servicios de seguridad. En 2014, el 24% de las pymes con menos de 499 empleados afirmó que no subcontrató ningún servicio. En 2015, solo el 18% de las pymes afirmó lo mismo.

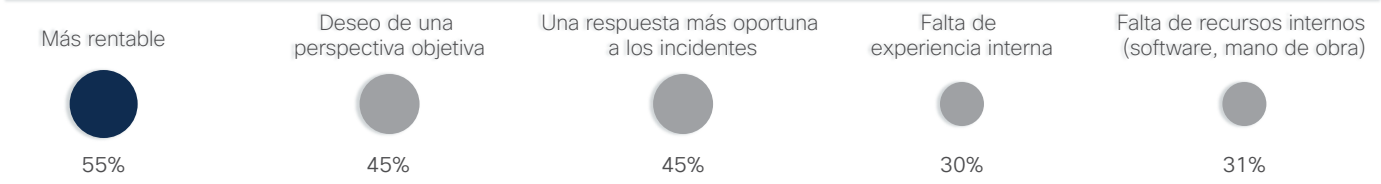
El hecho de que cada vez más pymes adopten la subcontratación como una forma de administrar la seguridad es bueno. Indica que, para proteger las redes, las pymes están buscando herramientas flexibles que no supongan una carga para su personal más pequeño o sus presupuestos más moderados. Sin embargo, las pymes pueden creer erróneamente que los procesos de subcontratación de seguridad reducirán considerablemente la probabilidad de una violación a la red. O pueden atribuir la responsabilidad de la seguridad a un tercero. Dicho punto de vista sería un pensamiento ilusorio, ya que solo un sistema de defensa ante amenazas realmente integrado, uno que no solo examine y mitigue los ataques sino que los impida, puede proporcionar protección de seguridad de nivel empresarial.

Figura 39. Una mayor cantidad de pymes subcontratan servicios de seguridad en 2015

Cuando se trata de seguridad, ¿cuál de los siguientes tipos de servicios se subcontratan a terceros en forma total o parcial, si es que se subcontrata algún servicio?

Tamaño de la empresa	250-499	500-999	1000-9999	10,000+
Asesoramiento y consultoría	46%	51%	54%	55%
Supervisión	45%	46%	42%	44%
Auditoría	42%	46%	46%	56%
Respuesta ante incidentes	39%	44%	44%	40%
Inteligencia de amenazas	35%	37%	42%	41%
Corrección	33%	38%	36%	36%
Ninguna	18%	12%	11%	10%

¿Por qué su organización (pyme, 250-499) elige subcontratar estos servicios?



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Estudio comparativo sobre capacidades de seguridad de Cisco

Estudio comparativo sobre capacidades de seguridad de Cisco

Para evaluar las percepciones de los profesionales de seguridad respecto del estado de la seguridad en las organizaciones, Cisco consultó a directores generales de seguridad (CSO) y a gerentes de operaciones de seguridad (SecOps) de varios países y organizaciones de diferentes tamaños sobre sus percepciones de los procedimientos y recursos de seguridad. En el Estudio comparativo sobre capacidades de seguridad 2015 de Cisco se ofrecen información sobre el nivel de madurez de las operaciones y las prácticas de seguridad actualmente en uso, y también se comparan estos resultados con los del estudio inaugural de 2014.

Disminución de la confianza en medio de indicios de preparación

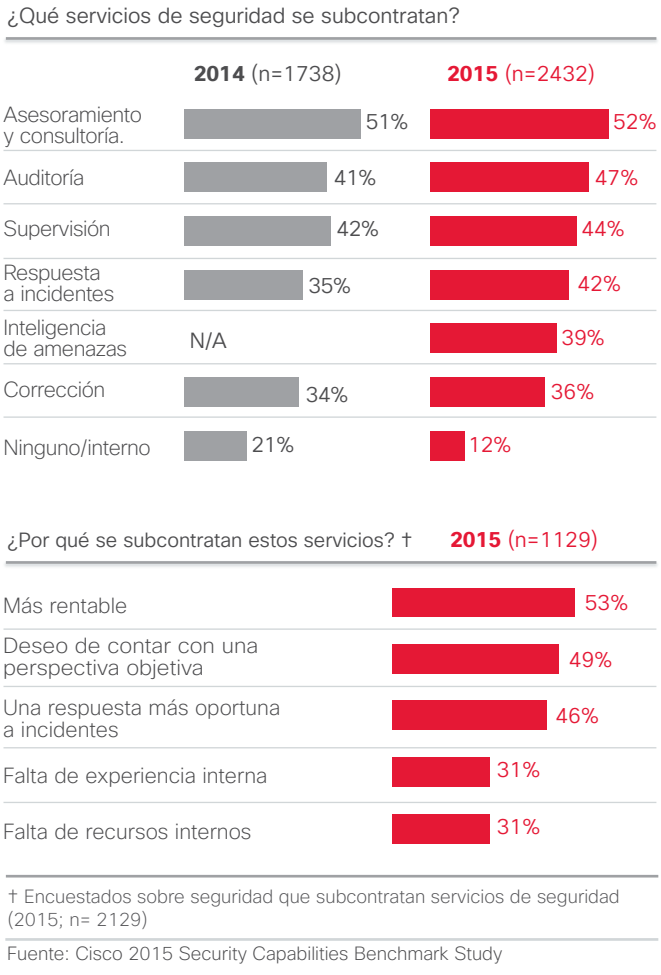
Frente a amenazas más sofisticadas, el estudio de Cisco sugiere que la confianza de los profesionales de seguridad parece estar decayendo. Por otro lado, la creciente preocupación por la seguridad está cambiando la manera en que estos profesionales protegen las redes. Por ejemplo, pueden observarse más capacitaciones en seguridad, un incremento en las políticas formales y escritas, y más subcontratación de tareas, como auditorías de seguridad, consultoría y respuesta ante incidentes. En resumen, los profesionales de seguridad muestran señales de que están tomando medidas para combatir las amenazas que acechan las redes.

El avance hacia la capacitación y la subcontratación son acontecimientos positivos, pero el sector de seguridad no puede detenerse aquí. Debe continuar aumentando el uso de herramientas y procesos a fin de mejorar la detección, contención y corrección de amenazas. Dados los obstáculos de las limitaciones de presupuesto y la compatibilidad con las soluciones, el sector también debe explorar soluciones eficaces que proporcionen una defensa integrada ante amenazas. El sector también debe mejorar la colaboración con otras organizaciones cuando se producen violaciones públicas (como el botnet SSHPsychos; consulte la **página 14**), ya que el intercambio de conocimientos puede ayudar a prevenir ataques futuros.

RECURSOS: ORGANIZACIONES CON MÁS POSIBILIDADES DE SUBCONTRATAR

A medida que los profesionales de seguridad son más conscientes de las amenazas, pueden buscar formas de mejorar las defensas; por ejemplo, subcontratando las tareas de seguridad que los asesores o proveedores pueden administrar de manera más eficiente. En 2015, el 47% de las empresas encuestadas subcontrató auditorías de seguridad, un aumento del 41% en comparación con el año 2014. También en 2015, el 42% subcontrató procesos de respuesta ante incidentes, en comparación con el 35% en 2014 (Figura 40).

Figura 40. Descripción general de servicios subcontratados



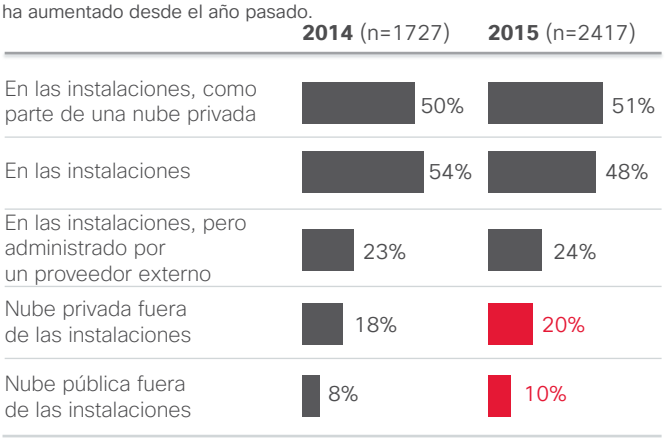
† Encuestados sobre seguridad que subcontratan servicios de seguridad (2015; n= 2129)

Fuente: Cisco 2015 Security Capabilities Benchmark Study

Además, más profesionales de seguridad subcontratan al menos algunas funciones de seguridad. En 2014, el 21% de los encuestados dijo que no subcontrató ningún servicio de seguridad. En 2015, esa cifra disminuyó considerablemente al 12%. El 53% afirmó que subcontrata servicios porque es más rentable, mientras que el 49% afirmó que subcontrata servicios para obtener perspectivas objetivas.

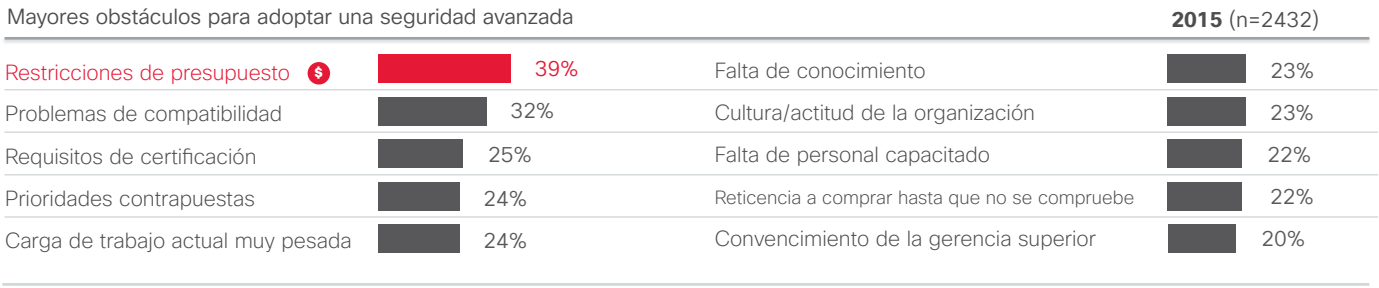
Para agregar protección a las redes y los datos, los profesionales de seguridad indicaron que son receptivos al concepto de alojar redes fuera de las instalaciones. Mientras que el alojamiento en las instalaciones sigue siendo la opción preferida, la cantidad de profesionales que usan soluciones fuera de las instalaciones ha aumentado. En 2015, el 20% utilizó soluciones de nube privada fuera de las instalaciones, en comparación con el 18% en 2014 (Figura 41).

Figura 41. Alojamiento fuera de las instalaciones en aumento



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

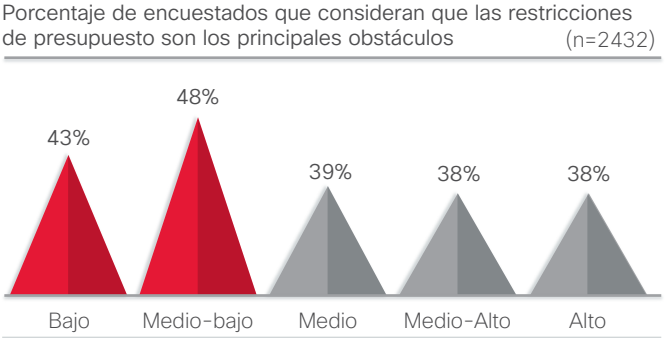
Figura 42. Las restricciones de presupuesto constituyen el mayor obstáculo para las actualizaciones de seguridad



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Los equipos de seguridad encuestados por Cisco están más resueltos a proteger sus redes con mayor eficacia, pero pueden verse limitados en sus capacidades para llevar a cabo sus planes. Los profesionales de seguridad indicaron que las restricciones de presupuesto (un 39%) encabezan la lista de las posibles razones para elegir o rechazar los servicios y herramientas de seguridad, seguidos de los problemas de compatibilidad con la tecnología (un 32%; consulte la Figura 42). Las restricciones de presupuesto se convierten más bien en un problema para las empresas que clasifican en los niveles bajo y medio-bajo de madurez (consulte la Figura 43). En las respuestas de todos los profesionales de seguridad, el 39% menciona las restricciones de presupuesto como un obstáculo para adoptar procesos de seguridad avanzada. Esa cifra representa el 43% de las empresas en la clasificación de madurez baja y el 48% en la clasificación de madurez media-baja.

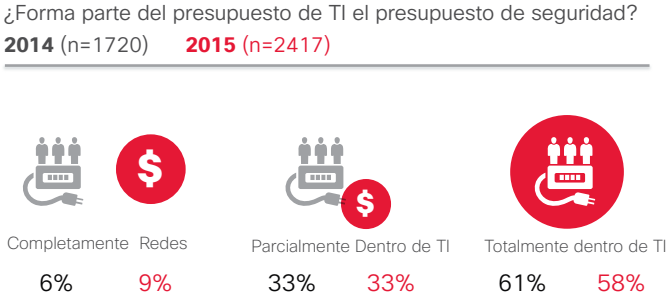
Figura 43. Las restricciones de presupuesto son el obstáculo principal para las empresas de baja madurez



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Una señal de que algunas organizaciones están prestando más atención a los recursos de seguridad es cómo estructuran sus presupuestos de seguridad. La encuesta refleja un leve incremento en la cantidad de organizaciones que separan el presupuesto de seguridad del presupuesto de TI general. En 2014, el 6% de los profesionales dijo que habían separado por completo los presupuestos de seguridad y de TI; en 2015, esa cifra aumentó al 9% (consulte la Figura 44).

Figura 44. Leve aumento en organizaciones con presupuestos de seguridad separados

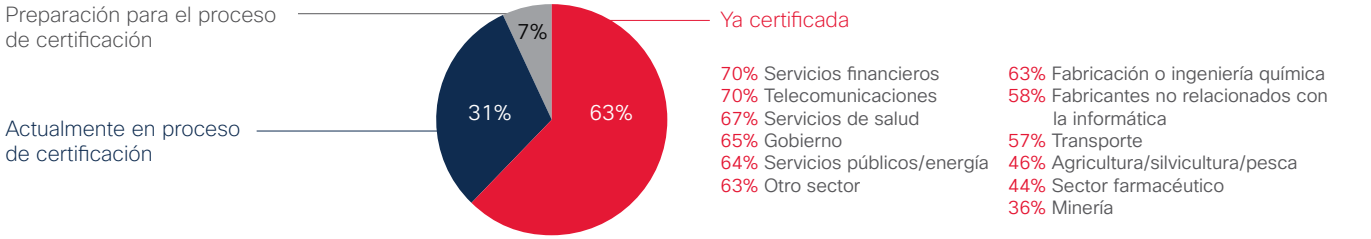


Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Cuando las organizaciones estandarizan las políticas de seguridad o buscan la certificación, muestran un compromiso con mejorar la seguridad. Casi dos tercios de los profesionales de seguridad afirmaron que sus organizaciones están certificadas en políticas o prácticas estandarizadas de seguridad, o que están por obtener la certificación (Figura 45). Este es otra señal positiva de que las empresas hallan valor en mejorar sus conocimientos sobre seguridad y respuesta a las amenazas.

Figura 45. La mayoría de las organizaciones están certificadas o buscan obtener la certificación

La organización sigue la práctica estandarizada de la política de seguridad informática (**2015** n=1265)



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

En el análisis del uso de las defensas de seguridad, descubrimos que los firewalls son las herramientas de seguridad utilizadas con más frecuencia por las empresas (un 65%), seguidas de la prevención de pérdida de datos (u 56%) y las herramientas de autenticación (un 53%; consulte la Figura 46). En 2015, era menos probable que las empresas confiaran en las herramientas basadas en la nube. Aunque los profesionales de seguridad demostraron predisposición para subcontratar servicios de seguridad (consulte la **página 43**), es posible que tiendan hacia una implementación interna de herramientas. (Consulte la **página 71** para obtener una lista completa).

Figura 46. Los firewalls y la prevención de pérdida de datos son las herramientas de seguridad que se usan con mayor frecuencia

Defensas contra amenazas de seguridad utilizadas por la organización	**2014** (n=1738)	**2015** (n=2432)	Defensas administradas a través de los servicios basados en la nube (encuestados sobre seguridad que utilizan las defensas contra amenazas de seguridad) **2014** (n=1646)	**2015** (n=2268)
Firewall*	N/D	65%		31%
Prevención de pérdida de datos	55%	56%		
Autenticación	52%	53%		
Cifrado/privacidad/protección de datos	53%	53%		
Seguridad de mensajería/correo electrónico	56%	52%	37%	34%
Seguridad web	59%	51%	37%	31%
Red, seguridad, firewalls y prevención de intrusiones*	60%	N/A	35%	

*El firewall y la prevención de intrusiones constituían un código en 2014: "Seguridad de la red, firewalls y prevención de intrusiones".

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

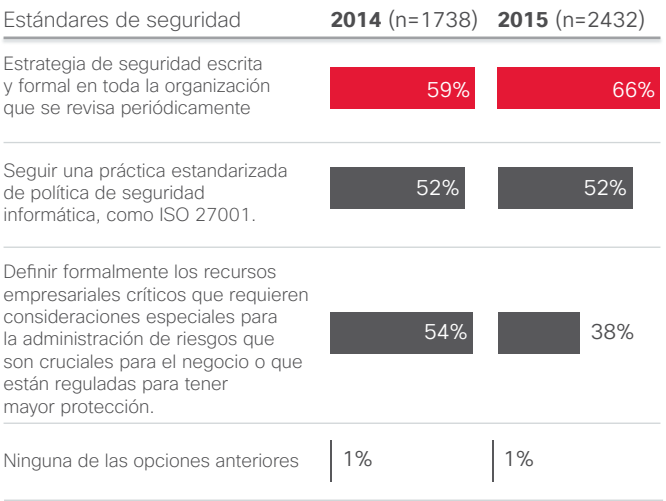
CAPACIDADES: CONFIANZA EN BAJA

En 2015, los profesionales de seguridad se sentían menos seguros de que sus infraestructuras de seguridad estuvieran actualizadas, en comparación con el año 2014. Sin dudas, esta disminución de la confianza se debe al redoble constante de ataques de alto perfil a empresas importantes, al robo correspondiente de datos privados y a las disculpas públicas de las empresas cuyas redes fueron vulneradas.

Sin embargo, esta disminución de la confianza está acompañada de un creciente interés en desarrollar políticas más sólidas. Como se muestra en la Figura 47, en 2015, hay más empresas (un 66%) que cuentan con una estrategia de seguridad escrita y formal que en 2014 (un 59%).

Figura 47. Más organizaciones crean políticas de seguridad formales

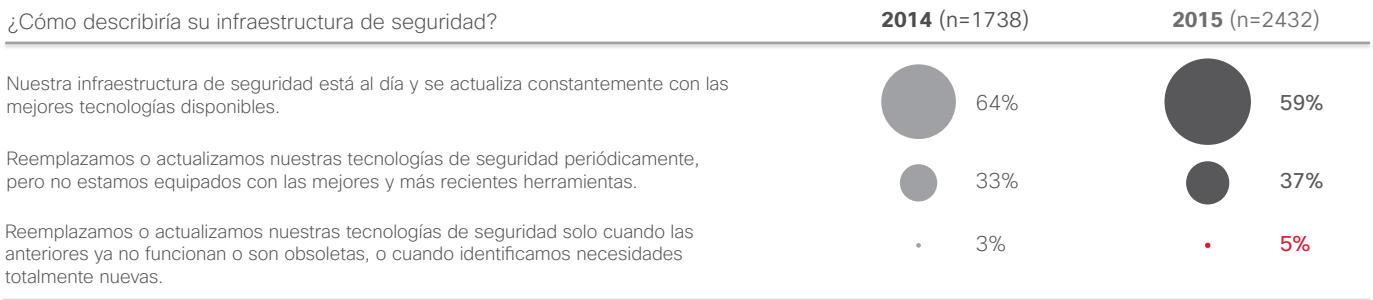
Casi dos tercios están certificados en una política o práctica estandarizadas de seguridad.



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

COMPARTIR

Figura 48. La confianza es menor en 2015

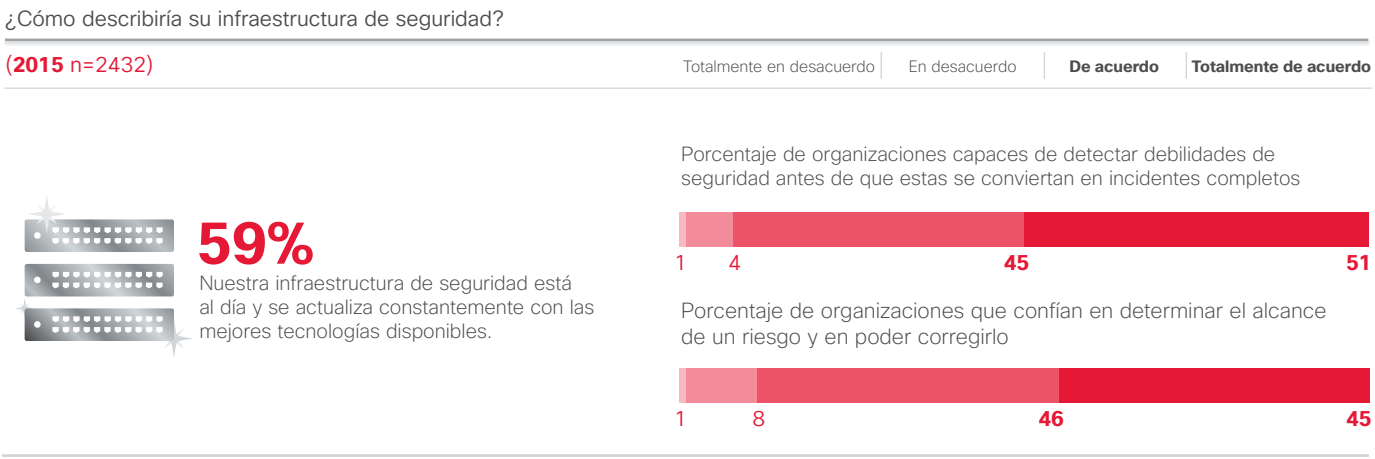


Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Como señal de que la confianza está disminuyendo, los profesionales de seguridad muestran un poco menos confianza en sus tecnologías. En 2014, el 64% dijo que sus infraestructuras de seguridad estaban al día y se actualizaban constantemente. En 2015, esa cifra se redujo a un 59% (Figura 48). Además, en 2014, el 33% dijo que sus organizaciones no estaban equipadas con las últimas herramientas de seguridad; esa cifra aumentó a un 37% en 2015.

La confianza es bastante elevada entre los directores generales de seguridad (CSO), que son más optimistas que los gerentes de operaciones de seguridad (SecOps): el 65% de los CSO cree que su infraestructura de seguridad está actualizada en comparación con el 54% de los gerentes de SecOps. Es posible que la confianza de los gerentes de SecOps se vea afectada porque responden a incidentes de seguridad diarios, lo que les proporciona una visión menos positiva de su preparación para la seguridad.

Figura 49. Confianza variada en la capacidad para detectar riesgos

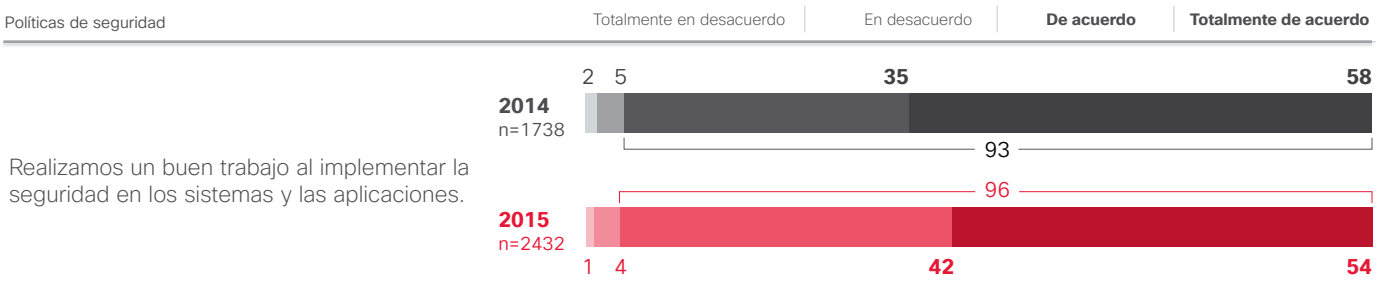


Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Los profesionales de seguridad también muestran niveles combinados de confianza en lo que respecta a sus capacidades de frustrar atacantes. El 51% cree firmemente que puede detectar debilidades de seguridad antes de que estas se conviertan en incidentes a gran escala; solo el 45% confía en su capacidad para determinar el alcance de un riesgo en la red y solucionar el daño (consulte la Figura 49).

Los profesionales de seguridad también muestran niveles de confianza más débiles en su capacidad para defender sus redes de los ataques. Por ejemplo, en 2015, menos profesionales creen firmemente que hacen un buen trabajo al implementar la seguridad en los procedimientos para adquirir, desarrollar y mantener los sistemas (un 54% en 2015, en comparación con un 58% en 2014; consulte la Figura 50). (Consulte la **página 76** para obtener una lista completa).

Figura 50. Menos confianza en la capacidad para implementar la seguridad en sistemas

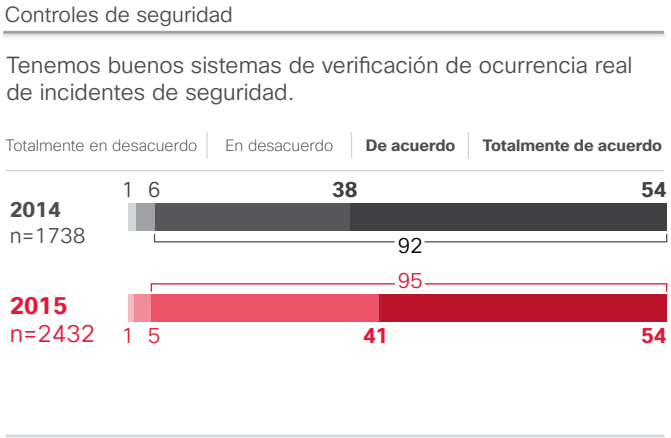


Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

En algunas áreas, los niveles de confianza en capacidades de seguridad no son muy altos. Por ejemplo, en 2015, solo el 54% de los encuestados indicó que creen que tienen un buen sistema para verificar si en realidad se produjeron incidentes de seguridad (consulte la Figura 51). (Consulte la **página 77** para obtener una lista completa).

Los encuestados tampoco se sienten completamente seguros de que sus sistemas puedan determinar el alcance y contener tales riesgos. El 56% dijo que revisa y mejora las prácticas de seguridad de forma periódica, formal y estratégica; el 52% considera que las tecnologías de seguridad están bien integradas y que funcionan eficazmente juntas (consulte la Figura 52). (Consulte la **página 79** para obtener una lista completa).

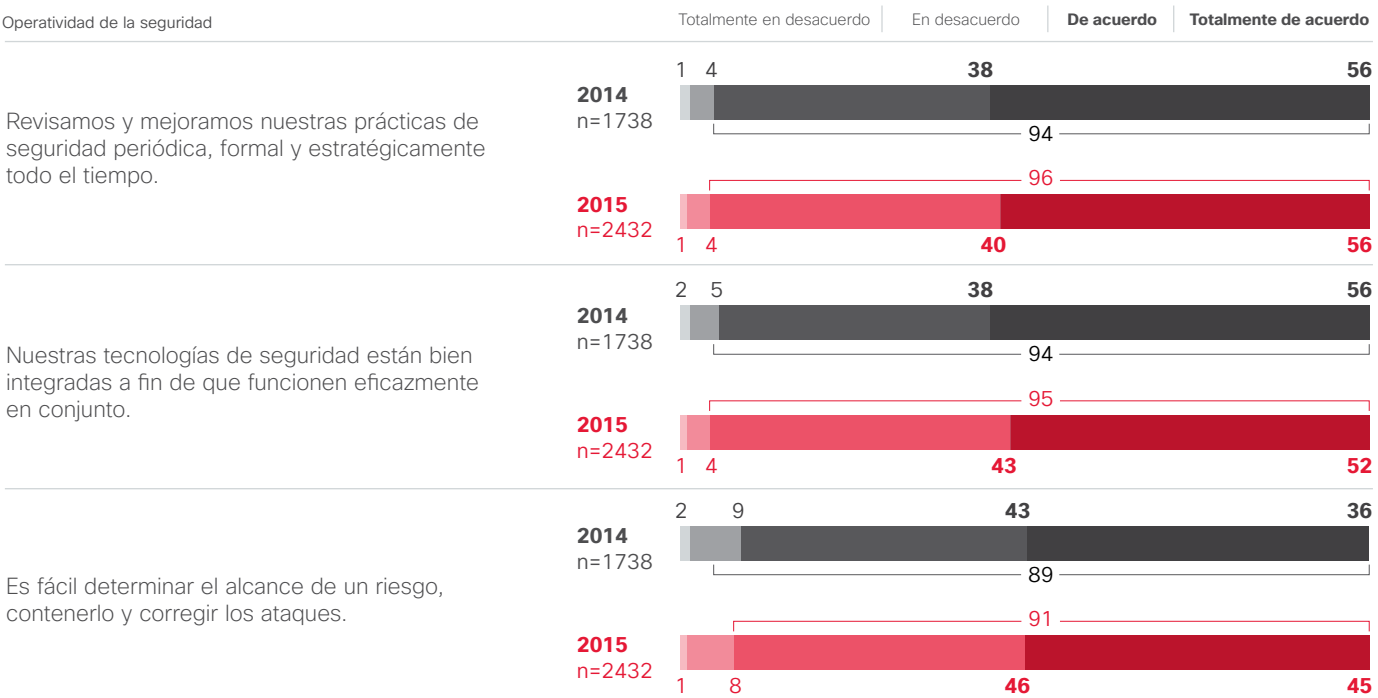
Figura 51. Las empresas creen que cuentan con buenos controles de seguridad



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

COMPARTIR

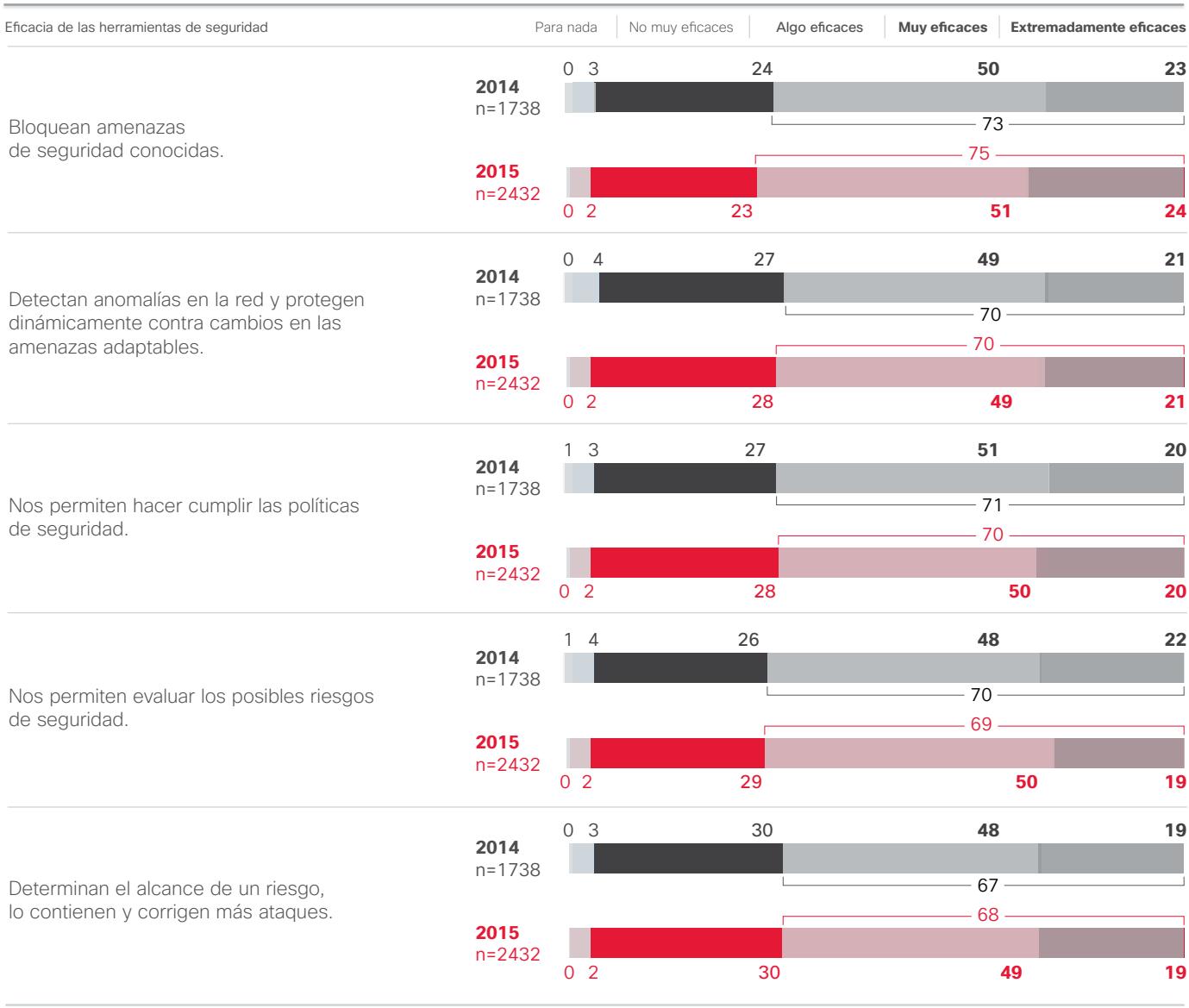
Figura 52. Las empresas expresan una confianza variada en la capacidad para contener el riesgo



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 53. Una cuarta parte de las empresas considera que las herramientas de seguridad son solo algo eficaces

De modo similar al año pasado, más de una cuarta parte de los entrevistados percibe que sus herramientas de seguridad son solo "algo" eficaces en lugar de "muy" o "extremadamente" eficaces.



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

De forma similar a los encuestados en 2014, más de una cuarta parte de los profesionales de seguridad dijo que perciben que sus herramientas de seguridad son solo algo eficaces en 2015 (Figura 53).

Las violaciones públicas a la seguridad suelen ser un momento decisivo para las organizaciones. Una vez que se producen, las organizaciones parecen tomar mayor conciencia de la necesidad de evitar violaciones futuras. Sin embargo, en 2015, menos profesionales de seguridad afirmaron que sus organizaciones tuvieron que enfrentar violaciones públicas a la seguridad: el 53% de los profesionales en 2014 y el 48% en 2015 (Figura 54).

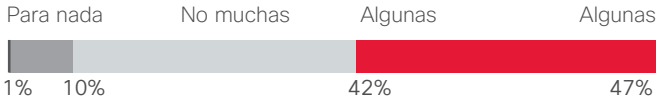
Los profesionales reconocen el valor que las violaciones tienen en términos de hacer un llamado de atención sobre la importancia de fortalecer los procesos de seguridad: el 47% de los profesionales de seguridad afectados por violaciones públicas dijo que las violaciones dieron lugar a mejores políticas y procedimientos. Por ejemplo, el 43% de los encuestados dijo que aumentaron las capacitaciones en seguridad tras una violación pública y el 42% afirmó que aumentaron las inversiones en tecnologías de defensa de seguridad.

La buena noticia es que las organizaciones que sufrieron una violación pública posiblemente fortalezcan cada vez más sus procesos de seguridad. En 2015, el 97% de los profesionales de seguridad dijo que realiza una capacitación en seguridad al menos una vez al año, un fuerte incremento del 82% en 2014 (consulte la Figura 90 en la **página 82**).

Figura 54. Las violaciones públicas pueden mejorar la seguridad

¿Su organización debió enfrentarse alguna vez al escrutinio público tras una violación a la seguridad? (n=1701) (n=1347)

¿Cuántas mejoras impulsó la violación en sus políticas, procedimientos o tecnologías de defensa ante amenazas de seguridad? (n=1134)



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 55. Más organizaciones realizan capacitaciones en seguridad

En 2015, el 43% de los encuestados dijo que las capacitaciones en seguridad aumentaron tras una violación pública.

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

MADUREZ: LAS RESTRICCIONES DE PRESUPUESTO ESTÁN EN PRIMER LUGAR EN CADA NIVEL

A medida que las organizaciones implementan políticas y prácticas de seguridad más sofisticadas, sus percepciones respecto a la preparación para la seguridad pueden cambiar. El Estudio comparativo sobre capacidades de seguridad 2015 de Cisco coloca a los encuestados y sus organizaciones en cinco categorías de madurez, según las respuestas acerca de sus procesos de seguridad (Figura 56). En el estudio se analiza cómo las diferentes características, como las capacidades, los sectores y los países, pueden afectar los niveles de madurez.

Curiosamente, organizaciones en diferentes niveles de madurez parecen compartir algunos de los obstáculos para implementar procesos y herramientas de seguridad más sofisticados. Aunque los porcentajes precisos pueden variar, el desafío de las restricciones de presupuesto se posiciona en el primer lugar de la lista para cada nivel de madurez (Figura 57).

Figura 56. El modelo de madurez clasifica a las organizaciones según los procesos de seguridad

Cisco exploró varias opciones de segmentación de muestra antes de seleccionar una solución de cinco segmentos basada en una serie de preguntas dirigidas a los procesos de seguridad. La solución de cinco segmentos es relativamente similar a la integración de modelos de madurez de capacidades (CMMI).

	Nivel		Solución basada en 5 segmentos
Optimizado	1	Se enfoca en la mejora del proceso	Alto
Administrado cuantitativamente	2	Procesos controlados y medidos cuantitativamente	Medio-alto
Definido	3	Procesos caracterizados para la organización (generalmente proactivos)	Medio
Repetible	4	Procesos caracterizados para los proyectos (generalmente reactivos)	Medio-bajo
Inicial	5	Procesos específicos (impredecibles)	Bajo

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 57. Los obstáculos para adoptar una mejor seguridad no se ven afectados por el nivel de madurez

¿Cuáles de las siguientes opciones considera que son los principales obstáculos para adoptar procesos y tecnología de seguridad avanzada?

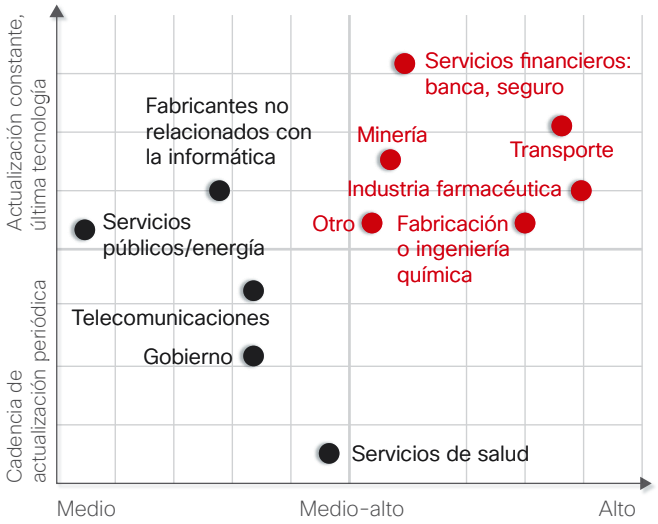
Nivel de sofisticación	Baja	Medio-bajo	Medio	Medio-alto	Alto
Restricciones de presupuesto	41%	48%	39%	38%	38%
Convencimiento de la gerencia superior	14%	20%	20%	22%	19%
Prioridades contrapuestas	19%	27%	26%	26%	22%
Falta de personal capacitado	21%	27%	22%	19%	23%
Falta de conocimiento sobre procesos y tecnologías de seguridad avanzada	31%	20%	25%	23%	22%
Problemas de compatibilidad con sistemas antiguos	21%	28%	29%	34%	33%
Prioridades contrapuestas	14%	17%	26%	27%	25%
Actitud de la cultura organizativa sobre seguridad	31%	23%	22%	25%	22%
Reticencia a comprar hasta que no estén comprobados en el mercado	12%	25%	24%	25%	19%
Carga de trabajo actual muy pesada como para hacerse cargo de nuevas responsabilidades	36%	23%	25%	25%	22%

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

El gráfico a la derecha refleja la calidad de la infraestructura de seguridad y los niveles de madurez de varios sectores. Se basa en las percepciones de los encuestados respecto a sus procesos de seguridad. Los sectores que aparecen en el cuadrante superior derecho registran los niveles más altos de madurez, así como también de la calidad de la infraestructura.

En el gráfico al pie del texto se muestra la ubicación de los niveles de madurez de Cisco por sector. En 2015, casi la mitad de las organizaciones de transporte y farmacéuticas encuestadas se encuentra en el segmento de mayor madurez. Las telecomunicaciones y los servicios públicos tienen menos probabilidades de estar en el segmento de mayor madurez en 2015 en comparación con el año 2014. Los resultados se basan en las percepciones de los encuestados respecto a sus procesos de seguridad.

Figura 58. Evaluación de la madurez de la seguridad por infraestructura y sector



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 59. Niveles de madurez por sector

Distribución de segmentos por país

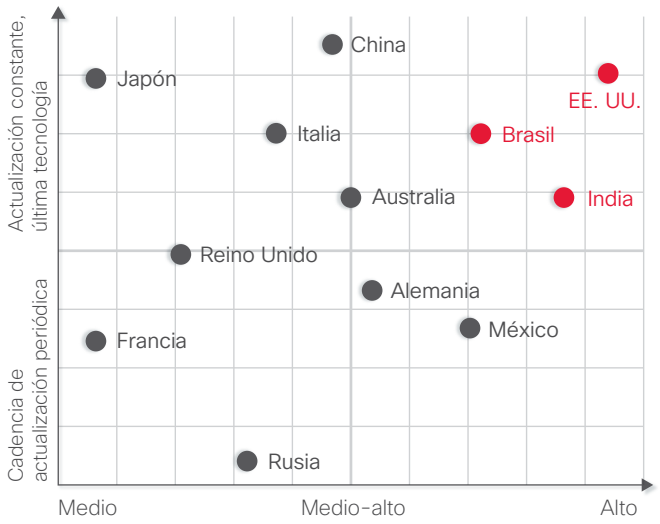
Nivel de sofisticación	Bajo	Medio-bajo	Medio	Medio-alto	Alto
Servicios públicos/ energía	1%	15%	28%	32%	23%
Transporte	1%	5%	28%	20%	46%
Telecomunicaciones	2%	11%	26%	28%	33%
Industria farmacéutica	2%	3%	30%	21%	44%
Fabricantes no relacionados con la informática	1%	10%	34%	22%	32%
Atención médica	1%	10%	30%	22%	37%
Gobierno	3%	10%	28%	25%	34%
Servicios financieros: banca, seguro	1%	10%	26%	26%	38%
Fabricación	1%	6%	21%	33%	39%

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

El gráfico a la derecha refleja la calidad de la infraestructura de seguridad y los niveles de madurez de varios países. Los países que aparecen en el cuadrante superior derecho registran los niveles más altos de madurez, así como también de la calidad de la infraestructura. Es importante tener en cuenta que estas conclusiones se basan en la percepción de los profesionales de seguridad respecto a su preparación para la seguridad.

En el gráfico al pie del texto se muestra la ubicación en los niveles de madurez de Cisco por país. Los resultados se basan en las percepciones de los encuestados respecto a sus procesos de seguridad.

Figura 60. Evaluación de la madurez de la seguridad por infraestructura y país



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 61. Niveles de madurez por país

Distribución de segmentos por país	**2014** (n=1637)				**2015** (n=2401)	
Nivel de sofisticación	2014	Bajo	Medio-bajo	Medio	Medio-alto	Alto
Estados Unidos	3%	10%	27%	16%	44%	
	2%	4%	22%	27%	45%	
Brasil	2%	5%	24%	35%	34%	
	1%	9%	24%	26%	40%	
Alemania	1%	4%	27%	25%	43%	
	1%	12%	24%	24%	39%	
Italia	1%	23%	13%	25%	38%	
	4%	3%	36%	23%	34%	
Reino Unido	8%	8%	25%	18%	41%	
	0%	14%	32%	22%	32%	
Australia	9%	7%	19%	35%	30%	
	1%	5%	29%	36%	29%	
China	0%	3%	32%	29%	36%	
	0%	6%	37%	25%	32%	
India	7%	3%	20%	16%	54%	
	1%	4%	21%	34%	40%	
Japón	7%	15%	14%	40%	32%	
	2%	16%	34%	16%	32%	
México	6%	8%	20%	16%	50%	
Rusia	1%	14%	27%	26%	32%	
Francia	1%	15%	35%	20%	29%	

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

RECOMENDACIONES: RESPONDER A LA CONFRONTACIÓN CON LA REALIDAD

Tal como nuestro Estudio comparativo sobre capacidades de seguridad muestra, la realidad enfrentó a los profesionales de seguridad. La confianza de los profesionales de seguridad en su preparación para bloquear atacantes es dudosa. Sin embargo, las confrontaciones con la realidad proporcionadas por ataques de alto perfil tuvieron un efecto positivo en el sector, a juzgar por el repunte de la capacitación en seguridad y el desarrollo de políticas formales. Además, la subcontratación más frecuente de auditorías y servicios de respuesta ante los incidentes indica que los defensores están buscando la ayuda de expertos.

Las empresas deben seguir aumentando su conciencia sobre su preparación para la seguridad y los profesionales de seguridad deben luchar por el crecimiento de los gastos presupuestarios para respaldar la tecnología y al personal. Además, la confianza aumentará cuando los profesionales de seguridad implementen herramientas que no solo puedan detectar amenazas, sino también que contengan su impacto y aumenten la comprensión de las formas de prevenir ataques futuros.

Una mirada hacia adelante

Una mirada hacia adelante

Los expertos en geopolítica de Cisco ofrecen una perspectiva sobre el panorama cambiante para la gestión de Internet, que comprende cambios en la legislación relativa a la transferencia de datos y el debate sobre el uso de cifrado. En esta sección, también se incluyen conclusiones específicas arrojadas por dos estudios de Cisco. En uno de los estudios se examinan las preocupaciones de los ejecutivos con respecto a la ciberseguridad. En el otro, se aborda la percepción que tienen los responsables de la toma de decisiones de TI acerca de los riesgos de seguridad y la confiabilidad. También ofrecemos una descripción general del valor de una arquitectura de defensa ante amenazas integrada y proporcionamos una actualización del progreso de Cisco en la reducción del tiempo de detección (TTD).

Perspectiva geopolítica: Incertidumbre en el panorama de la gestión de Internet

En la era posterior a Edward Snowden, el panorama geopolítico para la gestión de Internet ha cambiado radicalmente. Actualmente, hay una incertidumbre generalizada en torno al flujo libre de información a través de las fronteras. El caso emblemático presentado por el activista de la privacidad austríaco Max Schrems en contra de Facebook, el gigante de las redes sociales, tuvo, quizás, el mayor impacto, ya que derivó en la anulación del acuerdo Safe Harbor con EE. UU el 6 de octubre de 2015 por parte del Tribunal de Justicia de la Unión Europea (CJEU). [7]

En consecuencia, las empresas ahora deben recurrir a mecanismos y medidas de protección legales diferentes de Safe Harbor cuando transfieren datos de la Unión Europea a los Estados Unidos, los que, a su vez, están sujetos a investigación. Las empresas de datos aún intentan evaluar las repercusiones de este cambio. Mientras que las autoridades de la Unión Europea y de los Estados Unidos han trabajado en el desarrollo de un reemplazo de Safe Harbor durante los últimos dos años, el nuevo mecanismo previsto genera inquietudes. Podría no llegar a materializarse para la fecha límite de enero de 2016 o, lo que es más probable, podría no recuperar la confianza del mercado si no aborda por completo las preocupaciones del CJEU y demuestra, una vez más, correr el riesgo de ser anulado. [8]

Los expertos en protección de datos no esperan que Safe Harbor 2.0 sea menos controvertido que su predecesor. Es posible que, incluso, siga el mismo camino y sea refutado ante el tribunal y también declarado no válido. [9]

El cifrado completo (cómo beneficia a los consumidores y a las organizaciones, y qué desafíos plantea para la autoridad encargada del orden público en sus investigaciones de actividades delictivas y terroristas) también será un tema de mucho debate entre los gobiernos y el sector durante el próximo año. Los ataques terroristas que tuvieron lugar en noviembre de 2015 en París hicieron que algunos creadores de políticas ejerzan incluso más presión para darles a los investigadores la posibilidad de acceder al contenido de comunicaciones cifradas.[10] Esto podría darle un impulso adicional al desarrollo de Safe Harbor 2.0, ya que las preocupaciones por las libertades civiles quedan en segundo plano con respecto a las preocupaciones por la seguridad.

[7] "The Court of Justice declares that the Commission's U.S. Safe Harbour Decision is invalid" (El Tribunal de Justicia declara que la decisión de *Safe Harbor* para los EE. UU tomada por la Comisión Europea no es válida), CJEU, 6 de octubre de 2015: **http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.**

[8] "Safe Harbor 2.0 framework begins to capsize as January deadline nears" (El marco *Safe Harbor 2.0* comienza a zozobrar a medida que se aproxima la fecha límite de enero), por Glyn Moody, *Ars Technica*, 16 de noviembre de 2015: **http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**.

[9] "Safe Harbor 2.0 framework begins to capsize as January deadline nears" (El marco *Safe Harbor 2.0* comienza a zozobrar a medida que se aproxima la fecha límite de enero), por Glyn Moody, *Ars Technica*, 16 de noviembre de 2015: **http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**.

[10] "Paris Attacks Fan Encryption Debate" (Los ataques en Paris avivan el debate en torno al cifrado), por Danny Yadron, Alistair Barr y Daisuke Wakabayashi, *The Wall Street Journal*, 19 de noviembre de 2015: **http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407**.

En medio de semejante incertidumbre, ¿qué deben solicitarles las organizaciones a los proveedores de datos para asegurarse de que el negocio cumpla con las normas de transferencia de datos? A corto plazo, deben, sin lugar a dudas, tener la garantía de que los proveedores se rigen por modelos de cláusulas contractuales o normas corporativas vinculantes de la Unión Europea, y no solo Safe Harbor, cuando transfieren datos desde la Unión Europea.

Otro problema geopolítico importante que las organizaciones deben supervisar se relaciona con las vulnerabilidades y los ataques. Algunos gobiernos expresan estar realmente preocupados por el surgimiento de un mercado de vulnerabilidades sin corrección, denominadas " software como arma". Las herramientas de este tipo son vitales para la comunidad de investigación sobre seguridad, ya que busca maneras de proteger las redes en todo el mundo. Sin embargo, en las manos incorrectas, particularmente en las de regímenes represivos, esta tecnología, diseñada para tareas útiles, podría usarse para cometer delitos financieros, robar secretos nacionales y comerciales, eliminar el disenso político o alterar la infraestructura crítica.

Cómo restringir el acceso a las vulnerabilidades sin corrección sin impedir que las personas que realizan investigaciones esenciales continúen trabajando es un problema con el que los gobiernos indudablemente lidiarán en los próximos meses y años. A medida que los gobiernos intentan solucionar este problema controvertido, deben evaluar cuidadosamente cómo las decisiones sobre la creación de políticas afectan la seguridad. Por ejemplo, la incertidumbre en torno a las disposiciones que rigen la transmisión de información sobre vulnerabilidades no publicadas puede enlentecer el avance de la investigación sobre amenazas a la seguridad o alentar la publicación de vulnerabilidades antes de que los proveedores tengan la oportunidad de corregirlas. Cualquier medida que se adopte para resolver esta incertidumbre debe ser compatible en todo el mundo.

La ciberseguridad: Una preocupación para los ejecutivos

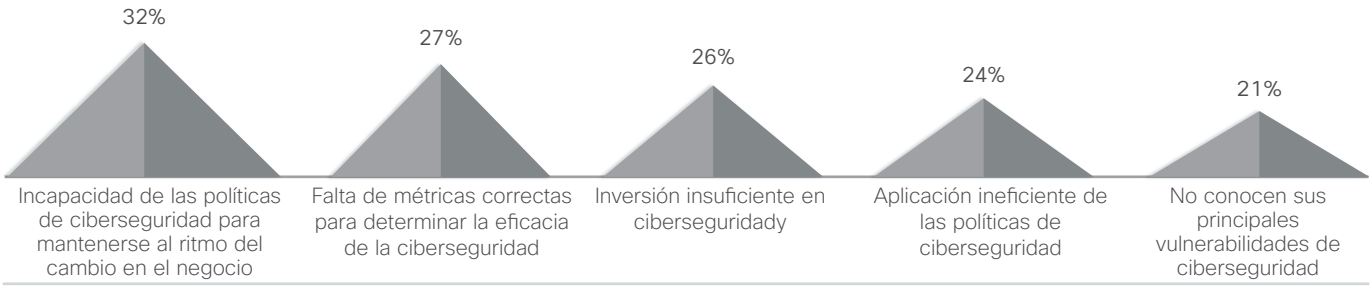
Obviamente, una seguridad integral puede ayudar a las empresas a evitar violaciones y ataques catastróficos. Sin embargo... ¿puede ayudar a mejorar las oportunidades de éxito de una empresa? Según un estudio realizado por Cisco en octubre de 2015 en el que participaron ejecutivos financieros y de la línea de negocios con el objeto de analizar el rol de la ciberseguridad en la estrategia digital y comercial, los ejecutivos empresariales comprenden que proteger el negocio de amenazas puede determinar su posible éxito o fracaso. A medida que las organizaciones se digitalizan cada vez más, el crecimiento dependerá de la capacidad de proteger la plataforma digital.

Tal como refleja la encuesta, la ciberseguridad es una preocupación cada vez mayor para los ejecutivos: el 48% de los encuestados indicó estar muy preocupado y el 39% indicó estar moderadamente preocupado por las violaciones a la ciberseguridad. Esta preocupación está en aumento: el 41% afirmó estar mucho más preocupado por las violaciones a la seguridad ahora que hace tres años y el 42% afirmó estar un poco más preocupado que antes.

Los líderes empresariales también prevén que los inversores y organismos reguladores harán preguntas más rigurosas acerca de los procesos de seguridad, del mismo modo en que interrogan sobre otras funciones empresariales. El 92% de los encuestados estuvo de acuerdo en que los inversores y organismos reguladores esperarán que las empresas proporcionen más información sobre la exposición a riesgos de ciberseguridad en el futuro.

Las empresas también parecen tener una idea clara de los desafíos que enfrentan en torno a la ciberseguridad. La imposibilidad de que las políticas de ciberseguridad avancen al mismo ritmo que los cambios en el negocio fue el desafío mencionado con más frecuencia, seguido por la falta de métricas para determinar la eficacia de la seguridad (Figura 62).

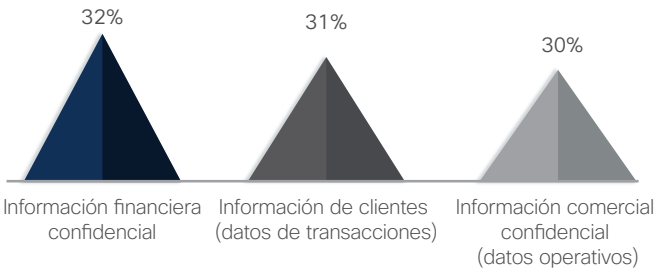
Figura 62. Las empresas enfrentan desafíos de ciberseguridad complejos



Fuente: Cisco Security Research

Alrededor de un tercio de los ejecutivos también está preocupado por su capacidad para proteger datos críticos. Cuando se les pidió que nombren los tipos de datos más difíciles de proteger, el 32% seleccionó “información financiera confidencial”. Los encuestados seleccionaron “información del cliente” e “información comercial confidencial” como los siguientes dos tipos de datos más difíciles de proteger (consulte la Figura 63).

Figura 63. Ejecutivos preocupados por la seguridad de los datos críticos



Fuente: Cisco Security Research

Estudio de confiabilidad: Aclaraciones sobre los riesgos y desafíos para las empresas

El continuo aumento de violaciones a la seguridad informática acentúa la profunda necesidad que tienen las empresas de confiar en que sus sistemas, datos, socios comerciales, clientes y ciudadanos estén seguros. Vemos que la confianza se convierte en un factor importante para los negocios que seleccionan infraestructura de red y TI. De hecho, muchos ahora exigen que la seguridad y la confiabilidad se integren durante todo el ciclo de vida de las soluciones que forman parte de su infraestructura.

En octubre de 2015, Cisco realizó un estudio para evaluar la percepción que tienen los responsables de toma de decisiones de TI acerca de los riesgos de seguridad y los desafíos relacionados, y para determinar el rol que desempeña la confiabilidad del proveedor de TI en las inversiones de TI. Encuestamos a responsables de la toma de decisiones relacionadas y no relacionadas con la seguridad informática en organizaciones de diversos países. (Consulte el **Apéndice** para obtener más información sobre el Estudio de riesgo de seguridad y confiabilidad, que incluye nuestra metodología).

A CONTINUACIÓN, SE INCLUYEN CONCLUSIONES ESPECÍFICAS ARROJADAS POR LA INVESTIGACIÓN:

Descubrimos que el 65% de los encuestados cree que su organización enfrenta un nivel de riesgo de seguridad considerable, que surge concretamente por el uso de movilidad, seguridad de TI y soluciones basadas en la nube en la empresa (Figura 64).

Figura 64. Percepciones de riesgo de seguridad

Fuente: Estudio del riesgo de seguridad y confiabilidad, Cisco

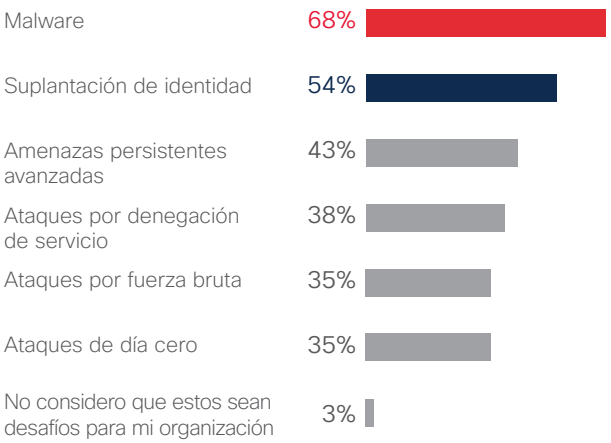
El 68% de los encuestados del estudio identificó que el malware constituye el principal desafío de seguridad externo que enfrenta la organización. A esta respuesta le siguen la suplantación de identidad y las amenazas persistentes avanzadas (APT), con un 54% y 43%, respectivamente (consulte la Figura 65).

En cuanto a los desafíos de seguridad internos (consulte la Figura 66), más de la mitad (54%) de los encuestados mencionó las descargas de software malicioso como la principal amenaza, seguida por las violaciones a la seguridad interna por parte de los empleados (47%) y las vulnerabilidades de hardware y software (46%).

También descubrimos que la mayoría de las empresas (92%) utiliza un equipo de seguridad exclusivo en su organización. El 88% de los encuestados informó contar con una estrategia de seguridad formal en toda la organización, que se renueva regularmente. Sin embargo, solo el 59% dispone de políticas y procedimientos estandarizados vigentes para validar la confiabilidad del proveedor de TI (consulte la Figura 67).

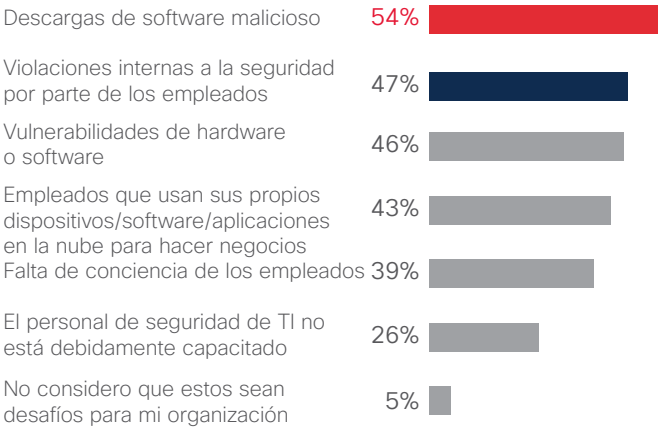
Además, aproximadamente la mitad (49%) de las grandes organizaciones empresariales mantiene su infraestructura de seguridad actualizada con las tecnologías más recientes y la mayoría del resto actualiza la infraestructura con regularidad. De acuerdo con el estudio, muy pocas esperan hasta que la tecnología que utilizan sea obsoleta para actualizar su infraestructura.

Figura 65. Desafíos externos enfrentados (total de encuestados)



Fuente: Estudio del riesgo de seguridad y confiabilidad, Cisco

Figura 66. Desafíos de seguridad internos enfrentados (total de encuestados)



Fuente: Estudio del riesgo de seguridad y confiabilidad, Cisco

Figura 67. La mayoría de las grandes empresas tiene un equipo de seguridad exclusivo local

Fuente: Estudio del riesgo de seguridad y confiabilidad, Cisco

Cómo los proveedores pueden demostrar confiabilidad

En el actual panorama centrado en amenazas, la confianza en los procesos, las políticas, las tecnologías y el personal de un proveedor —y la capacidad para corroborarlos— son fundamentales para entablar una relación duradera y de confianza entre los proveedores y las empresas.

Los proveedores de tecnología demuestran confiabilidad de las siguientes maneras:

- integrando la seguridad en sus soluciones y en la cadena de valor desde un principio;
- contando con políticas y procesos que reducen los riesgos, y respetándolos;
- creando una cultura de concientización sobre la seguridad;
- respondiendo a las violaciones con rapidez y transparencia;
- ofreciendo una solución rápida y una vigilancia constante después de un incidente.

Actualizar la infraestructura es aconsejable, por supuesto. Las organizaciones de todos los tamaños necesitan implementar una infraestructura segura y confiable en la que la seguridad esté integrada en todos los aspectos de la red. Sin embargo, también pueden ayudar a reducir la superficie de ataque fomentando una cultura abierta y consciente con respecto a la seguridad.

El desarrollo de esta cultura requiere que las organizaciones implementen políticas y procesos uniformes en toda la empresa que garanticen que la seguridad sea parte integral de cada aspecto del negocio. Luego, deben trabajar para hacer llegar esta mentalidad centrada en la seguridad al ecosistema de partners y proveedores y para demostrar transparencia y responsabilidad con clientes, partners y otras partes interesadas.

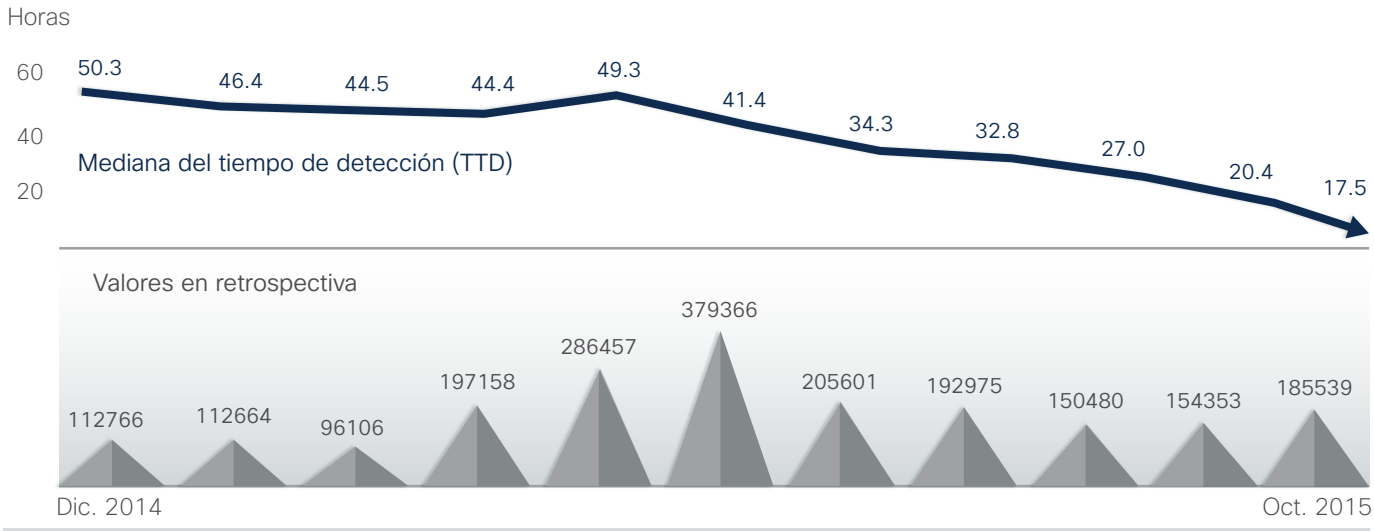
Tiempo de detección: La carrera para seguir acortándolo

Definimos “tiempo de detección” (TTD) como el tiempo que transcurre entre la primera observación de un archivo desconocido y la detección de una amenaza. Determinamos este período mediante la telemetría de seguridad de inclusión voluntaria reunida de los productos de seguridad de Cisco implementados en todo el mundo.

La categoría “Valores en retrospectiva” en la Figura 68 muestra la cantidad de archivos que Cisco clasificó inicialmente como “desconocidos” y que, luego, se convirtieron en “amenazas conocidas”.

Tal como revela el Informe semestral de seguridad 2015 de Cisco, la mediana del TTD era de aproximadamente dos días (50 horas).

Figura 68. Tiempo de detección, de diciembre de 2014 a octubre de 2015



Fuente: Cisco Security Research

De enero a marzo, este valor fue relativamente el mismo: de 44 a 46 horas, pero con una tendencia ligeramente descendiente. En abril, había aumentado apenas a 49 horas. Sin embargo, a fines de mayo, el TTD de Cisco había disminuido aproximadamente a 41 horas.

Desde entonces, la mediana del TTD ha experimentado un rápido descenso. Para octubre, Cisco había reducido este valor a aproximadamente 17 horas (menos de un día). Esto supera ampliamente el cálculo actual de TTD del sector, que es 100 a 200 días. La velocidad se debe a la inclusión de más detalles sobre cómo se mitigan las infecciones efímeras.

La industrialización del hackeo y el mayor uso de malware a través de productos han jugado un rol importante en nuestra capacidad para achicar la ventana de TTD. No bien una amenaza se industrializa, se torna más amplia y, por lo tanto, más fácil de detectar.

Sin embargo, también sugerimos que la combinación de defensas ante amenazas sofisticadas y de una estrecha colaboración entre investigadores expertos en seguridad ha sido quizás mucho más crucial para nuestra capacidad de reducir de manera sistemática y significativa la mediana de TTD durante el 2015.

Figura 69. Comparación de tiempo de detección, de diciembre de 2014 a octubre de 2015

Fuente: Cisco Security Research

La comparación de TTD de la Figura 69 revela que muchas amenazas en junio eran atrapadas en aproximadamente 35,3 horas. En septiembre, una mayor cantidad de amenazas se detenía en aproximadamente 17,5 horas. Una vez más, atribuimos la reducción de la mediana del TTD, en parte, a una identificación más rápida de malware de productos, como Cryptowall 3.0, Upatre y Dyre. La integración de nuevas tecnologías, como las de ThreatGRID, una empresa de Cisco, es otro factor.

Sin embargo, incluso con una ventana reducida de TTD, algunas amenazas siguen siendo más difíciles de detectar que otras. Los programas para descarga orientados a los usuarios de Microsoft Word suelen ser los más fáciles de detectar (menos de 20 horas). Las inyecciones en navegadores y adware se encuentran entre las amenazas más difíciles de detectar (menos de 200 horas).

Una de las razones por la que estas últimas amenazas son tan difíciles de detectar es que, generalmente, los equipos de seguridad las señalan como amenazas de prioridad baja; por lo tanto, suelen ignorarse en el afán de bloquear la arremetida de ataques de día cero (consulte “Las infecciones de navegadores se expanden y son una fuente importante de filtración de datos” en la **página 16**).

En la Figura 70 se proporciona una descripción general de los tipos de amenazas que generalmente aparecen en 100 días.

Figura 70. Nube de etiquetas durante 100 días

Source: Cisco Security Research

COMPARTIR

Los seis principios de una defensa ante amenazas integrada

En el Informe semestral de seguridad 2015 de Cisco, los expertos en seguridad de Cisco afirmaron que la necesidad de soluciones adaptables e integradas dará lugar a cambios importantes en el sector de seguridad en los próximos cinco años. Los resultados serán la consolidación del sector y un movimiento unificado hacia una arquitectura de defensa ante amenazas escalable e integrada. Una arquitectura de este tipo proporcionará visibilidad, control, inteligencia y contexto a través de varias soluciones.

Este marco de trabajo de "detección y respuesta" permitirá brindar una respuesta más rápida ante amenazas conocidas y emergentes. En el centro de esta nueva arquitectura habrá una plataforma de visibilidad que ofrecerá reconocimiento contextual total y que se actualizará continuamente para evaluar amenazas, correlacionar la inteligencia local y global, y optimizar las defensas. El objetivo de esta plataforma es crear una base en la que todos los proveedores puedan operar y con la que puedan contribuir. La visibilidad ofrece más control y esto permite una mejor protección contra más vectores de amenaza y la capacidad de frustrar más ataques.

A continuación, presentamos seis principios de defensa ante amenazas integrada para ayudar a las organizaciones –y a sus proveedores de seguridad– a comprender mejor la intención y los posibles beneficios de esta arquitectura:

1. **Se necesita una arquitectura de red y seguridad más eficiente para manejar el volumen y la sofisticación en aumento de los artífices de amenazas.**

   Durante los últimos 25 años, el modelo tradicional de seguridad ha sido "se detecta un problema, se compra un solución". Sin embargo, estas soluciones, a menudo una serie de tecnologías de diversos proveedores de seguridad, no pueden comunicarse entre sí de ninguna manera significativa. Elaboran información e inteligencia sobre eventos de seguridad, las que se integran en una plataforma de eventos y luego son analizadas por el personal de seguridad.

   Una arquitectura integrada de defensa ante amenazas es un marco de detección y respuesta que ofrece más capacidades y permite respuestas más rápidas ante amenazas mediante la recopilación de más información de la infraestructura instalada en forma automatizada y eficiente. El marco observa el entorno de seguridad de una manera más inteligente. En lugar de alertar a los equipos de seguridad sobre eventos sospechosos y violaciones de políticas, puede brindar un panorama claro de la red y de lo que está sucediendo en ella para una mejor toma de decisiones relacionadas con la seguridad.

2. **Contar con la mejor tecnología de su clase no alcanza para hacer frente al panorama de amenazas actual o futuro; simplemente aumenta la complejidad del entorno de red.**

   Las organizaciones invierten en las mejores tecnologías de seguridad, pero, ¿cómo saben si esas soluciones están funcionando de verdad? Las noticias sobre importantes violaciones a la seguridad durante el último año demuestran que muchas tecnologías de seguridad no están funcionando correctamente. Y cuando fallan, es un gran problema.

   Una proliferación de proveedores de seguridad que ofrecen las mejores soluciones de su clase no es ayuda para mejorar el entorno de seguridad, a menos que dichos proveedores ofrezcan soluciones radicalmente diferentes (no solo un poco diferentes) de las que ofrecen sus competidores. Pero, en la actualidad, no hay diferencias claras en muchas de las ofertas de proveedores líderes orientadas a la mayoría de las áreas centrales de la seguridad.

3. **Para un mayor tráfico cifrado, se necesitará una defensa ante amenazas integrada capaz de reunir la actividad maliciosa cifrada que hace que determinados productos puntuales se vuelvan ineficientes.**

   Como se analizó en este informe, el tráfico web cifrado se encuentra en aumento. Existen buenas razones para usar cifrado, obviamente, pero el cifrado también les dificulta el seguimiento de amenazas a los equipos de seguridad.

   La respuesta al "problema" del cifrado es tener más visibilidad de lo que sucede en los dispositivos o en las redes. Las plataformas de seguridad integrada pueden dar esta respuesta.

4. **Las API abiertas son fundamentales para una arquitectura de defensa ante amenazas integrada.**

   Los entornos de múltiples proveedores necesitan una plataforma común que proporcione más visibilidad, contexto y control. El desarrollo de una plataforma de integración front-end puede respaldar una mayor automatización e integrar un mejor reconocimiento en los mismos productos de seguridad.

5. **Una arquitectura de defensa ante amenazas integrada requiere menos equipos y software para instalar y administrar.**

   Los proveedores de seguridad deben esforzarse por brindar plataformas que ofrezcan la mayor cantidad de características posible y funcionalidad extendida en una plataforma. Esto permitirá reducir la complejidad y la fragmentación en el entorno de seguridad, las que crean muchísimas oportunidades para el fácil acceso y ocultamiento de los atacantes.

6. **Los aspectos de automatización y coordinación de una defensa ante amenazas integrada ayudan a reducir el tiempo de detección, contención y corrección.**

   Si los casos de falsos positivos disminuyen, los equipos de seguridad pueden centrarse en lo que es más importante. La contextualización respalda el análisis de primera línea de los eventos en curso, ayuda a los equipos a evaluar si esos eventos requieren atención inmediata y puede, en última instancia, generar respuestas automatizadas y análisis más profundos.

Poder en números: El valor de la colaboración en el sector

La colaboración en el sector es esencial no solo para desarrollar una futura arquitectura para una defensa ante amenazas integrada que permitirá una respuesta más rápida ante amenazas, sino también para seguirle el ritmo hoy a una comunidad global de artífices de amenazas cada vez más atrevidos, innovadores y persistentes. Los atacantes se están volviendo más expertos en la implementación de campañas altamente rentables y difíciles de detectar. Actualmente, muchos utilizan recursos legítimos en la infraestructura para respaldar sus campañas y lo hacen con gran éxito.

Ante este panorama, no resulta sorprendente que los defensores encuestados en el Estudio comparativo sobre capacidades de seguridad 2015 de Cisco tengan menos confianza en su capacidad para ayudar a proteger su organización. Sugerimos que los defensores tengan en cuenta el enorme impacto que la colaboración dinámica y continua del sector puede tener en revelar la actividad de los ciberdelincuentes, debilitar la capacidad de generar ingresos de los atacantes y reducir la oportunidad de lanzar ataques futuros.

Tal como lo analizamos en profundidad anteriormente en este informe (consulte “Casos destacados”, a partir de la **página 10**), la colaboración entre un partner colaborador de Cisco y dentro de nuestro ecosistema Cisco Collective Security Intelligence (CSI), y la cooperación con los proveedores de servicios fueron factores importantes en la capacidad de Cisco para detectar, verificar e impedir las operaciones globales que involucraban al kit de ataque Angler y para debilitar uno de los botnets de DDoS más grandes que los investigadores jamás hayan observado, SSHPsychos.

Acerca de Cisco

Acerca de Cisco

Cisco ofrece ciberseguridad inteligente para el mundo real a través de uno de los portafolios de soluciones de protección avanzada contra amenazas más integrales del sector, que aborda la gama más amplia de vectores de ataque. El enfoque sobre la seguridad de Cisco, operativo y centrado en amenazas, reduce la complejidad y la fragmentación al tiempo que proporciona visibilidad superior, control uniforme y protección avanzada contra amenazas antes, durante y después de un ataque.

Los investigadores especializados en amenazas del ecosistema Collective Security Intelligence (CSI) reúnen, en una misma estructura, la inteligencia de amenazas líder del sector; para ello, usan la telemetría obtenida de la enorme impronta de dispositivos y sensores, fuentes públicas y privadas, y la comunidad de código abierto de Cisco. Esto equivale a un ingreso diario de miles de millones de solicitudes web y millones de correos electrónicos, muestras de malware e intrusiones en las redes.

Nuestra sofisticada infraestructura y nuestros sistemas utilizan esta telemetría, lo que permite a investigadores y sistemas de aprendizaje automático seguir las amenazas en las redes, los centros de datos, los terminales, los dispositivos móviles, los sistemas virtuales, la web, los correos electrónicos y la nube a fin de identificar las causas principales y examinar el alcance del daño causado. La inteligencia resultante se traduce en protecciones en tiempo real para nuestra oferta de productos y servicios que se distribuyen inmediatamente a los clientes internacionales de Cisco.

Para obtener más información sobre el enfoque de seguridad centrado en amenazas de Cisco, visite **www.cisco.com/go/security**.

Colaboradores del informe anual de seguridad 2016 de Cisco

GRUPO DE INVESTIGACIÓN E INTELIGENCIA DE SEGURIDAD TALOS

Talos es una organización de inteligencia de amenazas de Cisco, un grupo selecto de expertos de seguridad dedicados a brindar protección superior para los clientes, productos y servicios de Cisco. Talos está compuesto por investigadores líderes especializados en amenazas y respaldados por sistemas sofisticados que les permiten crear inteligencia de amenazas para los productos Cisco que detectan, analizan y protegen contra las amenazas conocidas y emergentes. Talos mantiene el conjunto de reglas oficiales de Snort.org, ClamAV, SenderBase.org y SpamCop, y es el equipo principal que aporta información sobre amenazas al ecosistema Cisco CSI.

EQUIPO DE TRANSFORMACIÓN Y OPTIMIZACIÓN DE LA NUBE Y DE TI DE ADVANCED SERVICES

El equipo proporciona recomendaciones y optimiza redes, centros de datos y soluciones en la nube para las empresas y los proveedores de servicios más grandes del mundo. Esta oferta de consultoría se centra en maximizar la disponibilidad, el rendimiento y la seguridad de las soluciones críticas de los clientes. El servicio de optimización se presta a más del 75% de empresas Fortune 500.

EQUIPO ACTIVE THREAT ANALYTICS

El equipo Active Threat Analytics (ATA) de Cisco permite que las organizaciones se defiendan contra las intrusiones conocidas, los ataques de día cero y las amenazas persistentes avanzadas aprovechando las tecnologías avanzadas de datos masivos. La prestación de este servicio totalmente administrado está a cargo de nuestros expertos en seguridad y nuestra red global de centros de operaciones de seguridad. Ofrece vigilancia constante y análisis a pedido las 24 horas, todos los días.

CISCO THOUGHT LEADERSHIP ORGANIZATION

Cisco Thought Leadership Organization arroja luz sobre las oportunidades, las transiciones del mercado y las soluciones claves globales que transforman las organizaciones, los sectores y las experiencias. Esta organización ofrece una mirada incisiva y predictiva de lo que pueden esperar las empresas en un mundo que cambia rápidamente y del modo en que pueden competir mejor. La mayor parte del liderazgo intelectual del equipo se centra en ayudar a las organizaciones a digitalizarse tendiendo un puente entre los entornos físicos y virtuales, de un modo seguro y sin inconvenientes, para introducir innovaciones más rápidamente y obtener los resultados comerciales deseados.

COGNITIVE THREAT ANALYTICS

Cognitive Threat Analytics de Cisco es un servicio basado en la nube que detecta violaciones, malware que funciona dentro de redes protegidas y otras amenazas a la seguridad mediante al análisis estadístico de los datos del tráfico de red. Esta solución aborda las brechas de las defensas perimétricas mediante la identificación los síntomas de una infección de malware o violación de datos; para ello, hace uso del análisis de comportamiento y la detección de anomalías. Cisco Cognitive Threat Analytics depende del modelado estadístico avanzado y del aprendizaje automático para identificar amenazas nuevas de manera independiente, aprender de lo que ve y adaptarse con el tiempo.

ASUNTOS GUBERNAMENTALES GLOBALES

Cisco se relaciona con gobiernos en distintos niveles para colaborar en la creación de normas y políticas públicas que respaldan el sector tecnológico y ayudan a los gobiernos a alcanzar sus objetivos. El equipo de Asuntos gubernamentales globales desarrolla y ejerce influencia en las normas y las políticas públicas a favor de la tecnología. Mediante el trabajo en colaboración con las partes interesadas del sector y partners asociados, el equipo entabla relaciones con líderes gubernamentales para ejercer influencia en las políticas que afectan el negocio de Cisco y la adopción general de tecnologías de la información y la comunicación (TIC), con la intención de ayudar a crear decisiones sobre políticas tanto a nivel local como nacional y global. El equipo de Asuntos gubernamentales está compuesto por exfuncionarios electos, miembros del Parlamento, reguladores, altos funcionarios gubernamentales de EE. UU. y profesionales de asuntos gubernamentales que ayudan a Cisco a promover y proteger el uso de la tecnología en todo el mundo.

EQUIPO INTELLISHIELD

El equipo IntelliShield realiza la investigación, el análisis, la integración y la correlación de datos e información relacionados con amenazas y vulnerabilidades provenientes de Cisco Security Research & Operations y fuentes externas para brindar el servicio de inteligencia de seguridad IntelliShield, que respalda diversos productos y servicios de Cisco.

LANCOPE

Lancope, una empresa de Cisco, es un proveedor líder de visibilidad de red e inteligencia de seguridad para proteger las empresas contra las principales amenazas de la actualidad. Mediante el análisis de NetFlow, IPFIX y otros tipos de telemetría de red, el sistema StealthWatch® de Lancope ofrece análisis de seguridad sensible al contexto para detectar rápidamente una amplia gama de ataques, que comprende desde APT y DDoS hasta amenazas internas y malware de día cero. Mediante la combinación de supervisión lateral continua de todas las redes empresariales con el reconocimiento de aplicaciones, dispositivos y usuarios, Lancope acelera la respuesta ante los incidentes, mejora las investigaciones forenses y reduce los riesgos de la empresa.

OPENDNS

OpenDNS, una empresa de Cisco, es la plataforma de seguridad basada en la nube más grande del mundo. Presta servicio a más de 65 millones de usuarios a diario, distribuidos en más de 160 países. OpenDNS Labs es el equipo de investigación de seguridad de OpenDNS que da soporte a la plataforma de seguridad. Para obtener más información, visite **www.opendns.com** o **https://labs.opendns.com**.

SECURITY AND TRUST ORGANIZATION

Security and Trust Organization, de Cisco, subraya el compromiso que asume Cisco para abordar dos de los problemas más críticos que son la principal prioridad de salas de juntas y líderes mundiales por igual. Las tareas centrales de esta organización incluyen brindar protección a clientes públicos y privados de Cisco, habilitar y garantizar iniciativas de Ciclo de vida del desarrollo seguro y de Sistemas confiables de Cisco en todo el portafolio de productos y servicios de Cisco, y brindar protección a Cisco contra amenazas cibernéticas cambiantes. Cisco adopta un enfoque integral hacia la seguridad y la confianza generalizadas, que comprende personas, políticas, procesos y tecnología. Security and Trust Organization impulsa la excelencia operativa centrándose en seguridad informática, ingeniería confiable, protección y privacidad de datos, seguridad en la nube, transparencia y validación, e investigación y gestión de seguridad avanzada. Para obtener más información, visite **http://trust.cisco.com.**

SECURITY RESEARCH AND OPERATIONS (SR&O)

Security Research and Operations (SR&O) es responsable de la gestión de amenazas y vulnerabilidades de todos los productos y servicios de Cisco, incluido el Equipo de respuesta a incidentes de seguridad de productos (PSIRT), líder del sector. SR&O ayuda a los clientes a comprender el panorama de amenazas en evolución a través de eventos, como Cisco Live y Black Hat, y también a través de la colaboración con sus pares en Cisco y el sector. Además, SR&O introduce innovaciones para prestar nuevos servicios, como inteligencia de amenazas personalizada (CTI) de Cisco, que puede identificar indicadores de riesgo que no han sido detectados ni mitigados por las infraestructuras de seguridad existentes.

Partner colaborador de Cisco

LEVEL 3 THREAT RESEARCH LABS

Level 3 Communications es un proveedor líder en comunicaciones globales, con sede central en Broomfield, Colorado, EE.UU. Presta servicios de comunicaciones a empresas, gobiernos y operadoras. Su plataforma global de servicios, con extensas redes de fibra óptica en tres continentes y conectada por instalaciones submarinas, cuenta con amplios recursos metropolitanos, que llegan a más de 500 mercados en más de 60 países. La red de Level 3 brinda una vista amplia del panorama de amenazas global.

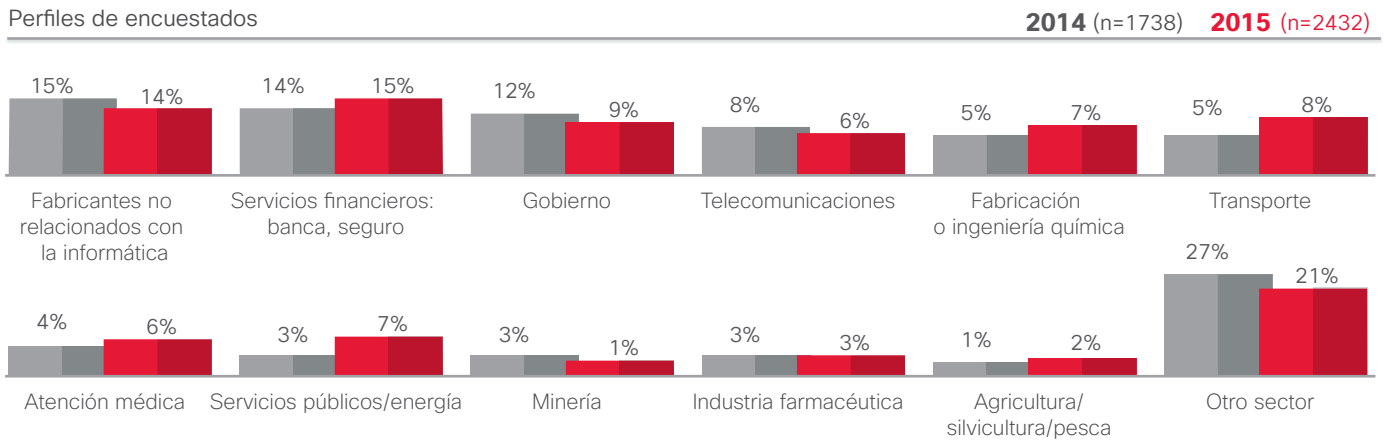
Level 3 Threat Research Labs es el grupo de seguridad que analiza dinámicamente el panorama de amenazas global y correlaciona la información de fuentes internas y externas con el fin de ayudar a proteger a clientes de Level 3, su red y la Internet pública. El grupo se asocia regularmente con los líderes del sector, como Cisco Talos, para ayudar a investigar y mitigar amenazas.

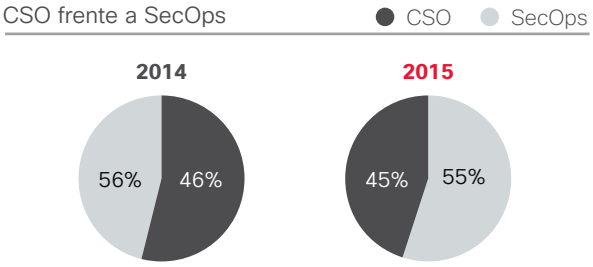
Apéndice

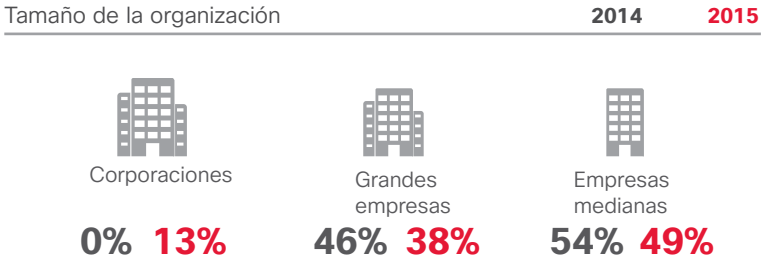
Apéndice

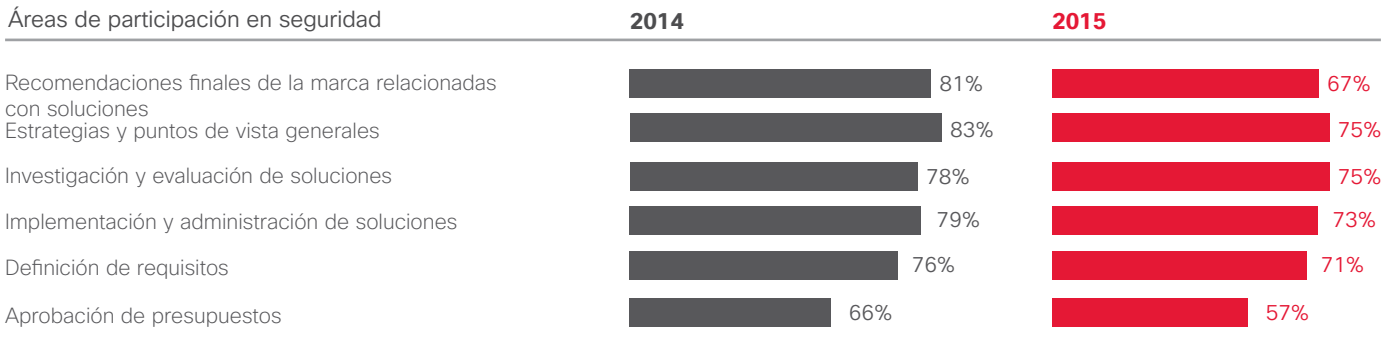
Estudio comparativo sobre capacidades de seguridad de Cisco 2015: Perfiles y recursos de los encuestados

Figura 71. Perfiles de los encuestados





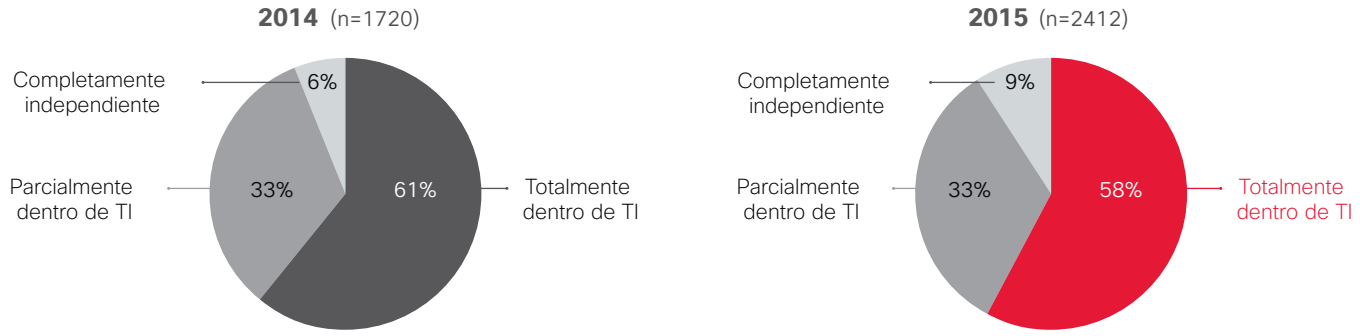




Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 72. Aunque solo el 9% tenga un presupuesto de seguridad aparte del presupuesto de TI, este porcentaje ha aumentado considerablemente desde 2014

¿Forma parte del presupuesto de TI el presupuesto de seguridad? (Miembros del departamento de TI)



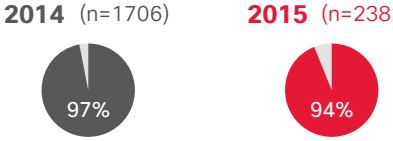
Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 73. Cargos: Los encuestados y sus gerentes

Miembros del departamento de TI

Departamento o equipo especializado en seguridad

Miembros de un equipo de seguridad



Cargo		Cargo del gerente	
Director general de seguridad	22%	Director general	34%
Director general de tecnología	18%	Presidente/propietario	18%
Director o gerente de TI	16%	Director general de seguridad	6%
Director general de información	13%	Director general de información	6%
Director de operaciones de seguridad	7%	Director general de tecnología	6%
Vicepresidente de seguridad informática	5%	Director o gerente de TI	4%
Responsable de cumplimiento y riesgo	4%	Vicepresidente de seguridad informática	4%
Gerente de operaciones de seguridad	4%	Vicepresidente de TI	2%
Arquitecto de seguridad	4%	Directorio	2%
Vicepresidente de TI	3%	Director general de operaciones	1%
Director general de operaciones	3%	Director general de finanzas	1%
Otro cargo	2%	Otro cargo	0%

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 74. El firewall es la herramienta de defensa ante amenazas de seguridad utilizada con más frecuencia; en comparación con el 2014, en el 2015 una menor cantidad de defensas ante amenazas de seguridad se administra a través de servicios basados en la nube.

Defensas contra amenazas de seguridad utilizadas por la organización	**2014** (n=1738)	**2015** (n=2432)	Defensas administradas a través de los servicios basados en la nube (encuestados sobre seguridad que utilizan las defensas contra amenazas de seguridad) **2014** (n=1646)	**2015** (n=2268)
Firewall*	N/D	65%		31%
Prevención de pérdida de datos	55%	56%		
Autenticación	52%	53%		
Cifrado/privacidad/protección de datos	53%	53%		
Seguridad de mensajería/correo electrónico	56%	52%	37%	34%
Seguridad web	59%	51%	37%	31%
Protección terminal/anti-malware	49%	49%	25%	25%
Control de acceso/autorización	53%	48%		
Administración de identidad/aprovisionamiento de usuarios	45%	45%		
Prevención de intrusiones*	N/D	44%		20%
Seguridad móvil	51%	44%	28%	24%
Tecnología inalámbrica protegida	50%	41%	26%	19%
Análisis de vulnerabilidades	48%	41%	25%	21%
VPN	48%	40%	26%	21%
Administración de información y eventos de seguridad	43%	38%		
Defensa de DDoS	36%	37%		
Prueba de penetración	38%	34%	20%	17%
Revisión y configuración	39%	32%		
Informática forense de red	42%	31%		
Informática forense de terminales	31%	26%		
Red, seguridad, firewalls y prevención de intrusiones*	60%	N/A	35%	
Ninguna de las opciones anteriores	1%	1%	13%	11%

*El firewall y la prevención de intrusiones constituían un código en 2014: "Seguridad de la red, firewalls y prevención de intrusiones"

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

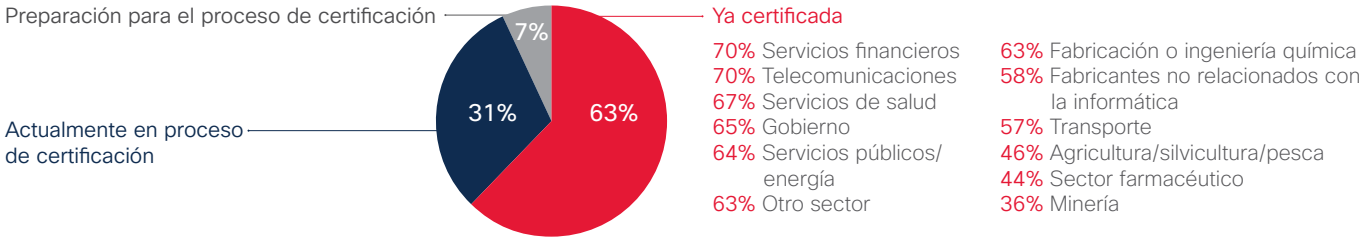
Subcontratación

Figura 75. Los servicios de asesoramiento y consultoría siguen siendo los servicios de seguridad más subcontratados

Considerables aumentos en la subcontratación de auditoría y respuesta ante incidentes. La subcontratación se considera más rentable.

La mitad (el 52%) sigue una práctica estandarizada de políticas de seguridad, como ISO 27001, igual que el año pasado. De estas, la gran mayoría ya está certificada o por obtener la certificación.

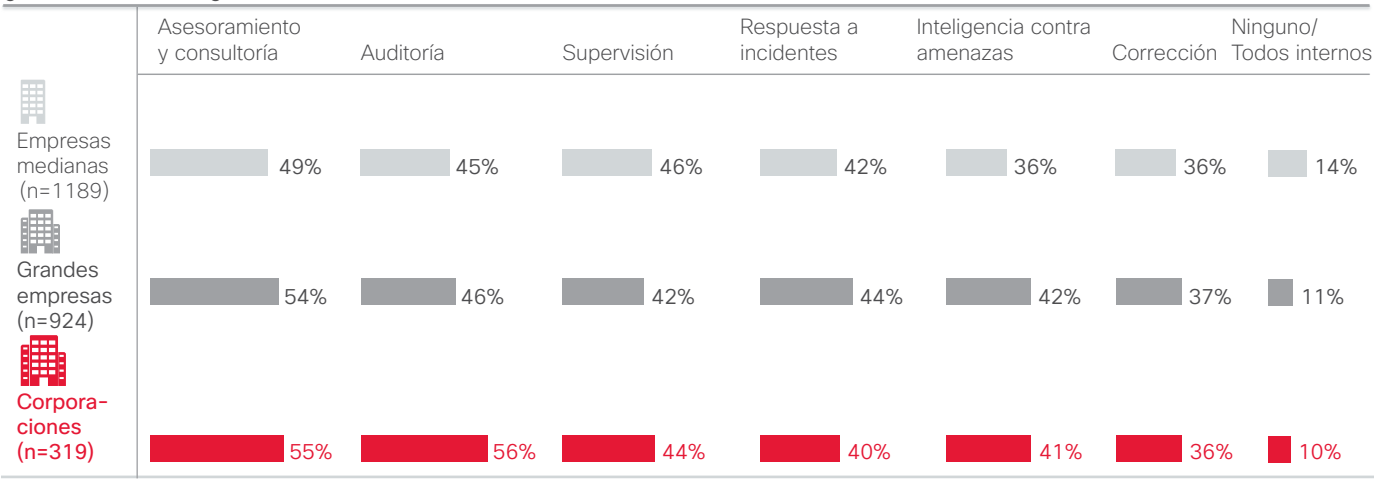
Práctica estandarizada de políticas de seguridad
La organización sigue la práctica estandarizada de políticas de seguridad de la información (**2015**: n=1265)



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 76. Vista de subcontratación por empresa: Las grandes empresas tienen muchas más probabilidades de subcontratar servicios de auditoría, asesoramiento y consultoría

¿Qué servicios de seguridad se subcontratan?



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

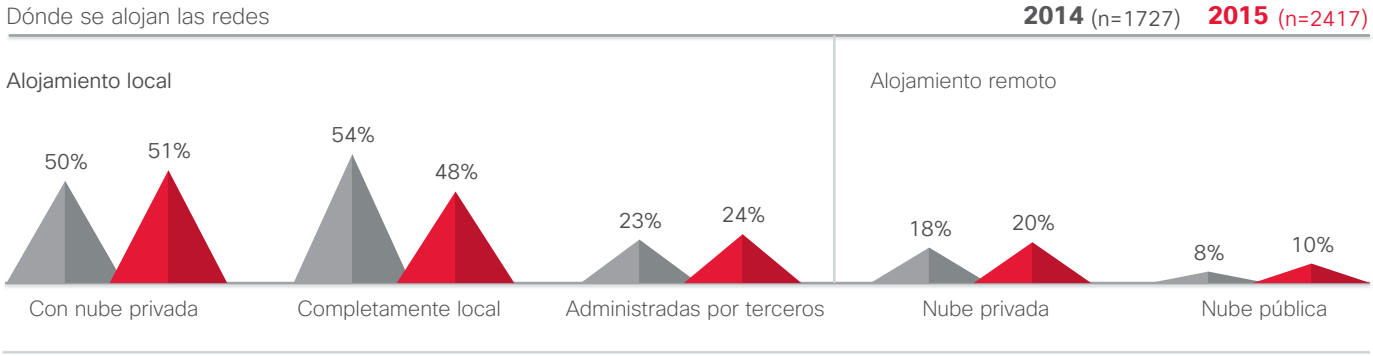
Figura 77. Vista de subcontratación por país: Japón tiene muchas más probabilidades de subcontratar servicios de asesoramiento y consultoría

¿Qué servicios de seguridad se subcontratan?

TOTAL	EE. UU	Brasil	Alemania	Italia	Reino Unido	Australia	China	India	Japón	México	Rusia	Francia
Asesoramiento y consultoría 52%	52%	51%	19%	51%	44%	54%	52%	54%	64%	58%	41%	55%
Auditoría 47%	50%	55%	38%	48%	50%	36%	33%	51%	41%	63%	40%	59%
Supervisión 44%	48%	49%	32%	39%	41%	52%	31%	51%	51%	49%	37%	50%
Respuesta a incidentes 42%	46%	39%	32%	38%	43%	53%	34%	49%	53%	45%	27%	54%
Inteligencia contra amenazas 39%	42%	40%	37%	46%	36%	16%	36%	48%	47%	44%	42%	39%
Corrección 36%	34%	32%	38%	34%	31%	47%	37%	41%	40%	21%	41%	41%
Ninguno/Todos internos 12%	18%	9%	18%	13%	19%	4%	19%	12%	10%	3%	16%	4%

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 78. El alojamiento local de las redes sigue siendo el más habitual; sin embargo, el alojamiento remoto ha aumentado desde el año pasado.



Source: Cisco 2015 Security Capabilities Benchmark Study

Brecha de seguridad pública

Figura 79. En 2015 una menor cantidad de organizaciones informa haber tenido que enfrentarse al escrutinio público tras una violación a la seguridad

Security Breaches Are Strong Drivers of Security Improvements:

Fewer Organizations in **2015** Report Having Had to Manage Public Scrutiny of Security Breaches Compared to **2014**.

2014 **53%** vs 2015 **48%**

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

How Much Did the Breach Drive Improvements in Your Security Threat Defense Policies, Procedures, or Technologies? (n=1134)

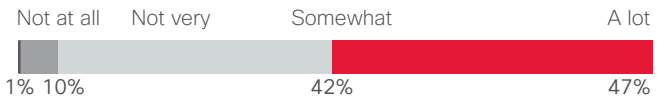


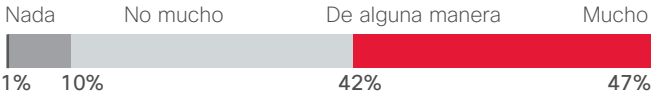
Figura 80. Las violaciones públicas pueden mejorar la seguridad

Las violaciones a la seguridad son factores importantes que motivan las mejoras en la seguridad:

Respondents Dedicated to Security.**2014** (n=1701) **2015** (n=1347)

2014 **53%** Yes en comparación con 2015 **48%** Yes

¿En qué medida la violación motivó mejoras en materia de políticas, procedimientos o tecnologías para la defensa ante amenazas a la seguridad? (n= 1134)



Los directores de seguridad señalan una mayor cantidad de mejoras tras una violación a la seguridad que los gerentes de operaciones de seguridad.

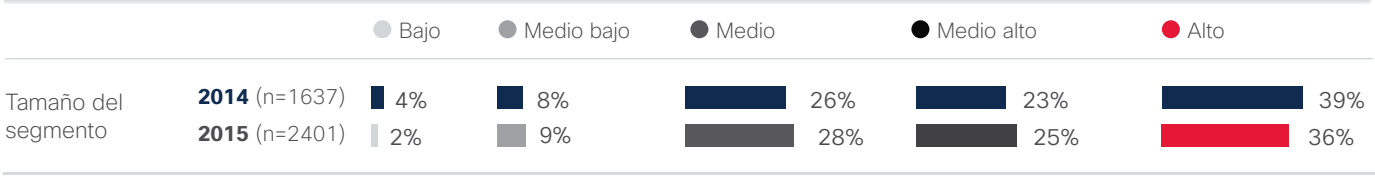
Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Liderazgo y madurez

Figura 81. El modelo de 5 segmentos sigue de cerca el modelo de madurez de capacidades (CMM) de seguridad.

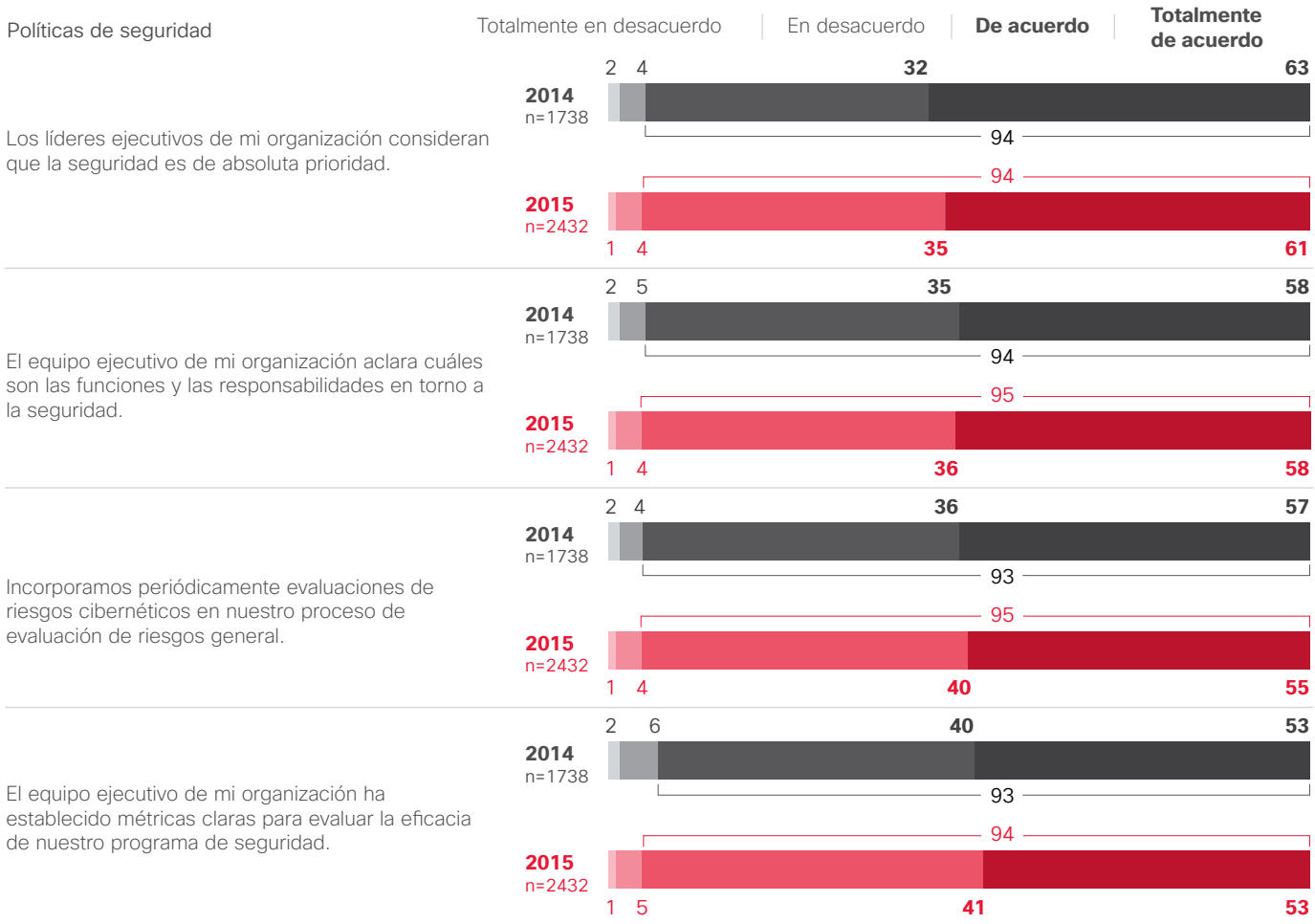
Los segmentos reflejan un patrón similar al arrojado por el estudio del año pasado en cuanto a la madurez en torno a la prioridad que tiene la seguridad y al modo en que esto se traduce en procesos y procedimientos.

Un **60%** o más encajan en perfiles de más madurez en torno a la seguridad. Esto sucede en la mayoría de los casos, en distintos países y sectores.



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 82. Tal como sucedió en el 2014, prácticamente todos estuvieron de acuerdo o totalmente de acuerdo con la declaración de que los líderes ejecutivos consideran que la seguridad es de absoluta prioridad



Una cantidad considerablemente mayor de encuestados del sector farmacéutico manifiesta estar totalmente de acuerdo con la declaración "El equipo ejecutivo de mi organización ha establecido métricas claras para evaluar la eficacia de nuestro programa de seguridad" en comparación con los profesionales de la mayoría de los demás sectores.

Una cantidad considerablemente mayor de directores de seguridad concuerda con todas las declaraciones en torno a la participación del equipo ejecutivo en comparación con el sector de operaciones de seguridad.

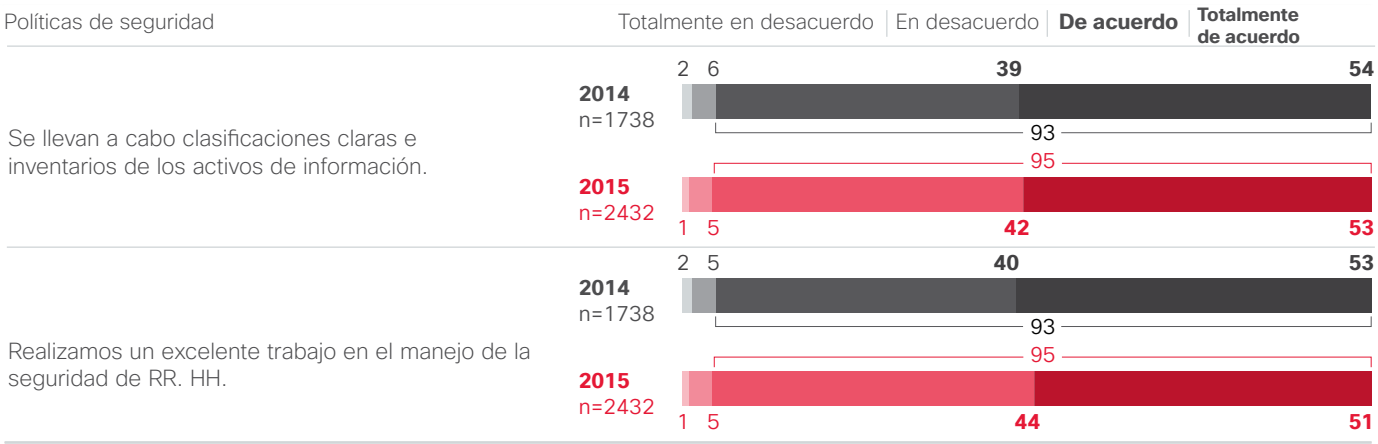
Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Procesos

Figura 83. Confianza variada en la capacidad de integrar la seguridad en los sistemas

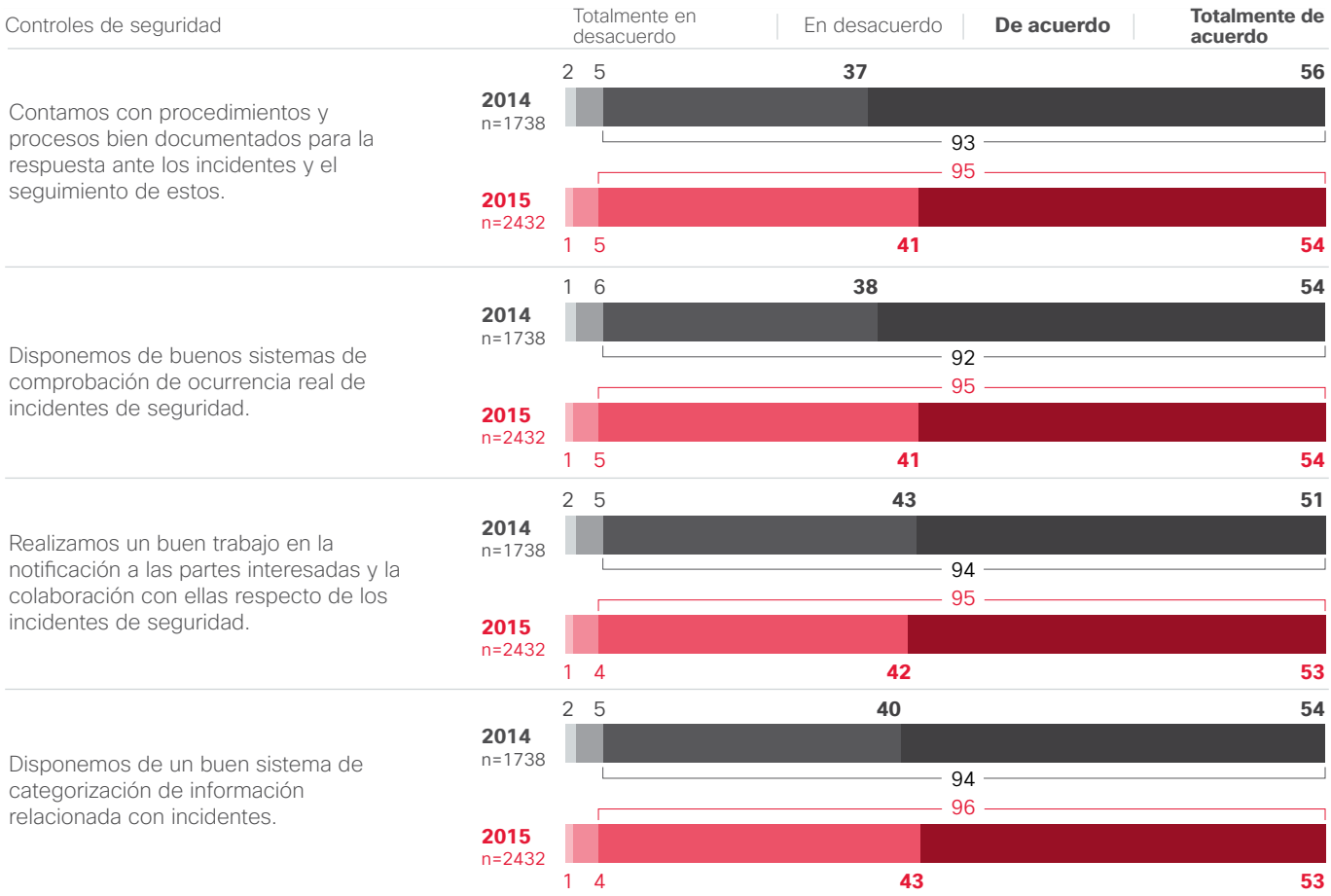
Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 83. Confianza variada en la capacidad de integrar la seguridad en los sistemas (continuación)



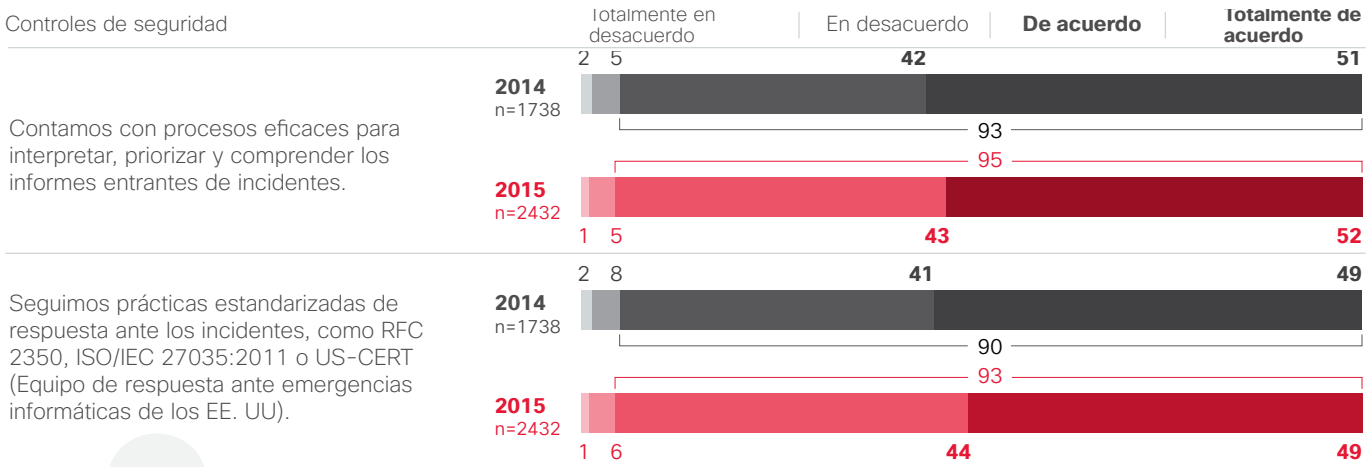
Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 84. Las empresas creen que disponen de buenos controles de seguridad



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 84. Las empresas creen que disponen de buenos controles de seguridad (continuación)



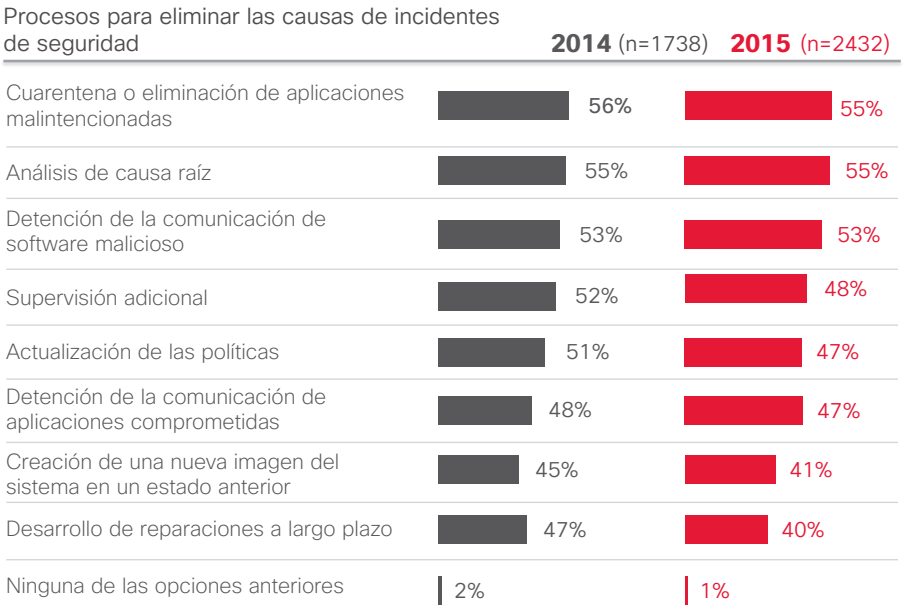
Los encuestados pertenecientes al sector de servicios financieros tienen más posibilidades de estar totalmente de acuerdo con la declaración "Disponemos de un buen sistema de categorización de información relacionada con incidentes" en comparación con los profesionales de la mayoría de los demás sectores.

Salvo por la declaración "Realizamos un buen trabajo en la notificación a las partes interesadas y la colaboración con ellas respecto de los incidentes de seguridad", los directores de seguridad tienen una actitud más positiva con respecto a los atributos en torno a los controles de seguridad que los gerentes de operaciones de seguridad.

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

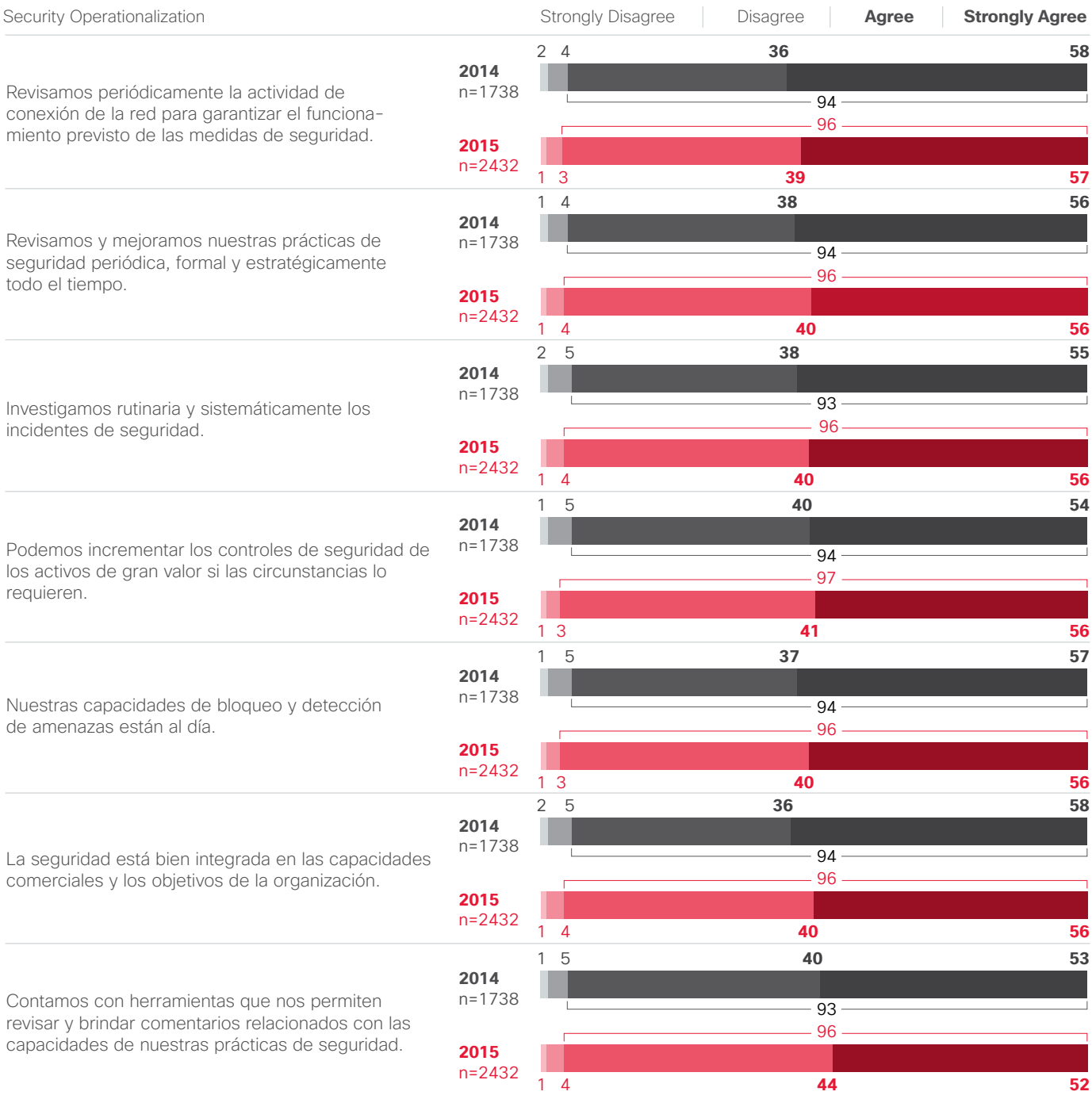
Figura 85. Poner en cuarentena/eliminar aplicaciones maliciosas y realizar análisis de causa raíz siguen siendo los principales procesos utilizados

Una cantidad considerablemente mayor de encuestados de EE. UU. opta por la respuesta "Ninguna de las opciones anteriores" cuando se le pregunta sobre procesos para eliminar la causa de un incidente de seguridad en comparación con los encuestados de la mayoría de los otros países.



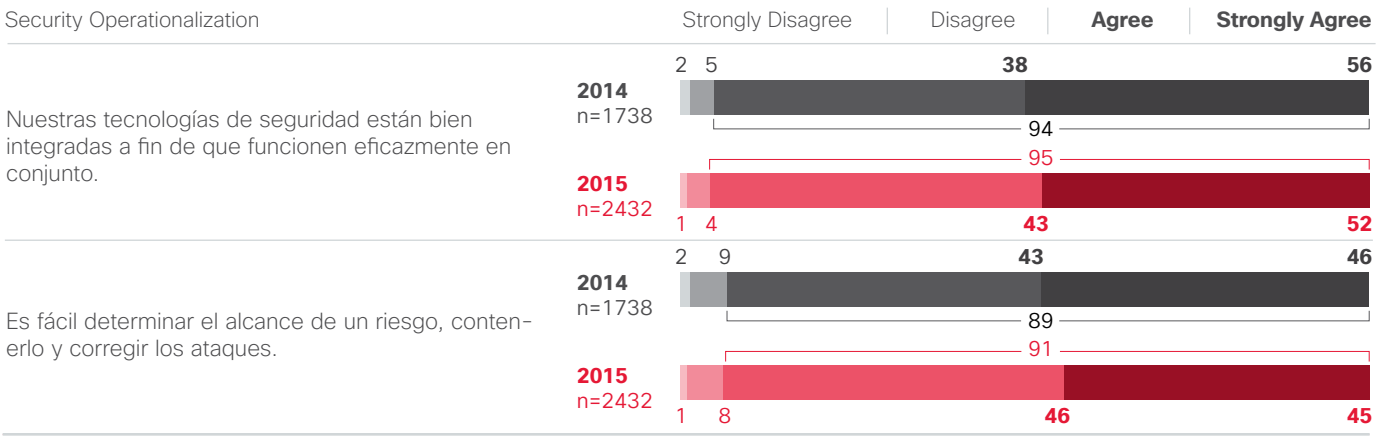
Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 86. Las empresas demuestran una confianza variada en la capacidad de contener riesgos



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

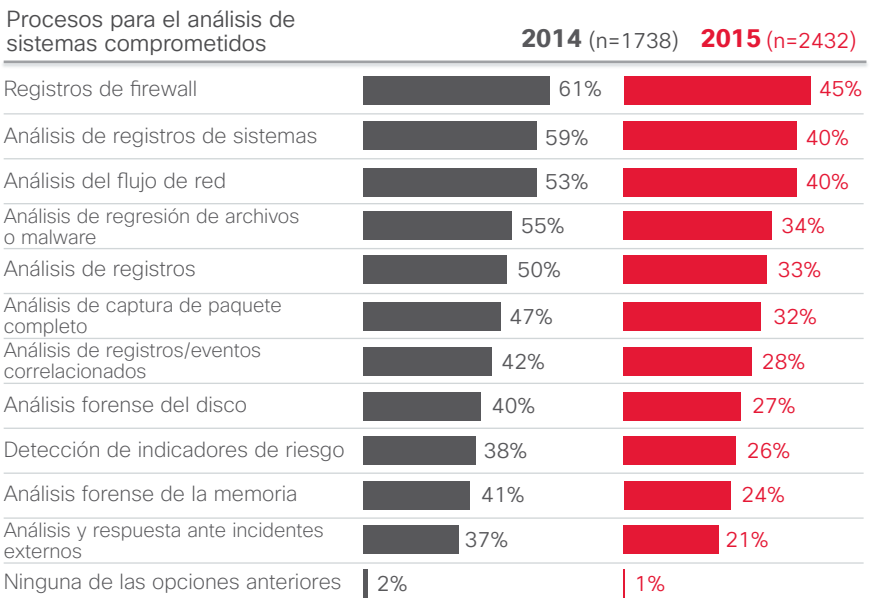
Figura 86. Las empresas demuestran una confianza variada en la capacidad de contener riesgos (continuación)



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 87. Los registros de firewall y los análisis de registros del sistema siguen siendo los procesos utilizados con más frecuencia para analizar sistemas comprometidos

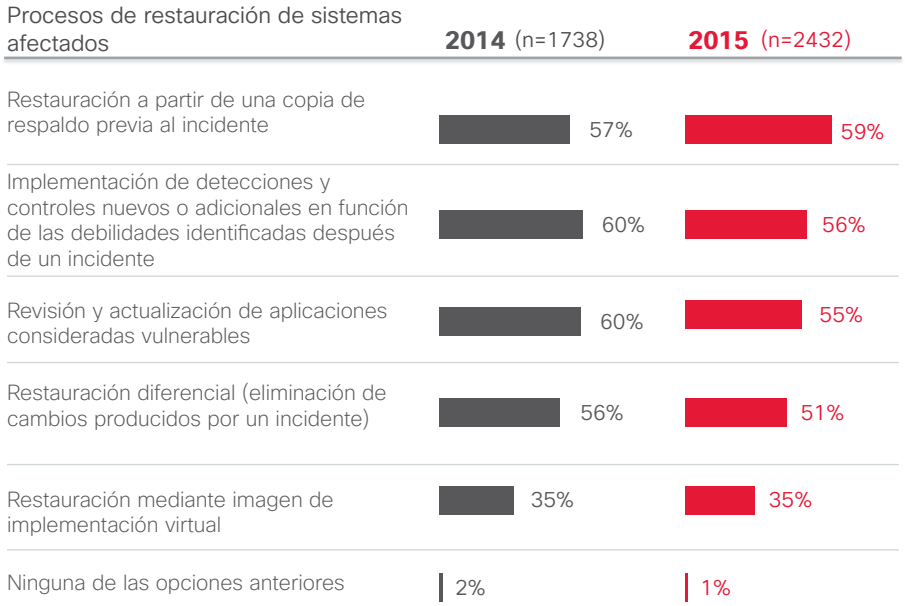
Las grandes empresas y las corporaciones informan un mayor uso de procesos para el análisis de sistemas comprometidos que las empresas medianas.



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 88. La restauración a partir de una copia de respaldo anterior a un incidente es el proceso más común utilizado para restaurar sistemas afectados en el 2015

Los encuestados de China expresan que corrigen y actualizan aplicaciones consideradas vulnerables con mayor frecuencia que los encuestados de otros países encuestados.

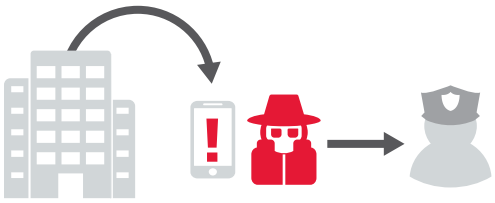


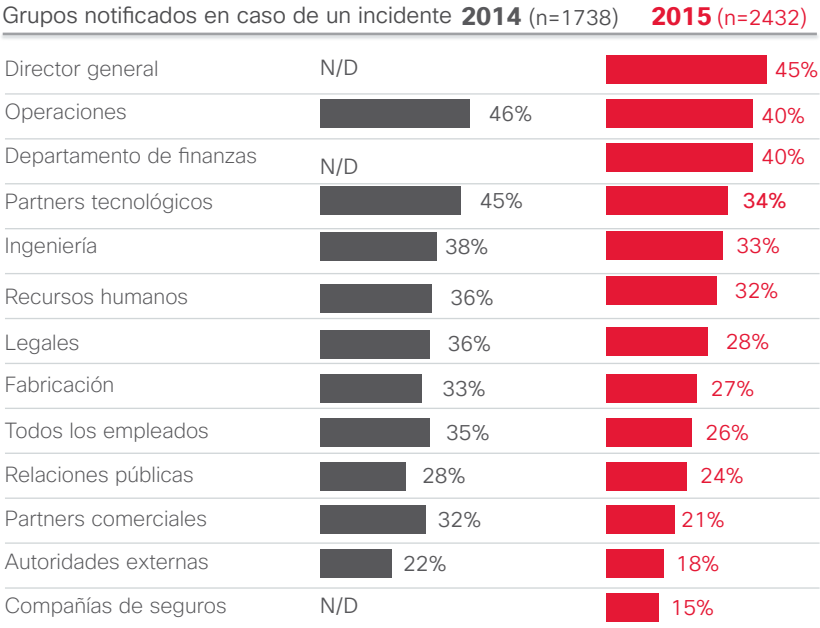
Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 89. El director ejecutivo o el presidente es quien tiene la mayor probabilidad de recibir una notificación de incidentes de seguridad, seguido por el departamento de operaciones y el departamento de finanzas

Una cantidad considerablemente mayor de los encuestados de corporaciones menciona que notifica a las autoridades externas en caso de incidentes en comparación con las empresas medianas y grandes.

Corporaciones



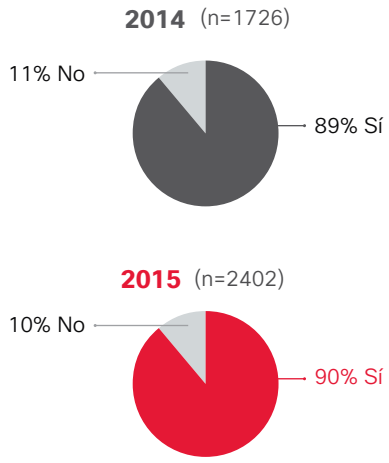


Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

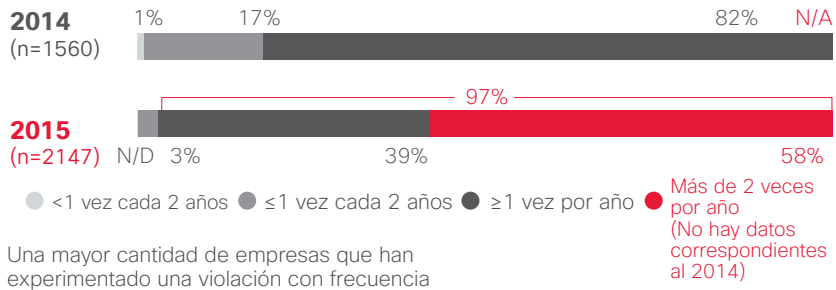
Capacitación

Figura 90. Casi todas las empresas (97%) imparten capacitación en seguridad al menos una vez al año

¿Se proporcionan programas de capacitación o concientización sobre la seguridad al personal de seguridad periódicamente? (Encuestados dedicados a la seguridad)



¿Con qué frecuencia se proporciona capacitación sobre la seguridad? (Encuestados cuyos equipos de seguridad reciben capacitación)



Una mayor cantidad de empresas que han experimentado una violación con frecuencia imparte programas de capacitación o concientización sobre la seguridad (96%) en comparación con las empresas que no han experimentado una violación (83%).

Tiene **96%** y No tiene **83%**

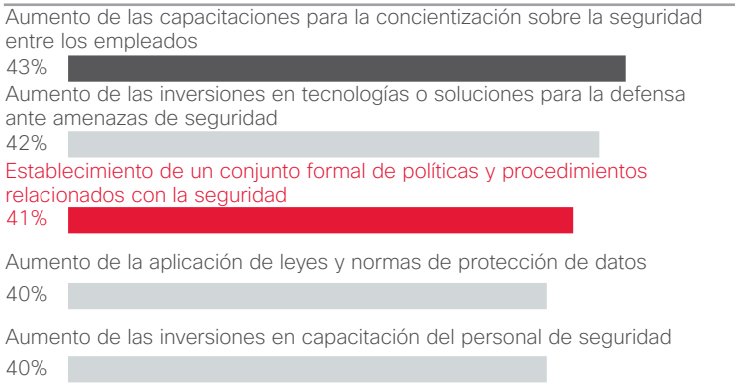
Una mayor cantidad de corporaciones indica impartir periódicamente programas de capacitación o concientización sobre la seguridad (93%) en comparación con las empresas medianas (88%) y grandes (89%).

Corporaciones **93%** Empresas medianas **88%** Empresas grandes **89%**

Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 91. La frecuencia de las capacitaciones de concientización sobre la seguridad y la incidencia de las políticas de seguridad formales se encuentran en aumento desde el 2014 (evidencia de acción)

(Cinco respuestas principales) Encuestados afectados por una violación a la seguridad (**2015** n=1109)



Aumento de las capacitaciones para la concientización sobre la seguridad entre los empleados

En el 2015, el 43% de los encuestados indicó haber aumentado las capacitaciones sobre la seguridad después de una violación pública.

43%

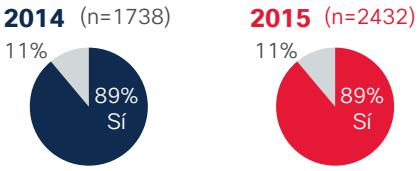
En el 2015, el 41% de los encuestados indicó haber establecido un conjunto formal de políticas y procedimientos relacionados con la seguridad.

41%

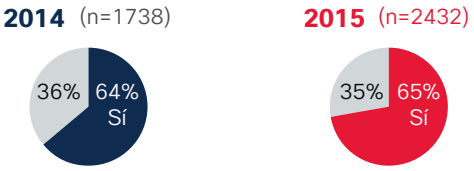
Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Figura 92. Tal como sucedió en 2014, aproximadamente 9 de cada 10 encuestados indican que el personal de seguridad asiste a conferencias o a capacitaciones orientadas a la seguridad

¿Los miembros del personal de seguridad asisten a conferencias o capacitaciones externas para mejorar y mantener sus habilidades?
(Encuestados dedicados a la seguridad)



¿Los empleados desempeñan funciones en comités o juntas de seguridad?
(Encuestados dedicados a la seguridad)



Fuente: Estudio comparativo sobre capacidades de seguridad 2015 de Cisco

Estudio del riesgo de seguridad y confiabilidad

Figura 93. Antecedentes y metodología

TI y grandes empresas acerca de los riesgos de seguridad y los desafíos relacionados que enfrenta la organización, además de la función que desempeña la confiabilidad del proveedor de TI en la compra de soluciones de TI.

Los beneficios específicos incluyen:

- Medir el nivel de riesgo de amenazas y vulnerabilidades externas e internas
- Comprender las estrategias, las políticas y las soluciones que se implementan para mitigar los riesgos de seguridad
- Identificar el proceso de compra de soluciones de TI y la función que desempeña la confiabilidad del proveedor de TI en el proceso
- Medir el interés en recibir comunicaciones sobre cómo validar la confiabilidad del proveedor de TI
- Determinar si hay diferencias en las perspectivas que se tienen de los riesgos de seguridad o en los enfoques que se adoptan para mitigar los riesgos en todos los sectores y públicos

Metodología: Enfoque cuantitativo y enfoque cualitativo

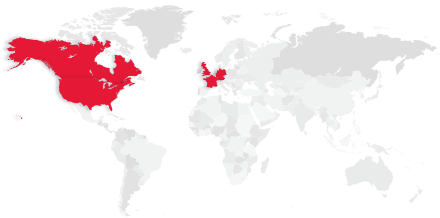
Se utilizaron dos metodologías para proporcionar información sobre cada uno de estos objetivos de investigación:

(Todos los encuestados involucrados en la toma de decisiones de compra de TI)

Encuesta cuantitativa realizada en Internet entre **1050 responsables de la toma de decisiones empresariales** (402 de EE. UU, 282 del Reino Unido, 197 de Alemania y 169 de Francia)

Entrevistas cualitativas exhaustivas entre **20 proveedores de servicios** (7 de EE. UU, 3 de Canadá, 3 del Reino Unido, 4 de Alemania y 3 de Francia)

La investigación se realizó en EE. UU, Reino Unido, Francia, Alemania, y Canadá (entrevistas exhaustivas solamente)



La recopilación de datos se llevó a cabo de agosto a septiembre de 2015.

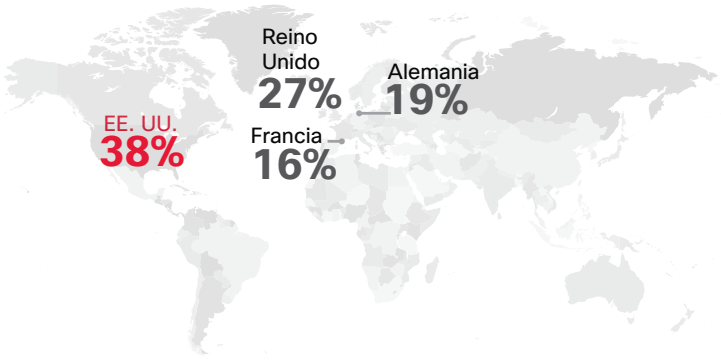
20 minutos Encuesta en línea

45 minutos Entrevistas exhaustivas

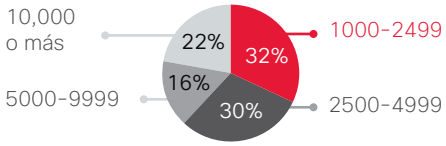
Fuente: Estudio del riesgo de seguridad y confiabilidad, Cisco

Figura 94. Perfil de los encuestados de grandes empresas: Cuantitativo

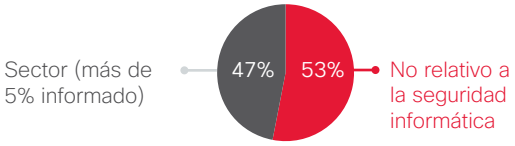
País



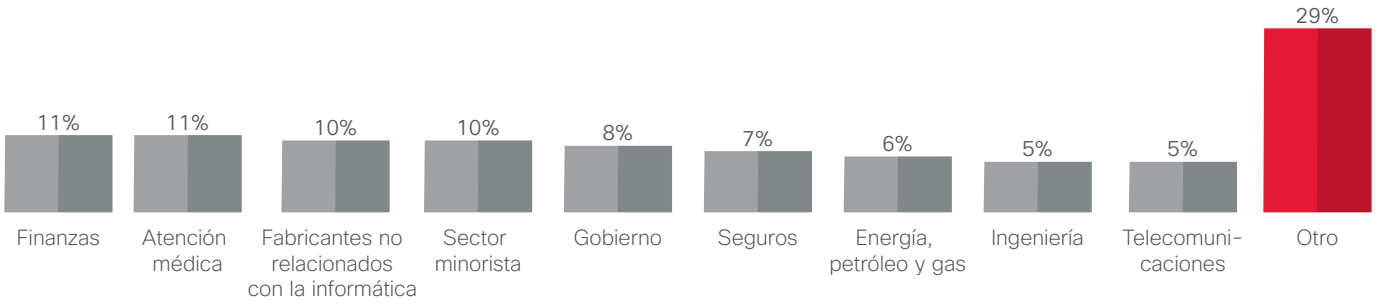
Tamaño de la empresa



Clasificación de seguridad informática



Sector (más de 5% informado)



Cargo

Nivel corporativo (CIO, CSO, CTO, etc.)	25%
Vicepresidente	9%
Director	30%
Ingeniero/arquitecto sénior	6%
Ingeniero	3%
Administrador	26%
Legales	2%

Participación en la compra

Establecer la visión/estrategia	69%
Garantizar el cumplimiento	71%
Aprobar compras importantes	69%
Investigar/evaluar soluciones	77%
Realizar aportes o tomar decisiones finales de la marca	80%
Implementar/administrar soluciones	77%
Autorizar la financiación/aprobar el presupuesto	53%

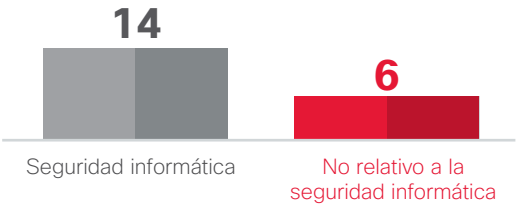
Fuente: Estudio del riesgo de seguridad y confiabilidad, Cisco

Figura 95. Perfil de los encuestados de proveedores de servicios: Cualitativo

País

Tamaño de la empresa

Clasificación de seguridad informática



Tipo de proveedor de servicios

Servicios de aplicaciones	11%
Servicios técnicos	11%
Telecomunicaciones móviles	6%
Servicios multimedia	4%
Telecomunicaciones por cable	3%

Cargo

CIO/CTO/CSO	7%
Vicepresidente de TI	1%
Director de TI	8%
Gerente ejecutivo	1%
Ingeniero/arquitecto sénior	2%
Administrador	1%

Participación en la compra

Establecer la visión/estrategia	80%
Garantizar el cumplimiento	100%
Aprobar compras importantes	70%
Investigar/evaluar soluciones	95%
Tomar decisiones finales de la marca	85%
Implementar/administrar soluciones	75%
Autorizar/aprobar la financiación	60%

Fuente: Estudio del riesgo de seguridad y confiabilidad, Cisco

Sede central en América
Cisco Systems, Inc.
San José. CA

Sede Central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco: **www.cisco.com/go/offices.**

Publicado en enero de 2016