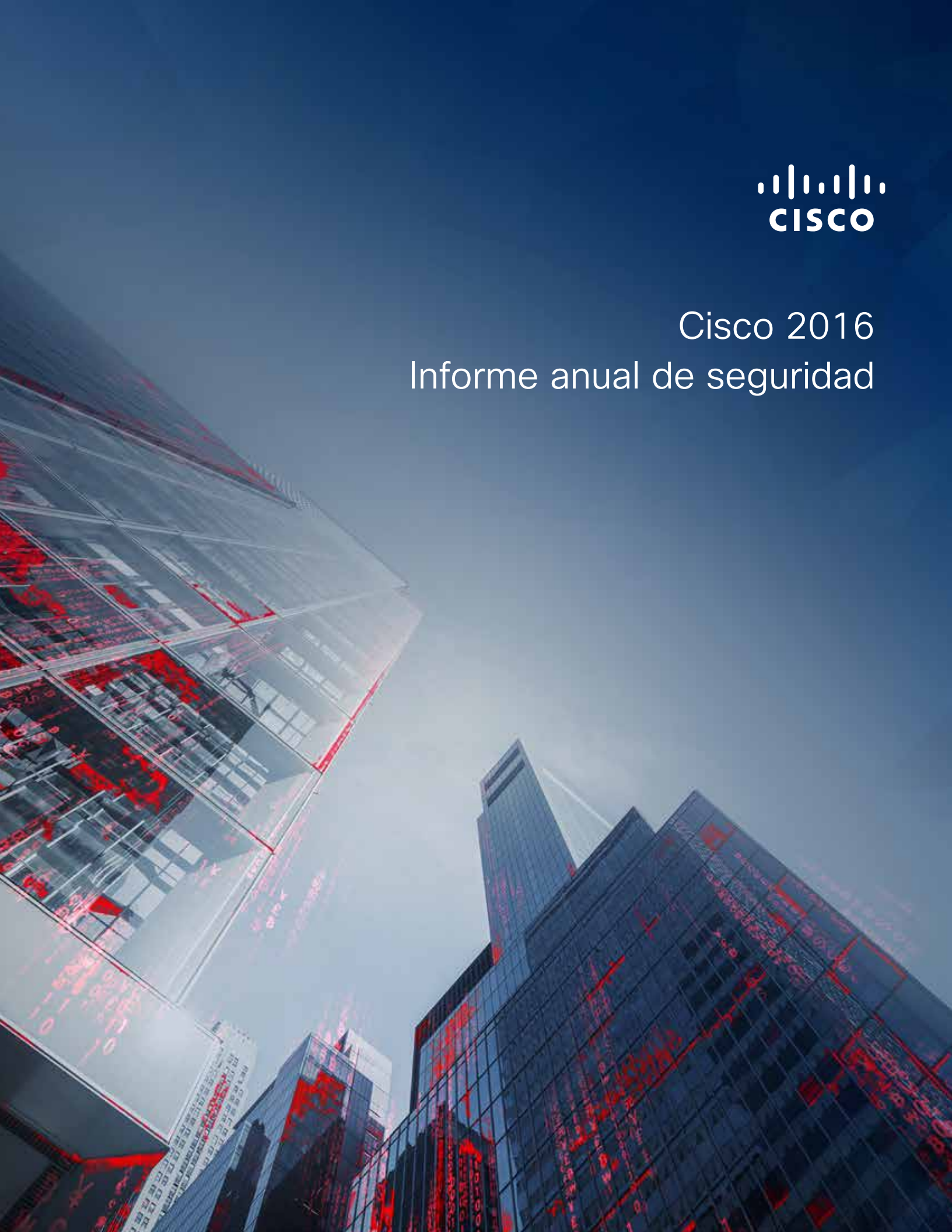


Cisco 2016
Informe anual de seguridad

Resumen ejecutivo

Los profesionales de la seguridad deben replantearse sus estrategias de defensa.

Los atacantes y los responsables de la seguridad están desarrollando tecnologías y tácticas cada vez más sofisticadas. Por su parte, los atacantes están creando infraestructuras back-end sólidas para el lanzamiento y soporte de sus campañas. Los ciberdelincuentes están perfeccionando sus técnicas para obtener dinero de sus víctimas y para evitar ser detectados mientras continúan robando datos y propiedad intelectual.

El informe anual de seguridad de Cisco 2016, que incluye estudios, datos y perspectivas del grupo de investigaciones de seguridad de Cisco, subraya los retos a los que se enfrentan los defensores a la hora de detectar y bloquear a los atacantes, que emplean una amplia gama de herramientas completas y en constante desarrollo. El informe también incluye la investigación de expertos externos, como Level 3 Threat Research Labs, con el fin de aportar nuevos puntos de vista sobre las actuales tendencias en el ámbito de las amenazas.

Observamos de cerca los datos recopilados por los investigadores de Cisco con el fin de mostrar los cambios a lo largo del tiempo, proporcionar información sobre el significado de dichos datos y explicar cómo los profesionales de la seguridad deberían responder ante las amenazas.

En este informe, presentamos y tratamos los siguientes aspectos:

INTELIGENCIA DE AMENAZAS

En esta sección se examinan algunas de las tendencias más convincentes de ciberseguridad identificadas por nuestros investigadores, así como actualizaciones sobre vectores y métodos de ataques web, así como las vulnerabilidades. También incluye un análisis más amplio de las amenazas emergentes, como el ransomware. Para elaborar su análisis de tendencias en 2015, el grupo de investigaciones de seguridad de Cisco utilizó un conjunto de datos de telemetría globales.

PERSPECTIVAS DEL SECTOR

En esta sección se analizan las tendencias de seguridad que afectan a las empresas, como el creciente uso del cifrado y los posibles riesgos que representa para la seguridad. Analizamos los puntos débiles de los métodos de protección de la red de pequeñas y medianas empresas (PYMES). Por otro lado, ofrecemos información sobre empresas que utilizan software desactualizado y sin soporte para respaldar sus infraestructuras de TI.

ESTUDIO COMPARATIVO SOBRE CAPACIDADES DE SEGURIDAD

Esta sección incluye los resultados del segundo estudio comparativo sobre capacidades de seguridad de Cisco, que se centra en las percepciones de los profesionales de seguridad sobre el estado de la seguridad en sus organizaciones. Al comparar los resultados de la encuesta de 2015 con los de 2014, Cisco identificó que los directores de seguridad (CSO) y los responsables de operaciones de seguridad (SecOps) no se muestran confiados con la actualización de sus infraestructuras de seguridad ni con su capacidad para evitar los ataques. Sin embargo, la encuesta también demuestra que las empresas están reforzando sus iniciativas de formación y otros procesos de seguridad a fin de fortalecer sus redes. Los resultados del estudio son exclusivos del informe anual de seguridad de Cisco 2016.

UNA MIRADA AL FUTURO

Esta sección ofrece una perspectiva del panorama geopolítico que afecta a la seguridad. Analizamos los resultados de dos estudios de Cisco, uno de ellos sobre las preocupaciones sobre ciberseguridad de los ejecutivos y el otro sobre las percepciones de los responsables de TI sobre los riesgos de seguridad y la confianza. También ofrecemos una actualización sobre nuestros avances en la reducción del tiempo de detección (TTD), haciendo hincapié en la importancia de adoptar una arquitectura de defensa frente a amenazas integrada como método para combatirlas.

Índice

Principales avances y descubrimientos

Principales avances y descubrimientos

Los ciberdelincuentes han perfeccionado sus infraestructuras de back-end con el fin de aumentar la eficacia y los resultados económicos de sus ataques.

- Cisco, con la ayuda de Level 3 Threat Research Labs y la colaboración del proveedor de alojamiento Limestone Networks, pudo identificar y aislar la mayor operación del kit de aprovechamiento de vulnerabilidades Angler en Estados Unidos, dirigido a 90 000 víctimas diarias y que estaba generando decenas de millones de dólares anuales para los autores de la campaña.
- SSHPsychos (Group 93), una de las botnets de denegación de servicio distribuida (DDoS) más grandes identificadas hasta la fecha por los investigadores de Cisco, fue debilitada considerablemente gracias a los esfuerzos combinados de Cisco y Level 3 Threat Research Labs. Al igual que el caso práctico de Angler mencionado anteriormente, este éxito señala la importancia de la colaboración dentro del sector a la hora de combatir a los atacantes.
- Las extensiones maliciosas de navegador pueden ser una fuente importante de filtración de datos de las empresas y son un problema muy extendido. Se calcula que más del 85% de las organizaciones analizadas sufre el problema de las extensiones maliciosas de navegador.
- Botnets muy conocidas, como Bedep, Gamarue y Miuref representan la mayor parte de la actividad de control y mando de botnets que afectaba a un grupo de organizaciones que analizamos en julio de 2015.
- El análisis de Cisco de malware validado como "problema conocido" concluyó que la mayoría del malware (91,3%) utiliza DNS (sistema de nombres de dominio) para llevar a cabo sus campañas. Mediante la investigación retrospectiva de consultas de DNS, Cisco descubrió clientes DNS (resolvers) maliciosos en uso en las redes de sus clientes. Los clientes no eran conscientes de que sus empleados utilizaban dichos "resolvers" como parte de su infraestructura de DNS.
- Las vulnerabilidades de Adobe Flash siguen siendo muy conocidas para 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.
- Tras observar las tendencias en 2015, nuestros investigadores sugieren que el tráfico cifrado HTTPS ha alcanzado un punto crítico: pronto se convertirá en la forma dominante de tráfico de Internet. Aunque el cifrado puede ayudar a proteger a los clientes, también puede minar la eficacia de las soluciones de seguridad, dificultando así el seguimiento de las amenazas. Lo que es aún peor, cierto malware puede iniciar comunicaciones cifradas a través de un variado conjunto de puertos.
- Los atacantes se sirven de Webs expuestas creadas por la popular plataforma de desarrollo web WordPress para sus actividades criminales. Allí pueden reunir recursos de servidor y evitar ser detectados.

- Las infraestructuras están cada vez más obsoletas, lo que aumenta la vulnerabilidad y el riesgo de las organizaciones. Analizamos 115 000 dispositivos Cisco® en Internet y descubrimos que el 92% de ellos ejecutaba software con vulnerabilidades conocidas. Además, el 31% de los dispositivos Cisco en uso que se incluyeron en el análisis ya no se comercializa y el 8% ya ha alcanzado el fin de su ciclo de vida útil.
- En 2015, los ejecutivos de seguridad mostraron una confianza menor en sus herramientas y procesos de seguridad que en el año 2014, según el estudio comparativo sobre capacidades de seguridad de Cisco de 2015. Por ejemplo, en el año 2015, el 59% de las organizaciones manifestó que su infraestructura de seguridad estaba "muy actualizada". En 2014, el porcentaje fue del 64%. Sin embargo, sus crecientes preocupaciones sobre la seguridad les están animando a mejorar sus defensas.
- El estudio comparativo muestra que las pequeñas y medianas empresas (PYMES) utilizan menos defensas que las organizaciones de gran tamaño. Por ejemplo, el 48% de las PYMES utilizó seguridad web en 2015, frente al 59% que lo hizo en 2014. Por otro lado, el 29% afirmó en 2015 utilizar herramientas de parches y configuración, mientras que en 2014 el porcentaje fue del 39%. Estos puntos débiles pueden poner en riesgo a los clientes empresariales de las PYMES, pues los atacantes pueden atacar más fácilmente las redes de las PYMES.
- Desde mayo de 2015, Cisco ha reducido el tiempo medio de detección (TTD) de las amenazas conocidas en nuestras redes hasta aproximadamente 17 horas, esto es, menos de un día. Este dato mejora considerablemente la estimación actual del sector que es de 100 a 200 días.

El gran premio: para los ciberdelincuentes modernos, lo principal es la recompensa económica

El gran premio: para los ciberdelincuentes modernos, lo principal es la recompensa económica

En el pasado, muchos ciberdelincuentes acechaban a la sombra de Internet. Intentaban evitar la detección haciendo solo breves incursiones en las redes empresariales para poner en marcha sus ataques. Actualmente, algunos envalentonados ciberdelincuentes acceden a recursos legítimos online. Disminuyen la capacidad del servidor, roban datos y exigen rescates a las víctimas online de cuya información se han apoderado.

Estas campañas suponen una escalada en la guerra entre defensores y atacantes. Si los atacantes encuentran más lugares online desde los que operar, su impacto puede crecer de forma exponencial.

En este informe, los investigadores de seguridad de Cisco destacan las tácticas que los responsables de las amenazas utilizan para crear una infraestructura sólida que fortalezca sus campañas y haga que sean más eficaces. Los atacantes siguen adoptando métodos más eficaces para multiplicar sus beneficios y muchos de ellos están prestando especial atención al aprovechamiento de los recursos del servidor.

La proliferación de ransomware (consulte la **página 10**) es un ejemplo típico. El ransomware proporciona a los delincuentes un método sencillo para obtener más dinero directamente de los usuarios. Cuando los atacantes ponen en marcha campañas que ponen en peligro a decenas de miles de usuarios al día con muy pocas interrupciones, o incluso ninguna, la "recompensa" a sus esfuerzos puede ser apabullante. Además de desarrollar mejores métodos de rentabilización de sus campañas, los atacantes están usurpando recursos legítimos desde los que iniciar sus ataques.

Los creadores de algunas variantes de ransomware, así como los desarrolladores de otros ataques ahora están redirigiendo el tráfico a sitios web pirateados de WordPress con el fin de evitar la detección y utilizar espacio del servidor (consulte la **página 33**). Los atacantes responsables de SSHPsychos, una de las mayores botnets nunca vistas por los investigadores de Cisco, operaban en redes estándar sin apenas interferencias hasta que el esfuerzo combinado de Cisco y Level 3 Threat Research Labs logró persuadir a los proveedores de servicios para que bloqueasen el tráfico del creador de la botnet.

Inteligencia de amenazas

Inteligencia de amenazas

Cisco ha reunido y analizado un conjunto global de datos de telemetría para este informe. Nuestras investigaciones y análisis continuos de las amenazas descubiertas, como el tráfico de malware, pueden ofrecer una serie de indicadores sobre un posible comportamiento delictivo futuro, así como ayuda a la hora de detectar las amenazas.

Historias destacadas

La colaboración del sector ayuda a Cisco a aislar y detener el avance de una campaña de ransomware y kit de aprovechamiento de vulnerabilidades altamente rentable

El kit de aprovechamiento de vulnerabilidades Angler es uno de los kits de aprovechamiento de vulnerabilidades más grandes y eficaces del mercado. Se ha vinculado a varias campañas notorias de ransomware y publicidad maliciosa. Además, ha sido un impulsor importante de la proliferación general de la actividad de ransomware que nuestros investigadores de amenazas han estado supervisando estrechamente en los últimos años. Los ciberdelincuentes utilizan ransomware para cifrar archivos de los usuarios a quienes proporcionan las claves de descifrado solo si pagan un "rescate", que suele oscilar entre los 300 y los 500 dólares.

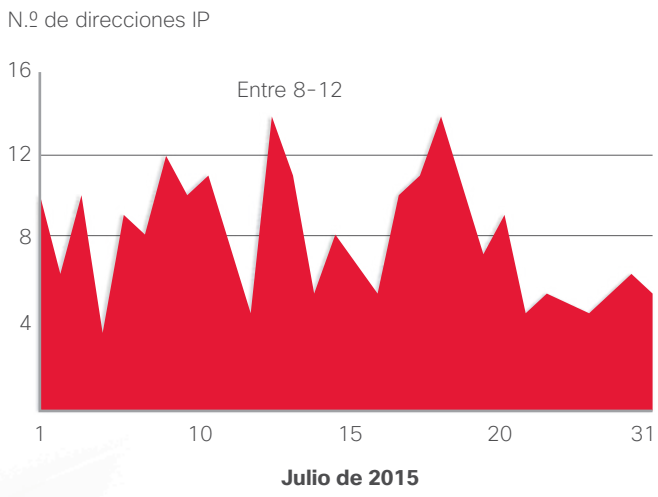
Tal y como se muestra en el informe de seguridad semestral de Cisco 2015, las criptodivisas como Bitcoin y las redes anónimas como Tor facilitan el acceso de los ciberdelincuentes a los mercados de malware y les permiten empezar a generar beneficios rápidamente. El aumento de la popularidad del ransomware puede vincularse a dos ventajas principales: resulta una operación de bajo mantenimiento para los atacantes y proporciona una rápida rentabilización, pues los usuarios pagan a los atacantes directamente en criptodivisas.

Gracias al análisis de las tendencias de Angler y ransomware relacionado, Cisco determinó que algunos operadores de kits de aprovechamiento de vulnerabilidades estaban utilizando un porcentaje desorbitado de servidores proxy mundiales para Angler que se encontraban en servidores operados por Limestone Networks. Este uso de servidores es un ejemplo típico de otra tendencia que los investigadores han observado en la economía sumergida más reciente: los atacantes combinan recursos legítimos y maliciosos para llevar a cabo sus campañas.

En este caso, la infraestructura de IP que apoyaba el Angler no era grande. El número diario de sistemas activos oscilaba normalmente entre 8 y 12. La mayoría estaba activo solo durante un día. La figura 1 muestra el número de direcciones IP únicas que Cisco observó en julio de 2015.

Cisco descubrió que los operadores de Angler se estaban lanzando básicamente a través de direcciones IP de un modo lineal para ocultar la actividad de las amenazas y evitar interrupciones en su flujo de beneficios.

Figura 1. Número de direcciones IP de Angler por fecha, julio de 2015



Fuente: grupo de investigaciones de seguridad de Cisco

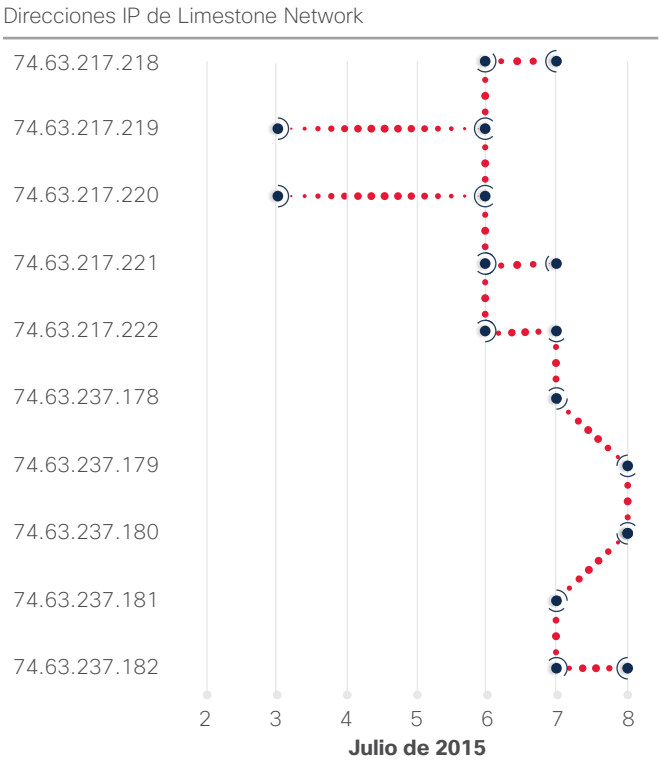
Como muestra la figura 2, el Angler comienza con una dirección IP (en este caso, 74.63.217.218). A medida que el sistema pone en peligro a los usuarios y genera el "ruido" que los responsables de seguridad comienzan a detectar, los atacantes cambian a una dirección IP adyacente (74.63.217.219). Esta actividad continúa a través de bloques casi contiguos de espacio IP de un solo proveedor de alojamiento.

Cisco examinó la información de IP para identificar los números de sistemas autónomos (ASN) y los proveedores asociados a las direcciones IP. Determinamos que la mayor parte del tráfico relacionado con Angler procedía de servidores operados por dos proveedores de alojamiento legítimos: Limestone Networks y Hetzner (figura 3). Ambos representaban casi el 75% del volumen de tráfico total del mes de julio.

Cisco contactó en primer lugar con Limestone Networks, que parecía alojar la porción de mayor tamaño de Angler a nivel global. Limestone aceptó la oportunidad de colaboración. La empresa había tenido un número excesivo de reembolsos de tarjetas de crédito cada mes debido a que los atacantes estaban utilizando nombres y tarjetas de crédito fraudulentos para adquirir lotes aleatorios de sus servidores por valor de miles de dólares.

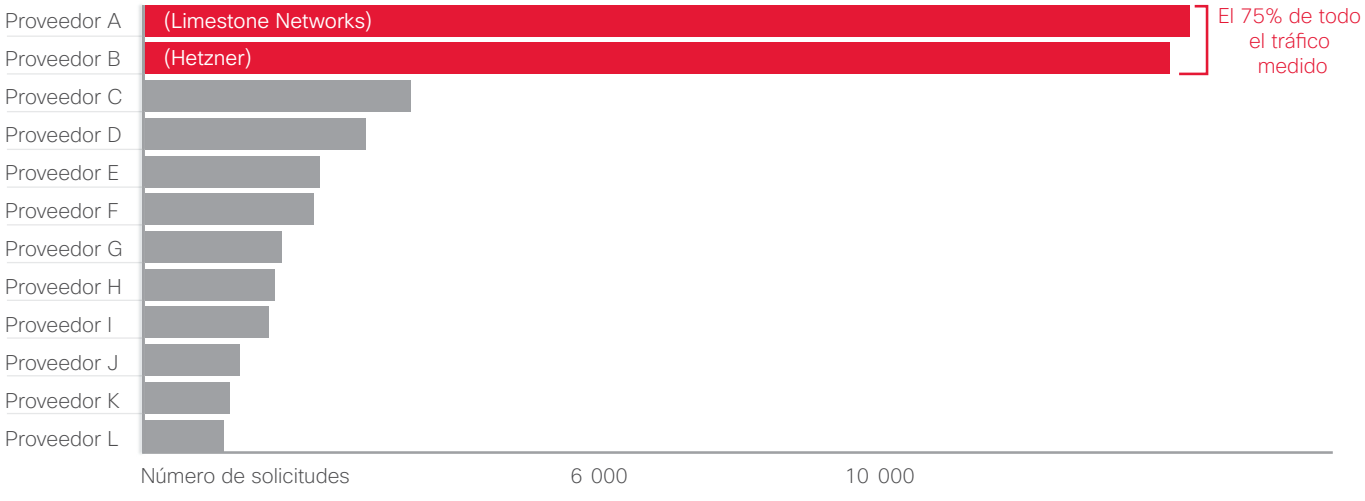
COMPARTIR

Figura 2. Baja infraestructura de IP de soporte de Angler



Fuente: grupo de investigaciones de seguridad de Cisco

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



Fuente: grupo de investigaciones de seguridad de Cisco

El enfoque utilizado por sus enemigos para adquirir los servidores dificultó la vinculación de la actividad fraudulenta con un único atacante. Por ejemplo, un ciberdelincuente podría adquirir tres o cuatro servidores en un día, y después utilizar un nombre o tarjeta de crédito diferentes para adquirir tres o cuatro más al día siguiente. De este modo, básicamente podría pasar de una dirección IP a la siguiente una vez que los defensores identificaran y desconectaran los servidores en peligro.

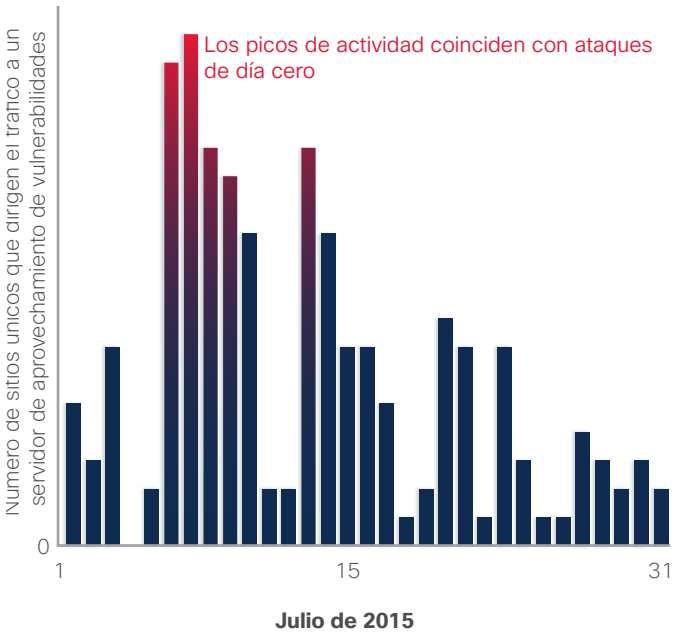
Para investigar esta actividad, Cisco contó con la ayuda de Level 3 Threat Research Labs, así como de OpenDNS, una empresa de Cisco Level 3 Threat Research Labs pudo proporcionar una perspectiva global más amplia de la amenaza, lo que permitió a Cisco profundizar en el alcance de la amenaza y saber en qué momento de su avance se encontraba. OpenDNS, por su parte, proporcionó una visión única de la actividad de dominio asociada con la amenaza, lo que sirvió a Cisco para comprender de forma más completa las técnicas que los atacantes están incorporando, como el "domain shadowing".

Los investigadores de amenazas de Cisco se centraron entonces en el modo en el que los usuarios se topaban con Angler y recibían posteriormente contenido malicioso. Los investigadores observaron que sitios web populares redirigían a los usuarios al kit de aprovechamiento de vulnerabilidades Angler a través de publicidad maliciosa. Los anuncios falsos se incluían en cientos de sitios populares de noticias, de inmobiliarias o culturales. Los responsables de seguridad se refieren normalmente a este tipo de sitios como "correcto conocido".

Además, los investigadores de amenazas de Cisco encontraron innumerables ejemplos de pequeños sitios web aparentemente aleatorios que ejecutaban el mismo tipo de redirección, incluso en el obituario de una persona en un pequeño periódico rural de Estados Unidos. Es muy probable que esta última estrategia estuviera pensada para personas de mayor edad. Este segmento de población es más propenso a utilizar los navegadores web predeterminados, como Microsoft Internet Explorer, y es menos probable que sea consciente de la necesidad de aplicar parches de forma periódica para evitar las vulnerabilidades de Adobe Flash.

Otro aspecto notable de esta operación de Angler es el volumen de referentes únicos y la baja frecuencia con la que se utilizaron (figura 4). Identificamos más de 15 000 sitios específicos que dirigían a las personas al kit de aprovechamiento de vulnerabilidades Angler, de los cuales el 98,8% se había utilizado en menos de 10 ocasiones. La mayor parte de los referentes, por tanto, solo había estado activos durante un corto periodo de tiempo y se habían retirado una vez alcanzado un grupo de usuarios. En nuestro análisis de julio de 2015, observamos que los picos de actividad coinciden con varios de los ataques de día cero de Hacking Team (CVE-2015-5119, CVE-2015-5122).[1]

Figura 4.
Referentes únicos por día, julio de 2015

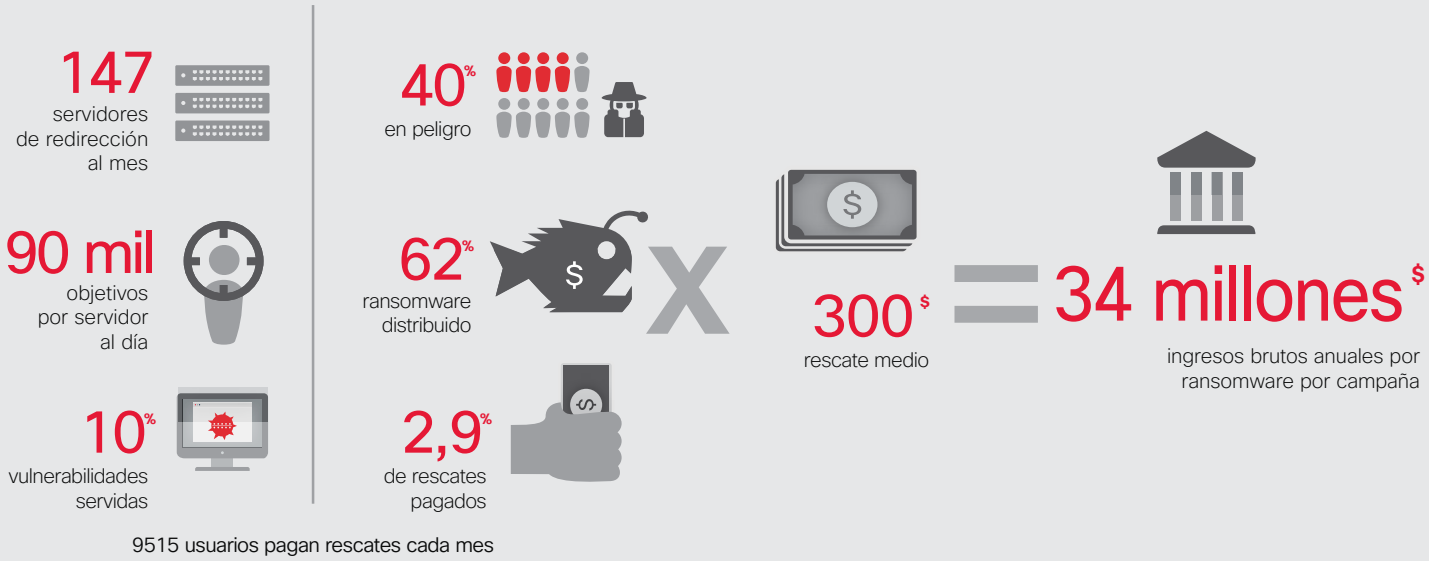


Fuente: grupo de investigaciones de seguridad de Cisco

Cisco determinó que cerca del 60% del contenido de Angler entregado a través de esta operación en concreto incluía algún tipo de variante de ransomware, en su mayoría Cryptowall 3.0. Otros tipos de contenido incluyen Bedep, un descargador de malware que se utiliza habitualmente para instalar malware de campañas de fraude por clic. (Consulte la sección "Infecciones de navegador: amplio alcance y una importante causa de filtración de datos" en la **página 16**.) Ambos tipos de malware están diseñados para que los atacantes obtengan mucho dinero de los usuarios expuestos muy rápidamente y con muy poco o nada de esfuerzo.

[1] " Adobe Patches Hacking Team's Flash Player Zero-Day", Eduard Kovacs, *SecurityWeek*, 8 de julio de 2015: **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day**.

Ingresos de Angler



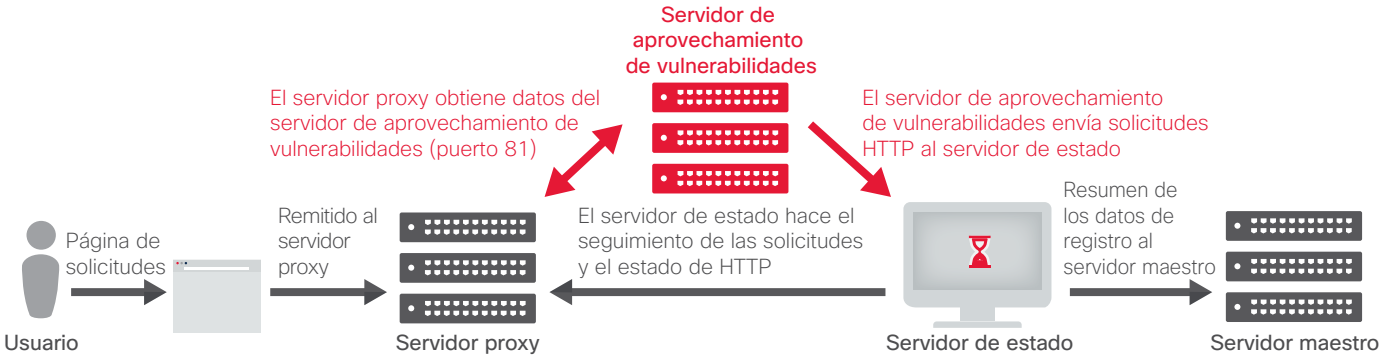
Source: Cisco Security Research

Según el estudio de Cisco, el principal responsable de cerca de la mitad de la actividad de Angler de esta campaña en particular dirigía su ataque a hasta 90 000 víctimas al día. Según nuestras estimaciones, la campaña aportaba a los atacantes más de 30 millones de dólares anuales.

COMPARTIR

Probablemente, el índice de éxito de la campaña de Hetzner fue similar. Esto significa que el responsable de las amenazas de la operación que involucraba servidores de Limestone Networks y Hetzner era responsable de la mitad de la actividad total de Angler en el momento del análisis de Cisco. Los investigadores de Cisco estiman que esta operación podría haber generado unos ingresos brutos de 60 millones de dólares al año.

Figura 5. Infraestructura back-end de Angler



Fuente: grupo de investigaciones de seguridad de Cisco

Cisco también descubrió que los servidores a los que los usuarios estaban conectados no alojaban realmente la actividad maliciosa de Angler. Únicamente servían como conducto. Los usuarios entraban en la cadena de redirección y enviaban una solicitud GET para una página de inicio que accedería al servidor proxy. El servidor proxy dirigía el tráfico a un servidor de aprovechamiento de vulnerabilidades en un país diferente, en un proveedor distinto. Durante nuestro estudio, observamos que un único servidor de aprovechamiento de vulnerabilidades estaba asociado con varios servidores proxy. (véase la figura 5).

Cisco identificó un servidor de estado que realizaba tareas como la supervisión del estado. Cada servidor proxy supervisado por el servidor de estado tenía un par de URL únicas. En caso de consulta de la ruta, el servidor de estado devolvía un mensaje de código de estado HTTP "204". Los atacantes podían identificar exclusivamente cada servidor de proxy y asegurarse no solo de que estaba en funcionamiento, sino de que los defensores no lo habían alterado. Con la otra URL, los atacantes podían recopilar los registros del servidor proxy y determinar el nivel de eficacia de la operación de su red.

La colaboración dentro del sector fue un factor decisivo para que Cisco pudiera investigar la actividad de Angler. En última instancia, ayudó a detener el redireccionamiento a los servidores proxy de Angler en un proveedor de servicios de EE. UU. y dio a conocer una operación muy sofisticada de cibercrimen que afectaba a miles de usuarios cada día.

COMPARTIR

Cisco trabajó estrechamente con Limestone Networks en la identificación de nuevos servidores tras su lanzamiento online y realizó un seguimiento de los mismos para garantizar su desmantelamiento. Transcurrido un tiempo, los atacantes se apartaron de Limestone Networks y se produjo un descenso global de la actividad de Angler.

Para obtener más información sobre cómo Cisco interrumpió un significativo flujo internacional de ingresos generados por Angler, lea la entrada del blog de seguridad de Cisco **"Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually from Ransomware Alone".**

Los esfuerzos coordinados en el sector ayudan a frenar una de las mayores botnets de DDoS de Internet

Las tecnologías integradas de defensa contra amenazas pueden a menudo frenar importantes ataques antes de que afecten a las redes empresariales. Sin embargo, en muchos casos, para acabar con un ataque potencialmente masivo se requieren no solo defensas tecnológicas, sino la coordinación entre proveedores de servicios, proveedores de soluciones de seguridad y grupos del sector.

Mientras que los ciberdelincuentes dan cada vez mayor importancia a la rentabilización de sus actividades, el sector tecnológico debe fomentar la colaboración para acabar con las campañas criminales. SSHPsychos (también denominado Group 93), una de las mayores botnets de DDoS identificadas hasta la fecha por los investigadores de seguridad de Cisco, se debilitó considerablemente gracias a los esfuerzos combinados de Cisco y Level 3 Threat Research Labs.

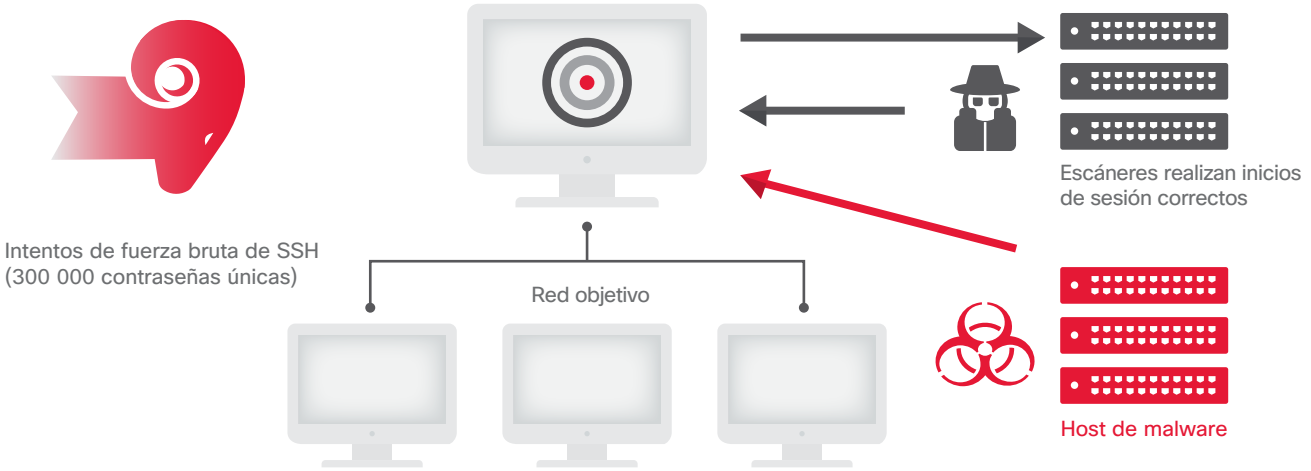
AMENAZAS EXCLUSIVAS

La red de SSHPsychos de DDoS es una amenaza única por varios motivos. Dado que incluye decenas de miles de máquinas distribuidas a través de Internet, tiene la capacidad de lanzar ataques de denegación de servicio distribuida (DDoS) que no se pueden abordar caso por caso. En este caso, la botnet se había creado mediante ataques de fuerza bruta que incluían tráfico de Secure Shell (SSH) (figura 6). El protocolo SSH se utiliza para permitir comunicaciones seguras y se emplea habitualmente para la administración remota de sistemas. En algunos momentos, SSHPsychos representó más del 35% de todo el tráfico SSH de Internet global (figura 7) según el análisis de Cisco y Level 3.

SSHPsychos está operativo en dos países: China y Estados Unidos. Los intentos de inicio de sesión por fuerza bruta, utilizando 300 000 contraseñas exclusivas, se originaron en un proveedor de alojamiento en China. Una vez que los atacantes pudieron iniciar sesión adivinando la contraseña raíz correcta, cesaron los ataques por fuerza bruta. Veinticuatro horas más tarde, los atacantes iniciaron sesión desde una dirección IP de EE. UU. e instalaron un rootkit DDos en la máquina afectada. Se trata claramente de una táctica para evitar levantar sospechas entre los administradores de redes. Los objetivos de la botnet eran diversos pero, en muchos casos, se dirigían a proveedores de servicios de Internet (ISP).

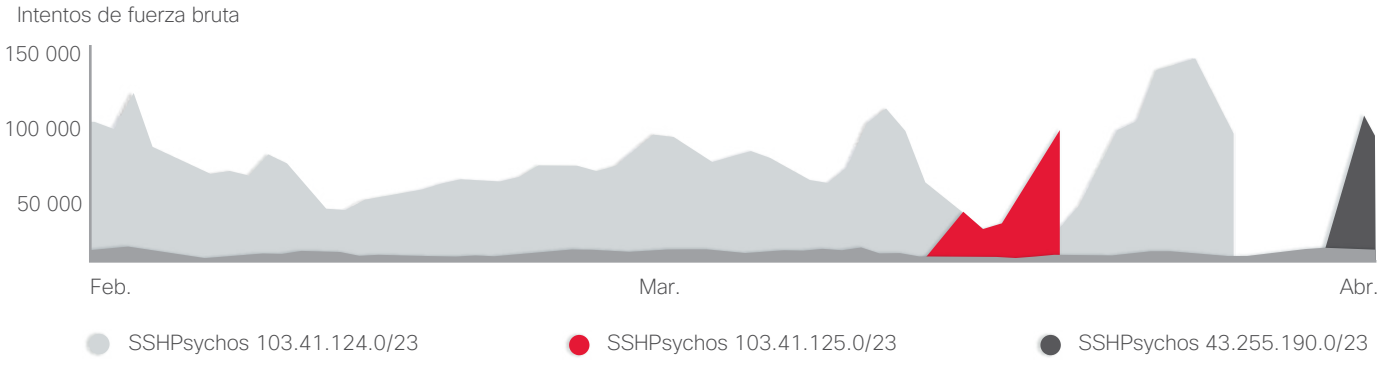
COMPARTIR

Figura 6. SSHPsychos utiliza ataques de fuerza bruta



Fuente: grupo de investigaciones de seguridad de Cisco

Figura 7. En su punto álgido, SSHPsychos representó el 35% del tráfico global de Internet



Fuente: grupo de investigaciones de seguridad de Cisco

COLABORACIÓN CON LOS EXPERTOS EN SEGURIDAD

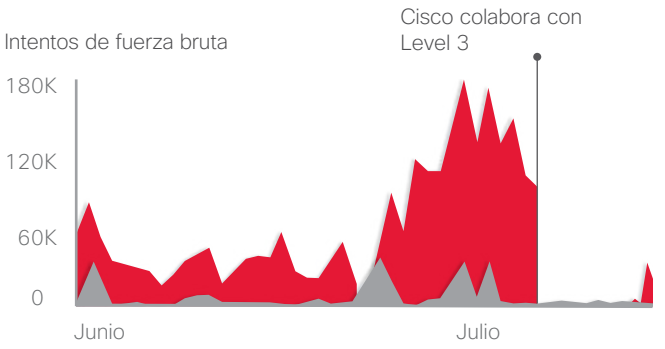
Dado el alcance de la red DDoS, nuestros investigadores creen que el daño habría sido difícil de contener. Fue fundamental trabajar en colaboración con una organización que pudiera retirar el grupo que empleaba la fuerza bruta de Internet de forma eficaz. Sin embargo, los proveedores de redes troncales se muestran reacios a la hora de filtrar el contenido de sus clientes.

Cisco solicitó la ayuda de Level 3 Threat Research Labs. Level 3 analizó el tráfico en el netblock, o rango de direcciones IP, donde se pensaba que se alojaba SSHPsychos (103.41.124.0/23). Confirmó que no existía tráfico legítimo originado en esa dirección ni dirigido a ella. Consiguió anular el redireccionamiento del tráfico de red dentro de sus propias redes. A continuación, se puso en contacto con proveedores de servicios de los dominios relevantes para pedirles que eliminaran el tráfico de red.

Los resultados de este esfuerzo se vieron de forma inmediata (figura 8). La red original prácticamente no presentó ninguna actividad nueva. Sin embargo, una nueva red en el netblock 43.255.190.0/23 presentó una gran cantidad de tráfico de ataques de fuerza bruta de SSH. Tuvo el mismo comportamiento que se ha asociado a SSHPsychos. Después de esta repentina reaparición de tráfico similar al de SSHPsychos, Cisco y Level 3 decidieron pasar a la acción frente a 103.41.124.0/23, así como al nuevo netblock 43.255.190.0/23.

La anulación de los netblocks utilizados por SSHPsychos no desactivó permanentemente la red de DDoS. Sin embargo, sin duda ralentizó la capacidad de sus creadores para ejecutar sus operaciones y evitó la expansión de SSHPsychos a nuevas máquinas, al menos temporalmente.

Figura 8. Descenso drástico del tráfico de SSHPsychos tras la intervención



Fuente: grupo de investigaciones de seguridad de Cisco

A medida que los ciberdelincuentes crean grandes redes de ataque, el sector de la seguridad debe explorar formas de colaboración cuando se enfrentan a una amenaza como SSHPsychos. Los proveedores de dominios de nivel superior, los ISP, los proveedores de alojamiento, los clientes de DNS y los proveedores de seguridad ya no pueden mantenerse al margen cuando los cibercriminales lanzan sus ataques en redes destinadas a transportar tráfico legítimo. En otras palabras, cuando los ciberdelincuentes lanzan tráfico malicioso más o menos a la vista, el sector debe eliminar las rutas maliciosas a estas redes legítimas.

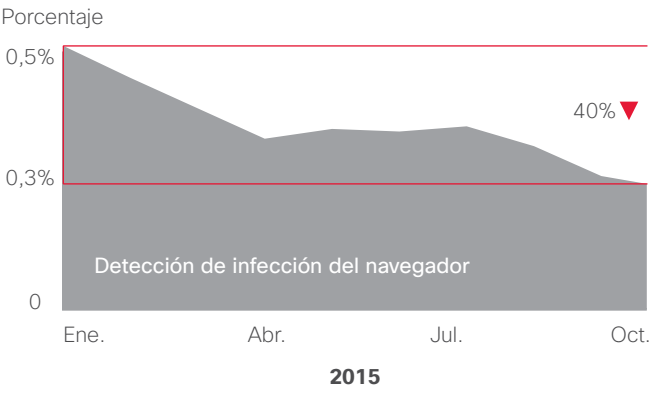
Para obtener más información sobre la respuesta de Cisco y Level 3 Threat Research Labs a la amenaza de SSHPsychos, lea la entrada del blog de seguridad de Cisco **"Threat Spotlight: SSHPsychos".**

Infecciones de navegador: amplio alcance y una importante causa de filtración de datos

Los equipos de seguridad a menudo ven en los complementos del navegador una amenaza de poca importancia. Sin embargo, deben dar mayor importancia a su supervisión con el fin de facilitar la rápida identificación y solución de este tipo de infecciones.

Motivo de la urgencia: nuestra investigación indica que las infecciones de navegador son mucho más frecuentes de lo que muchas organizaciones creen. Desde enero a octubre de 2015, examinamos 26 familias de complementos de navegador maliciosos (figura 9). Al observar el patrón de infecciones de navegador durante estos meses, vemos que se ha producido un descenso general del número de infecciones.

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



Fuente: grupo de investigaciones de seguridad de Cisco

Este patrón, no obstante, es engañoso. El creciente volumen de tráfico de HTTPS durante esos meses dificultó la identificación de los indicadores de compromiso asociados normalmente con las 26 familias que fueron objeto de supervisión, dado que la información de URL estaba cifrada y no era visible. (Para obtener más información sobre cifrado y los retos que supone para los responsables de la seguridad, consulte "Cifrado: una tendencia al alza y un reto para los defensores", en la **página 30**).

Las extensiones de navegador maliciosas pueden robar información y ser una fuente importante de filtración de datos. Cada vez que un usuario abre una nueva página web con un navegador expuesto, las extensiones de navegador maliciosas recopilan datos. Extraen mucho más que los detalles básicos de cada página web interna o externa que el usuario visita. Además, 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 multifunción se lanzan a través de paquetes de software o adware. Están diseñadas para obtener ganancias económicas mediante la explotación de los usuarios de diversas formas. En un navegador infectado, pueden llevar a los usuarios a hacer clic en publicidad maliciosa en forma de anuncios o elementos emergentes. También pueden distribuir malware persuadiendo a los usuarios para que hagan clic en un enlace expuesto o descarguen un archivo infectado a través de la publicidad maliciosa. Además, son capaces de interceptar las solicitudes de navegador e introducir páginas web maliciosas en las páginas de resultados de los motores de búsqueda.

Entre las 45 empresas de nuestra muestra, identificamos más del 85% de organizaciones afectadas cada mes por extensiones de navegador maliciosas, un resultado que pone de manifiesto la magnitud de este tipo de operaciones. Dado que los navegadores infectados a menudo se consideran una amenaza menor, pueden pasar inadvertidos durante días o incluso más tiempo. Esta circunstancia proporciona a los atacantes el tiempo y la oportunidad para seguir adelante con sus campañas (consulte "Tiempo de detección: la carrera por seguir acortando el ciclo", en la **página 60**).

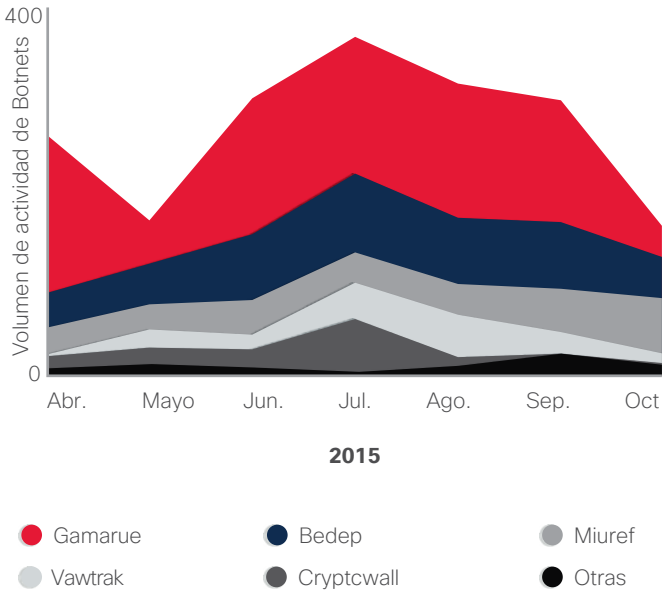
Es por esto que insistimos en la importancia de que los equipos de seguridad dediquen más recursos a supervisar este riesgo y que consideren el aumento del uso de sistemas automatizados que les ayuden a priorizar las amenazas.

Control y mando total de botnets: descripción general

Las botnets son redes de ordenadores infectadas con malware. Los atacantes pueden controlarlas como un grupo y ordenarles que realicen una tarea concreta, como el envío de spam o el lanzamiento de un ataque de DDoS. En los últimos años han crecido tanto en tamaño como en número. Para entender mejor el panorama actual de amenazas a escala mundial, hemos analizado las redes de 121 empresas entre abril y octubre de 2015 con el fin de identificar la presencia de una o más de ocho de las botnets más frecuentes. Los datos se normalizaron para ofrecer una descripción general de la actividad de las botnets (figura 10).

Durante este periodo observamos que Gamarue, un ladrón modular de información multifunción conocido desde hace años, era la amenaza de control y mando más habitual.

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



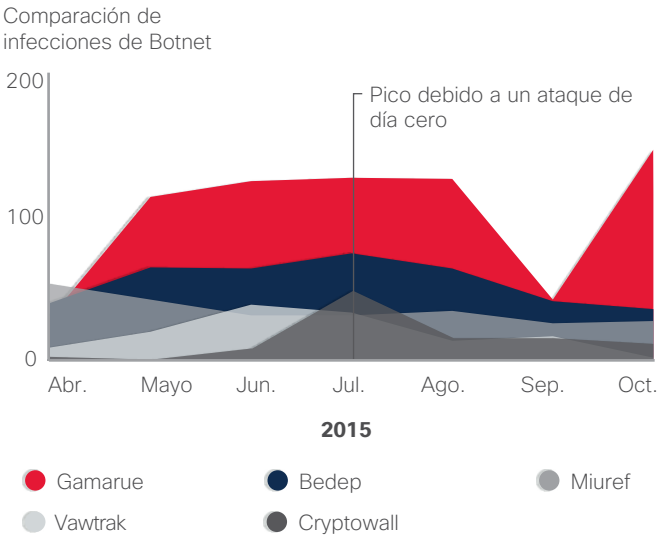
Fuente: grupo de investigaciones de seguridad de Cisco

En julio identificamos un aumento significativo del número de infecciones relacionadas con el ransomware Cryptowall 3.0. Esta actividad se atribuye en gran medida a Angler, cuya capacidad de difundir la carga de Cryptowall es ya conocida. Tal y como se muestra en el informe de seguridad semestral de Cisco 2015, los creadores de Angler y otros kits de aprovechamiento de vulnerabilidades se han dado prisa en aprovechar el tiempo de ausencia de parches de Adobe Flash, esto es, el tiempo entre el lanzamiento de una actualización de Adobe y el momento en el que el usuario instala la actualización.[2] Los investigadores de amenazas de Cisco atribuyen el aumento de julio de 2015 al ataque de día cero de Flash CVE-2015-5119 expuesto como parte de las filtraciones de Hacking Team.[3]

Angler también es responsable del troyano Bedep, utilizado para realizar campañas de fraude por clic. También en el mes de julio se observó un ligero aumento en la prevalencia de esta amenaza (figura 11).

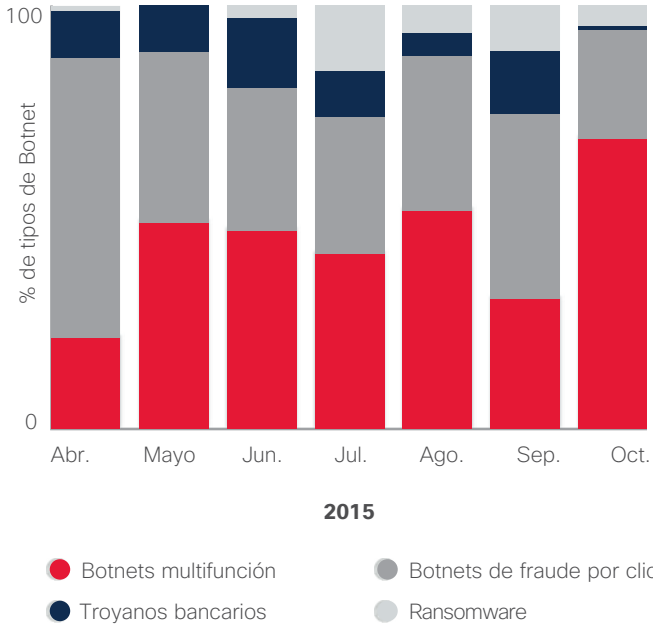
Bedep, Gamarue y Miuref (otro troyano y secuestrador de navegador que puede realizar fraude por clic) representaron en conjunto más del 65% de la actividad de control y mando de botnet en la base de usuarios objeto de investigación.

Figura 11. Alcance mensual de las amenazas, en función del número de usuarios infectados



Fuente: grupo de investigaciones de seguridad de Cisco

Figura 12. Alcance mensual de las amenazas en función de su categoría



Fuente: grupo de investigaciones de seguridad de Cisco

El porcentaje de infecciones de Bedep se mantuvo relativamente estable durante el periodo del análisis. Sin embargo, se observó una disminución de las infecciones de Miuref. Este hecho podría atribuirse al aumento del tráfico HTTPS, que ayudó a ocultar los indicadores de compromiso de Miuref.

La figura 12 muestra los tipos de botnets responsables de la mayoría de las infecciones en el periodo de tiempo que vigilamos. Las botnets multifunción, como Gamarue y Sality, están a la cabeza, seguidas por las botnets de fraude por clic. Los troyanos bancarios ocupan la tercera posición, lo que demuestra que este tipo de amenaza, a pesar de sus años de existencia, sigue estando muy extendida.

COMPARTIR

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

El punto débil de los DNS: ataques mediante DNS para obtener control y mando

El análisis de Cisco de malware validado como "problema conocido" concluyó que la mayoría de este malware (91,3%) utiliza el sistema de nombres de dominio con alguno de los fines siguientes:

- Para obtener control y mando
- Para robar datos
- Para redirigir el tráfico

Para obtener este porcentaje, extrajimos todos los comportamientos de muestra de diversos sandboxes propios. El malware que no utilizaba DNS en ningún modo, o que simplemente lo utilizaba para realizar comprobaciones de estado de Internet, se retiró del análisis de la muestra. El malware restante utilizaba DNS para conectarse a sitios validados como maliciosos o que se consideraban sospechosos.

A pesar de la dependencia de DNS que tienen los atacantes para apoyar sus campañas de malware, pocas empresas realizan un control de DNS con fines de seguridad (o incluso no realizan control alguno). Esta falta de previsión convierte a los DNS en una herramienta ideal para los atacantes. Según una encuesta reciente realizada por Cisco (consulte la figura 13), el 68% de los profesionales de la seguridad coincide en que sus organizaciones no realizan un control para evitar las amenazas de DNS recursivos. (Los servidores de nombres DNS recursivos proporcionan las direcciones IP de nombres de dominio esperados a los hosts solicitantes).

Figura 13. Supervisión de amenazas desde DNS recursivos

Fuente: grupo de investigaciones de seguridad de Cisco

¿Por qué los DNS son puntos débiles para tantas organizaciones? Uno de los principales motivos es que los equipos de seguridad y los expertos en DNS normalmente trabajan en diferentes grupos de TI dentro de la empresa y no interactúan con frecuencia.

Pero deberían hacerlo. La supervisión de los DNS es esencial para identificar y contener las infecciones de malware que ya utilizan DNS con uno de los fines señalados anteriormente. Es además un importante primer paso a la hora de planear otros componentes que pueden emplearse para investigar un ataque en profundidad, tanto para la identificación del tipo de infraestructura que soporta el ataque como para averiguar su origen.

No obstante, para la supervisión de DNS se requiere mucho más que la colaboración entre los equipos de seguridad y DNS. Es necesaria la alineación de la tecnología y la experiencia adecuadas para llevar a cabo un análisis de correlación. (Para obtener más información, consulte "La colaboración del sector ayuda a Cisco a aislar y detener el avance de una campaña de ransomware y exploit kit altamente rentable", en la **página 10** para descubrir cómo OpenDNS ayudó a Cisco a obtener mayor visibilidad del dominio de las IP que el exploit kit Angler estaba utilizando).

ANÁLISIS RETROSPECTIVO DE DNS

La investigación retrospectiva de Cisco sobre consultas de DNS y el posterior tráfico TCP y UDP identifica varios orígenes de malware. Entre ellos se incluyen servidores de control y mando, páginas web y puntos de distribución. Esta investigación retrospectiva también ha servido para detectar contenido que supone una amenaza elevada y que utiliza información de listas de amenazas, informes de amenazas de comunidades, tendencias observadas en cuanto a ciberriesgos, y conocimiento de las vulnerabilidades exclusivas para el sector de un cliente determinado.

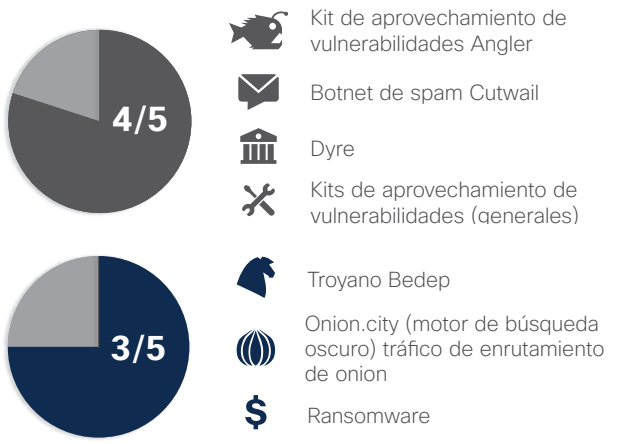
Nuestro informe retrospectivo ayuda a identificar los intentos de filtración "baja y lenta" que normalmente están asociados con un comportamiento de amenazas persistentes avanzadas (APT) y que, en muchos casos, pasan inadvertidos para las tecnologías de detección de amenazas tradicionales. El objetivo del análisis es identificar anomalías en el vasto volumen de tráfico de comunicaciones salientes. Este enfoque "de dentro hacia fuera" permite detectar posibles vulnerabilidades de datos y actividades de red dañinas que podrían, de otro modo, pasar desapercibidas.

De este modo hemos podido destapar clientes DNS (resolvers) maliciosos en uso en redes de clientes. Los clientes no eran conscientes de que sus empleados utilizaban dichos "resolvers" como parte de su infraestructura de DNS. La falta de control y gestión activos del uso de los clientes DNS puede originar un comportamiento malicioso, como el envenenamiento de caché DNS y el redireccionamiento de DNS.

Además de descubrir e identificar clientes DNS maliciosos, la investigación retrospectiva también ha permitido poner de manifiesto los siguientes problemas de redes de clientes:

- Espacio de dirección de clientes encontrado en listas de bloqueo de malware y spam de terceros
- Espacio de dirección de clientes utilizado como guía para los conocidos servidores de control y mando Zeus y Palevo
- Campañas activas de malware, como CTB-Locker, Angler y DarkHotel
- Actividades sospechosas, incluido el uso de Tor, reenvío automático de correo electrónico y conversión de documentos online
- Tunelización generalizada de DNS a dominios registrados en China
- "Typosquatting" de DNS[4]
- Clientes internos que evitan la infraestructura DNS de confianza del cliente

Al observar la muestra seleccionada de clientes de Cisco Custom Threat Intelligence en varios segmentos verticales, también identificamos los siguientes tipos de malware en el porcentaje respectivo del número total de clientes examinados:



[4] El "typosquatting" consiste en registrar un nombre de dominio similar a un nombre de dominio existente. Se trata de una estrategia utilizada por los atacantes para captar a aquellos usuarios que se equivoquen al introducir el nombre de dominio.

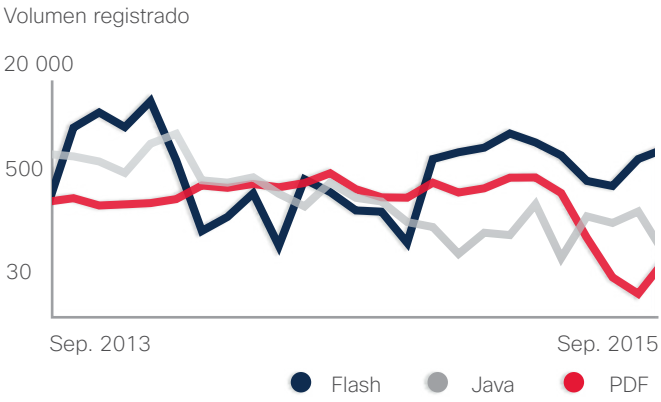
Análisis de la inteligencia de amenazas

Vectores de ataques web

ADOBE FLASH: EN VÍAS DE DESAPARICIÓN, FINALMENTE

A pesar de que el volumen total de Flash se ha reducido en el último año (consulte la siguiente sección, **"Tendencias de contenido de Adobe Flash y PDF"**), sigue siendo una de las herramientas favoritas para los desarrolladores de kits de aprovechamiento de vulnerabilidades. De hecho, en 2015 no hubo una tendencia perceptible por lo que respecta al malware Flash, ni de ascenso ni de descenso (figura 14). Es probable que el malware relacionado con Flash siga siendo uno de los principales vectores de explotación de vulnerabilidades durante un tiempo (los creadores de Angler se centraron en gran medida en las vulnerabilidades de Flash).

Figura 14. Distribución de los vectores de ataque, comparativa de dos años



Fuente: grupo de investigaciones de seguridad de Cisco

La presión del sector para eliminar Adobe Flash de la navegación en Internet está generando un descenso en la cantidad de contenido Flash presente en la Web (consulte la siguiente sección, **"Tendencias de contenido de Adobe Flash y PDF"**). Esto es similar a lo que ha ocurrido con el contenido Java en los últimos años y que, al final, ha generado una constante tendencia descendente en el volumen de malware de Java (de hecho, los creadores de Angler ya ni siguiera se molestan en incluir ataques contra Java). Mientras tanto, el volumen de malware de PDF se ha mantenido bastante constante.

Microsoft Silverlight también ha disminuido como vector de ataque, ya que muchos proveedores han dejado de ofrecer soporte para la API que utiliza Silverlight para integrarse en los navegadores. Muchas empresas están dejando de utilizar Silverlight y adoptando el uso de tecnologías basadas en HTML5. Microsoft ha indicado que no prevé un futuro lanzamiento de Silverlight y actualmente solo ofrece actualizaciones de seguridad.

TENDENCIAS DE CONTENIDO DE ADOBE FLASH Y PDF

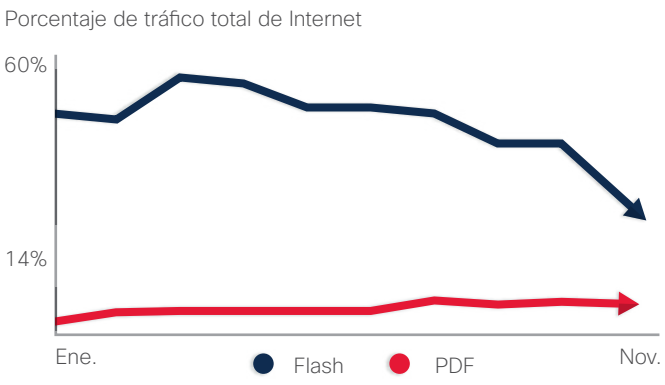
Los investigadores de Cisco han observado un descenso general de la cantidad de contenido de Adobe Flash en la Web (figura 15). Las recientes acciones de Amazon, Google y otros importantes protagonistas de Internet han sido determinantes en la disminución del contenido Flash. Estas empresas han dejado de aceptar anuncios que utilizan Flash, o bien lo bloquean.

Por otro lado, el contenido PDF se ha mantenido estable el último año y es probable que continúe así. Sin embargo, no ha sido un importante vector de ataques web desde hace algún tiempo.

Es probable que, a corto plazo, continúe el descenso del contenido Flash, o incluso que se acelere, ahora que Adobe ha anunciado la desaparición escalonada de Flash.[5] Sin embargo, posiblemente pasará algún tiempo hasta que el contenido Flash desaparezca por completo. Flash está integrado en navegadores como Google Chrome, Microsoft Internet Explorer y Microsoft Edge y su uso sigue estando muy extendido en contenido web, incluso en contenido de vídeo y juegos.

Sin embargo, en los próximos años, a medida que se adoptan nuevas tecnologías (como HTML5 y plataformas móviles), la tendencia a largo plazo para los vectores de ataques web como Java, Flash y Silverlight resulta bastante clara. Con el tiempo, serán cada vez menos frecuentes. Por lo tanto, es probable que sean vectores cada vez menos atractivos para atacantes en busca de beneficios económicos, que preferirán centrarse en otros vectores que les permitan explotar con facilidad un gran número de usuarios, generando así ingresos con mayor rapidez.

Figura 15. Porcentaje de tráfico total de Flash y PDF

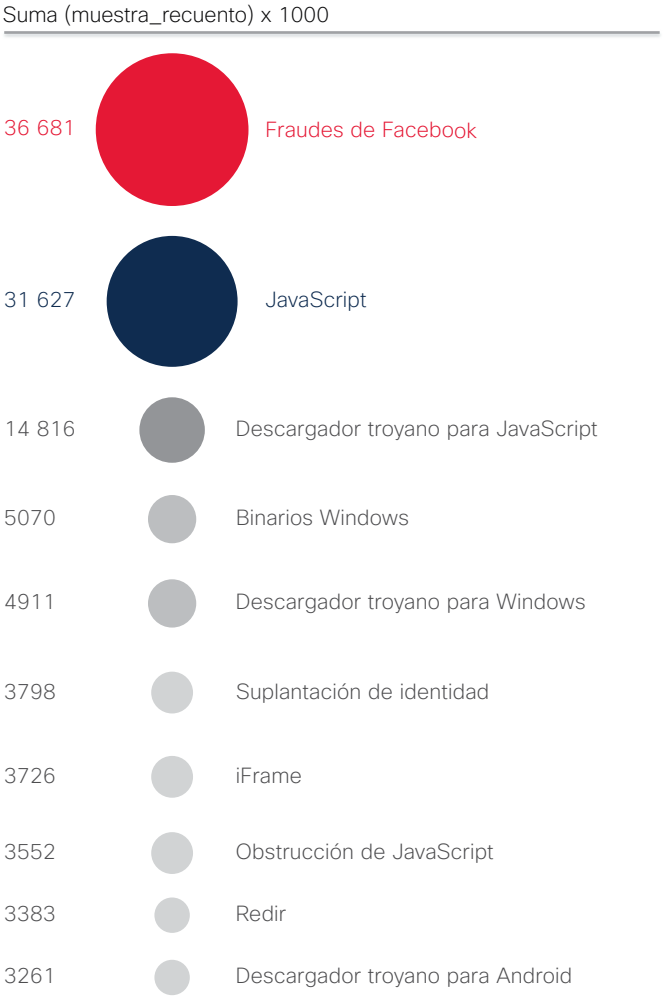


Fuente: grupo de investigaciones de seguridad de Cisco

Métodos de ataques web

Las figuras 16 y 17 muestran los diferentes tipos de malware que utilizan los atacantes para acceder a las redes de las organizaciones. La figura 16 muestra los tipos de malware más habituales: adware, spyware, redireccionadores maliciosos, vulnerabilidades de iFrame y suplantación de identidad.

Figura 16. Malware más frecuente



Fuente: grupo de investigaciones de seguridad de Cisco

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

La figura 16 se puede considerar una recopilación de los tipos de malware que los ciberdelincuentes utilizan para obtener el acceso inicial. Estos son los métodos probados y más rentables para atacar a un gran volumen de usuarios con relativa facilidad. Las vulneraciones de JavaScript y los fraudes de Facebook (ingeniería social) fueron los métodos de ataque más frecuentes, según se desprende de nuestra investigación.

La figura 17 muestra un volumen menor de malware. Hay que tener en cuenta que un "menor volumen" no supone una "menor eficacia". Según el grupo de investigación de seguridad de Cisco, un volumen menor de malware puede significar que están surgiendo nuevas amenazas o campañas extremadamente selectivas.

Muchas de estas técnicas más sofisticadas están diseñadas para obtener el máximo valor posible de los usuarios expuestos. Roban datos de gran valor o "secuestran" los recursos digitales de los usuarios y piden rescates por ellos.

Por lo tanto, al supervisar el malware web, no es suficiente con centrarse solo en los tipos de amenazas más frecuentes. Hay que tener en cuenta la gama completa de ataques.

Figura 17. Muestra de malware observado de menor volumen

Fuente: grupo de investigación de seguridad de Cisco

Actualizaciones de amenazas

ADOBE FLASH OCUPA EL PRIMER LUGAR EN LA LISTA DE VULNERABILIDADES

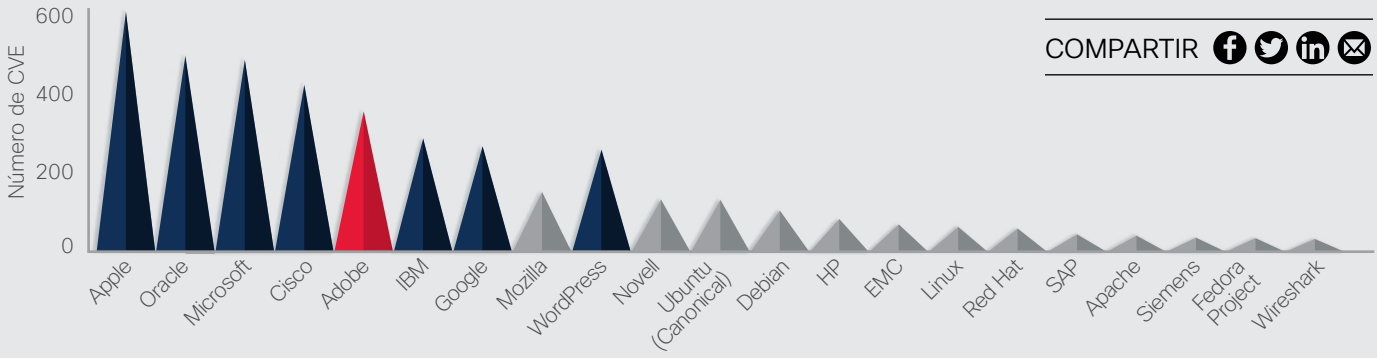
La plataforma de Adobe Flash ha sido un vector de amenazas muy popular entre los ciberdelincuentes durante muchos años. Las vulnerabilidades de Flash siguen apareciendo con frecuencia en las listas de alertas de extrema urgencia. Por lo que respecta al año 2015, la buena noticia es que los proveedores de productos a los que afectaban con frecuencia estas vulnerabilidades, como navegadores web, reconocieron su debilidad y han emprendido las acciones necesarias para reducir las posibilidades de ataque de los ciberdelincuentes.

En 2016, es muy probable que los ciberdelincuentes dirijan sus ataques y exploits a usuarios de Adobe Flash. Algunas de estas vulnerabilidades de Flash tienen exploits disponibles online, ya sea públicamente o a la venta como parte de kits de aprovechamiento de vulnerabilidades. (Como se ha indicado en la **página 21**, el volumen de contenido Flash se ha reducido, pero Flash sigue siendo uno de los principales vectores de ataque).

Siguiendo las tácticas utilizadas para reducir el impacto de Java, otro vector de ataques habitual, muchos navegadores web bloquean o aíslan (sandboxing) el contenido Flash con el fin de proteger a los usuarios. Aunque esto supone un avance positivo, es importante recordar que los atacantes seguirán lanzando ataques con éxito durante un tiempo. Es posible que los usuarios no actualicen sus navegadores de la forma adecuada y los ciberdelincuentes seguirán lanzando ataques dirigidos a las versiones más antiguas del software de los navegadores.

Sin embargo, los investigadores de Cisco creen que las protecciones que ahora se integran en los navegadores web y sistemas operativos más comunes aminorarán la confianza que los ciberdelincuentes tienen en Flash. Dado que los atacantes online se centran en la obtención de los mejores resultados posibles (como una alta rentabilidad) con la máxima eficacia, apenas se ocupan de ataques con menos probabilidades de generar ingresos.

Figura 18. Número total de CVE por proveedor



COMPARTIR

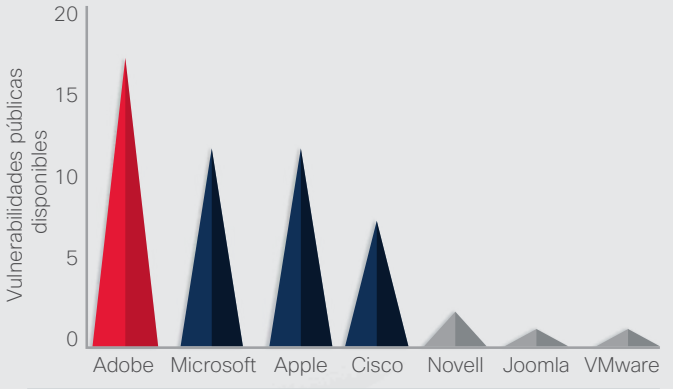
Fuente: grupo de investigaciones de seguridad de Cisco, National Vulnerability Database

El anterior gráfico muestra el número total de CVE publicados en 2015 por proveedor. Se observa que Adobe no es tan prominente en este gráfico como en el gráfico de la derecha, que muestra las vulnerabilidades para las que hay exploits disponibles.

Además, WordPress muestra solo 12 vulnerabilidades para 2015 para su propio producto. Las 240 vulnerabilidades adicionales proceden de plugins y scripts creados por contribuidores externos.

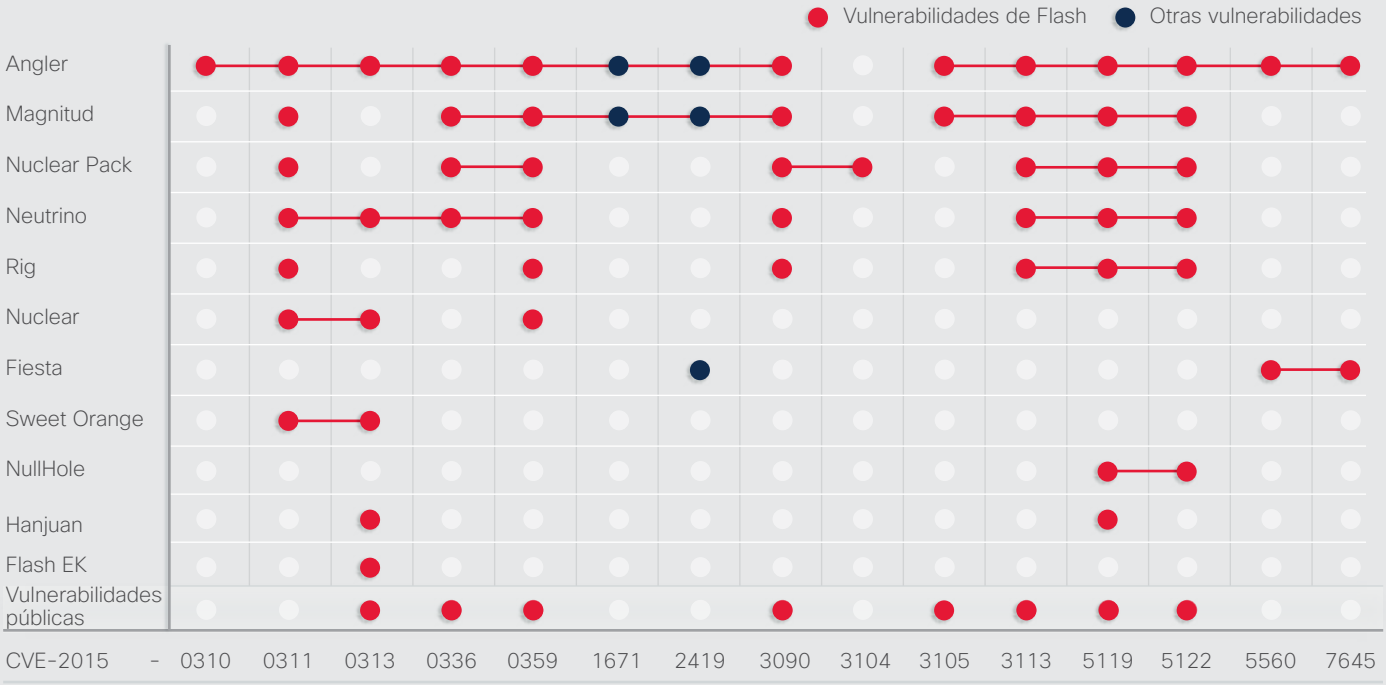
Como muestra la figura 20, las listas de vulnerabilidades y exploits relacionados pueden servir de orientación a los profesionales de la seguridad. Estos pueden utilizarlas para gestionar y priorizar las vulnerabilidades más comunes y que representan un riesgo mayor, y de este modo aplicarles los parches necesarios antes que a las vulnerabilidades de menor riesgo. Consulte la página web de detalles de CVE **(https://www.cvedetails.com/top-50-products.php)** para obtener más información sobre las CVE por proveedor.

Figura 19. Número de exploits públicos disponibles por vulnerabilidad de proveedor



Fuente: grupo de investigaciones de seguridad de Cisco, Metasploit, Exploit DB

Figura 20. Vulnerabilidades comunes



Fuente: grupo de investigaciones de seguridad de Cisco

La figura 20 muestra las vulnerabilidades de mayor riesgo e indica si la vulnerabilidad forma parte de un kit de aprovechamiento de vulnerabilidades de alquiler (consulte la línea "Flash EK") o tiene exploits disponibles públicamente (consulte la línea "Vulnerabilidades públicas"). Las vulnerabilidades para las que hay exploits funcionales disponibles tienen una prioridad alta a la hora de aplicar parches.

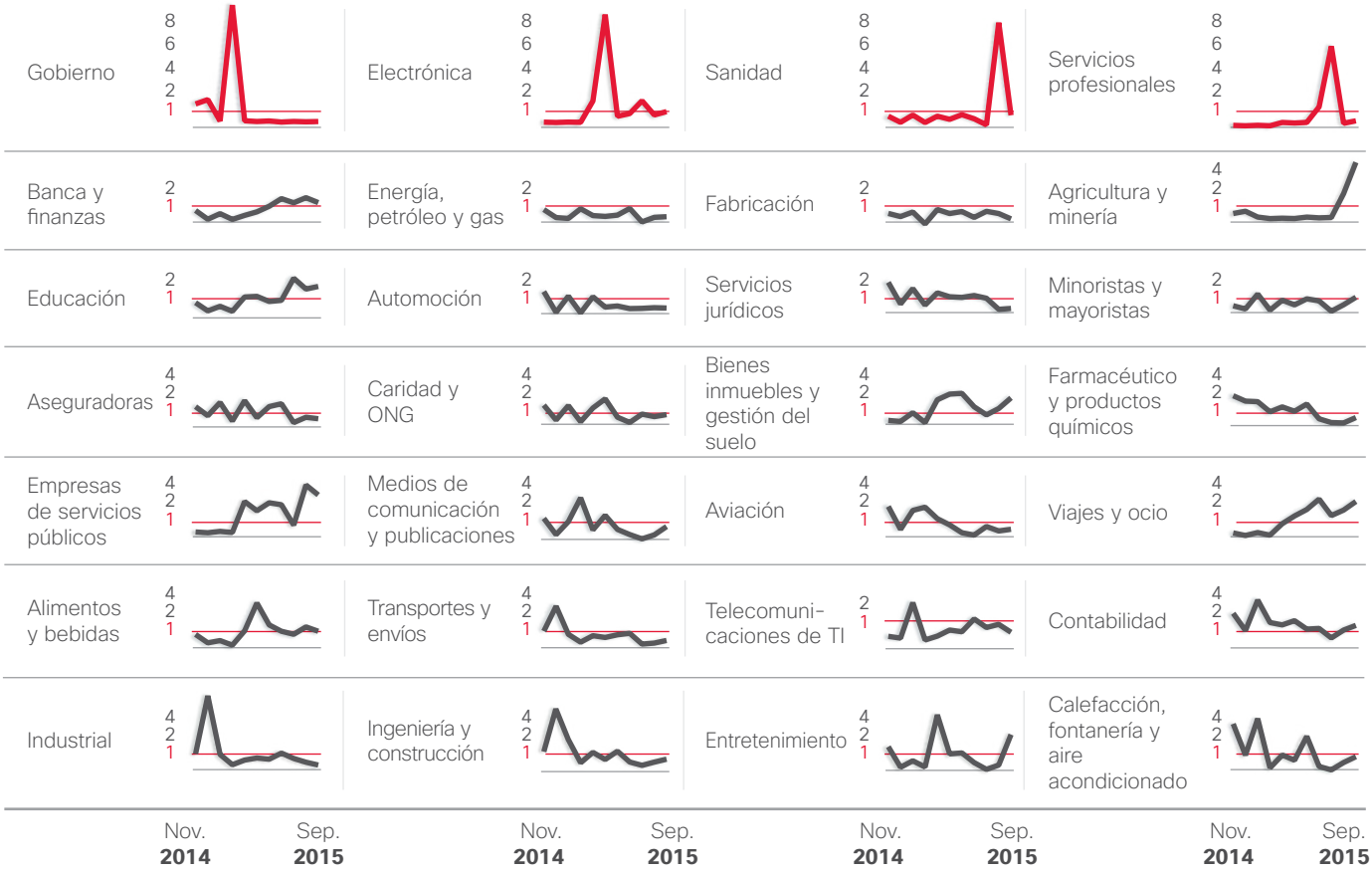
Esta lista se puede utilizar para ayudar a los profesionales de la seguridad a priorizar sus actividades de aplicación de parches y solución de incidencias. La existencia de una vulnerabilidad para un determinado producto, ya sea públicamente o como parte de un kit de aprovechamiento de vulnerabilidades, no indica necesariamente que se estén produciendo ataques.

Riesgo de incidencias de malware para los mercados verticales

Con el fin de realizar un seguimiento de los mercados verticales con mayor riesgo de ser atacados por malware web, examinamos los volúmenes relativos de tráfico de los ataques (índices de bloqueo) y el tráfico "normal" o esperado.

La figura 21 muestra los 28 sectores principales y su actividad de bloqueo relevante 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 valor por encima de 1,0 representa tasas de bloqueos superiores a las esperadas. Por el contrario, un valor inferior a 1,0 representa tasas de bloqueo inferiores a las esperadas.

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

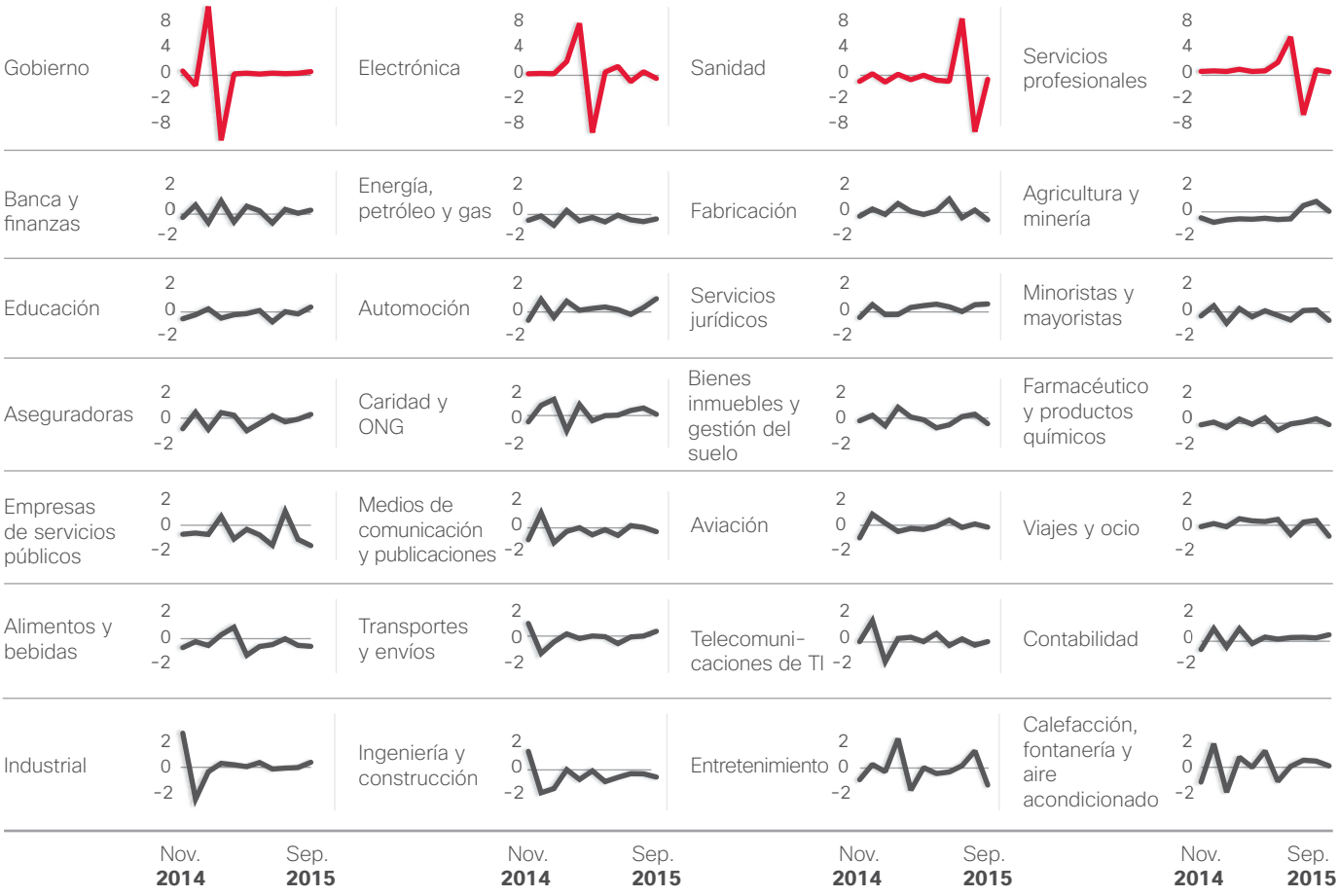


Fuente: grupo de investigaciones de seguridad de Cisco

La figura 22 muestra el carácter efímero del enfoque de los atacantes hacia mercados verticales específicos (el cero significa que no ha habido ningún cambio). Desde enero a marzo de 2015, la administración pública era el mercado vertical con el mayor índice de bloqueo. Entre marzo y mayo, lo era el sector de la electrónica. A mitad del verano, el índice más alto de bloqueos correspondió a los servicios profesionales. Y en otoño de 2015, fue la sanidad el sector que lideró los mercados verticales por índice de bloqueo.

Según nuestra investigación, los cuatro mercados verticales con mayor actividad de bloqueo en 2015 sufrieron ataques de troyanos. El mercado vertical de la administración pública tuvo que hacer frente a un número elevado de ataques de inyección PHP, mientras que el mercado vertical de los servicios profesionales recibió un gran número de ataques de iFrame.

Figura 22. Índices relativos de bloqueo de mercados verticales, comparación mes a mes



Fuente: grupo de investigaciones de seguridad de Cisco

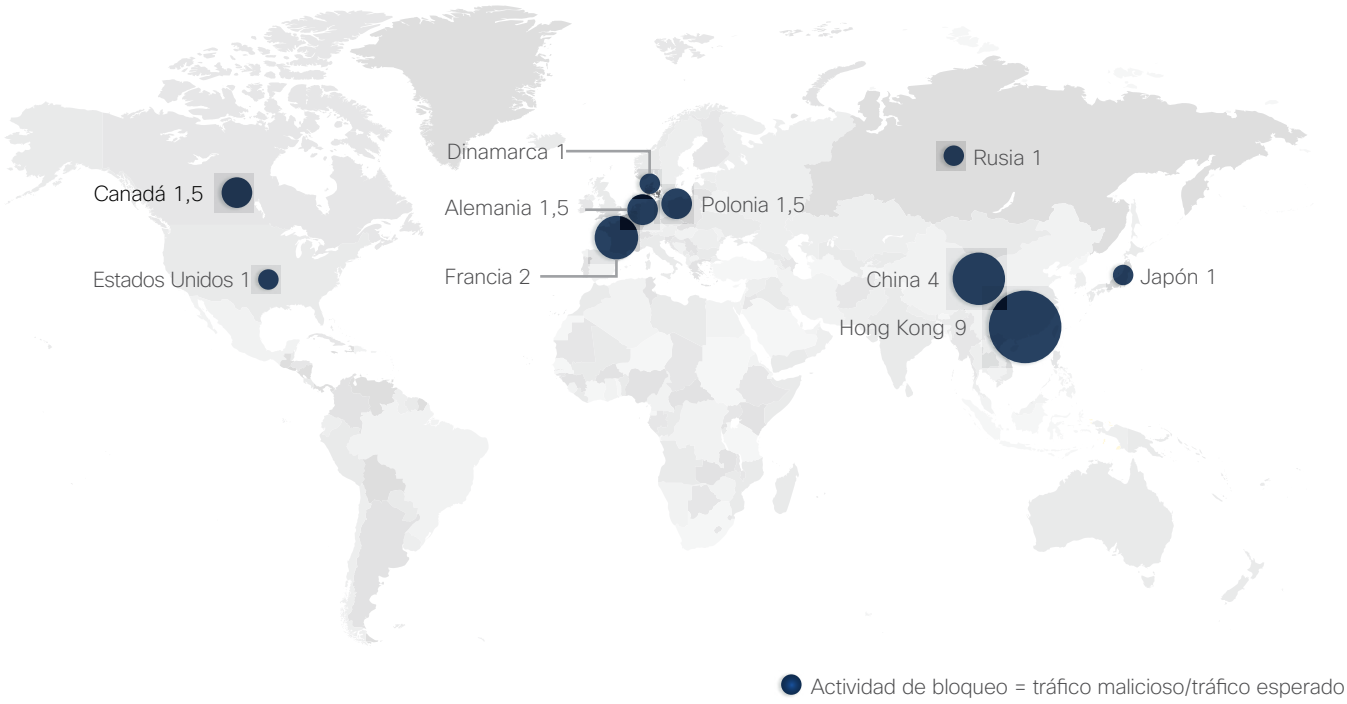
COMPARTIR

Actividad de bloqueo web: descripción general por zonas y países

También analizamos el origen de la actividad de bloqueo de malware por región o país, tal como muestra la figura 23. Los países se seleccionaron para el estudio en función de su volumen de tráfico de Internet. Una proporción de bloqueos de 1,0 significa que el número de bloqueos observado es proporcional al tamaño de la red.

Es posible que los países y las regiones con una actividad de bloqueos por encima de lo normal tengan numerosos servidores web y hosts con vulnerabilidades sin parches en sus redes. Los sujetos maliciosos no conocen fronteras y alojan el malware allí donde creen que resultará más eficaz.

Figura 23. Bloqueos web por país o región



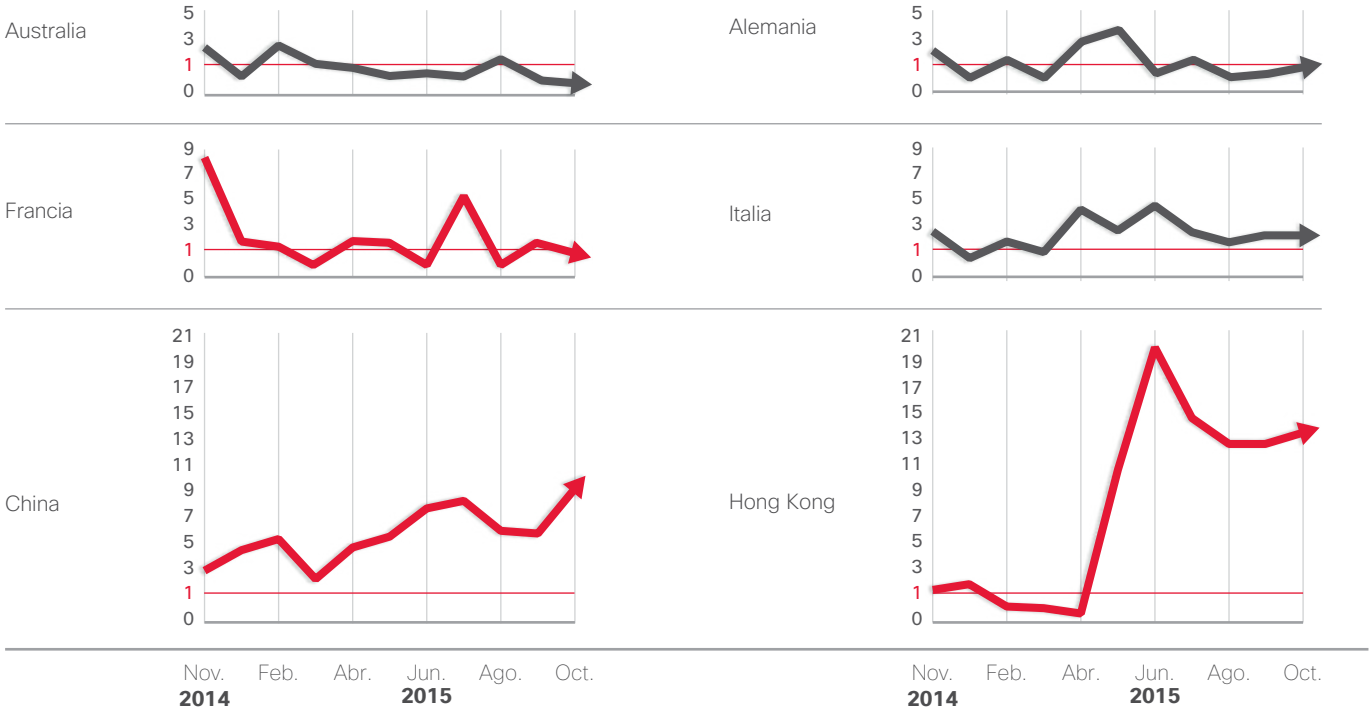
Fuente: grupo de investigaciones de seguridad de Cisco

La presencia en redes de gran tamaño y viables comercialmente que gestionan un alto volumen de tráfico de Internet es otro de los factores para una elevada actividad de bloqueo. Esta es una de las razones por las que Hong Kong ocupa el primer lugar de la lista.

La figura 24, que muestra una comparativa mensual de los bloqueos web en función del país o región entre noviembre de 2014 y octubre de 2015, proporciona contexto adicional para estas clasificaciones.

Puede observarse que Hong Kong experimentó una actividad de bloqueo web mayor de lo habitual al principio de la primavera de 2015, al igual que Francia. Desde entonces, ambos países muestran un descenso significativo en su actividad de bloqueo web pero, dado que los índices elevados de actividad a principios de este año estaban tan alejados de la línea de base, a pesar del reciente descenso de actividad, Hong Kong sigue teniendo un índice más elevado al final del año que al principio. Los índices máximos de actividad de bloqueo de Francia volvieron a niveles normales a mitad del verano.

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



Fuente: grupo de investigaciones de seguridad de Cisco

Perspectivas del sector

Consideraciones del sector

Cisco proporciona investigación y análisis sobre tendencias y prácticas de seguridad. De forma sorprendente, ciertos elementos pueden complicar la capacidad de los responsables de seguridad para rastrear amenazas y señalar a las organizaciones y a los usuarios individuales con mayor riesgo de peligro o ataque.

Cifrado: una tendencia creciente y un reto para los responsables de seguridad

El cifrado es importante. Las empresas necesitan proteger la propiedad intelectual y otros datos confidenciales, los publicistas desean conservar la integridad del contenido de los anuncios y los análisis back-end, y las empresas se están centrando más en la protección de la privacidad de sus clientes.

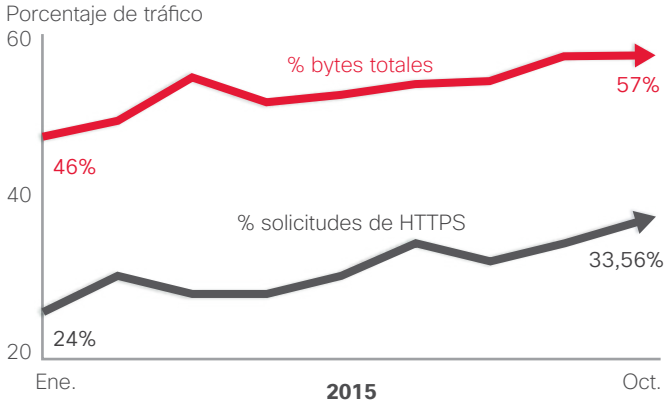
Pero el cifrado también genera problemas de seguridad para las organizaciones, lo que provoca una falsa sensación de seguridad. Las organizaciones han mejorado el cifrado de datos cuando se transmiten entre entidades, pero el resto de los datos suelen seguir estando poco protegidos. Muchas de las brechas más notables de los últimos años se han aprovechado de datos sin cifrar almacenados en el Data Center y en otros sistemas internos. Para los atacantes, esto es como seguir un camión de suministros protegido a un almacén desbloqueado.

También es importante que las organizaciones entiendan que el cifrado de extremo a extremo puede reducir la eficacia de algunos productos de seguridad. El cifrado oculta los indicadores de compromiso utilizados para identificar y controlar la actividad maliciosa.

Pero no hay excusa para no cifrar los datos confidenciales. Las herramientas de seguridad y sus operadores tienen que adaptarse a este valiente nuevo mundo recopilando encabezados y otras partes no cifradas del flujo de datos junto con otros orígenes de información contextual para analizar el tráfico cifrado. Las herramientas que confían en la visibilidad de pagos, como la captura de paquetes completos, se plantean menos eficaces. La ejecución de Cisco NetFlow y otros análisis basados en metadatos ahora es fundamental.

Al observar las tendencias de 2015, los investigadores sugieren que el tráfico cifrado, especialmente HTTPS, ha alcanzado un punto de inflexión. Aunque no son la mayoría de las transacciones, pronto se convertirán en la forma dominante de tráfico en Internet. De hecho, nuestro estudio muestra que ya representa de forma constante más del 50 por ciento (figura 25) de los bytes transferidos debido a la sobrecarga de HTTPS y al mayor contenido que se envía a través de HTTPS, como las transferencias a sitios de almacenamiento de archivos.

Figura 25. Porcentajes de SSL



Fuente: grupo de investigaciones de seguridad de Cisco

En cualquier transacción web, se envían (de salida) y se reciben varios bytes (de entrada). Las transacciones HTTPS tienen solicitudes de salida mayores que las solicitudes de salida HTTP, lo que supone un incremento de 2000 bytes. Sin embargo, las solicitudes HTTPS de entrada también tienen sobrecarga, pero esto es menos significativo con respuestas más grandes.

Al combinar los bytes de entrada y de salida por transacción web, podemos determinar el porcentaje total de todos los bytes implicados por transacción web que se cifran mediante HTTPS. Debido al aumento del tráfico HTTPS y a la sobrecarga adicional, determinamos que los bytes HTTPS representaban el 57 por ciento de todo el tráfico web en octubre de 2015 (figura 25), frente al 46 por ciento en enero.

También determinamos mediante el análisis de tráfico web que las solicitudes HTTPS han aumentado de forma gradual y significativa desde enero de 2015. Como muestra la figura 25, el 24 por ciento de las solicitudes de enero ha usado el protocolo HTTPS; el resto de ellas ha utilizado HTTP.

En octubre, el 33,56 por ciento de las solicitudes observadas era HTTPS. Además, descubrimos que el porcentaje de bytes HTTPS de entrada había aumentado. Esto ha sido así a lo largo del año. A medida que aumenta la cantidad de tráfico que usa HTTPS, es necesario más ancho de banda. Se necesitan 5 Kbps adicionales por transacción.

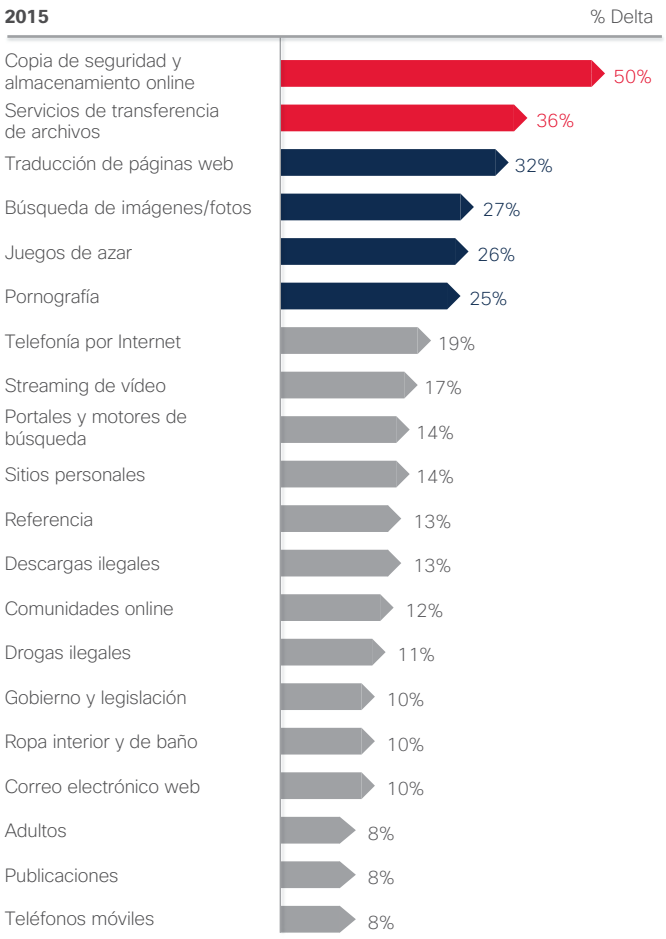
En nuestra opinión, el aumento masivo del tráfico web cifrado se debe principalmente a estos factores:

- **Más tráfico móvil de aplicaciones que, intrínsecamente, está cifrado**
- **Más solicitudes de usuarios para descargar vídeo cifrado**
- **Más solicitudes hacia servidores de copia de seguridad y almacenamiento que contienen "datos confidenciales," que los enemigos desean aprovechar**

De hecho, en la figura 26 se muestra que las solicitudes HTTPS hacia recursos de copia de seguridad y almacenamiento online habían aumentado en un 50 por ciento desde el inicio del año 2015. Los servicios de transferencia de archivos también han aumentado considerablemente durante el mismo período: un 36 por ciento.

En última instancia, hay un aumento en la actividad de cifrado que se produce tanto en el número de transacciones cifradas como en el número de bytes cifrados en cada transacción. Cada uno tiene sus propias ventajas y riesgos potenciales, lo que conduce a la necesidad de una defensa integrada frente a amenazas que ayude a aumentar a visibilidad.

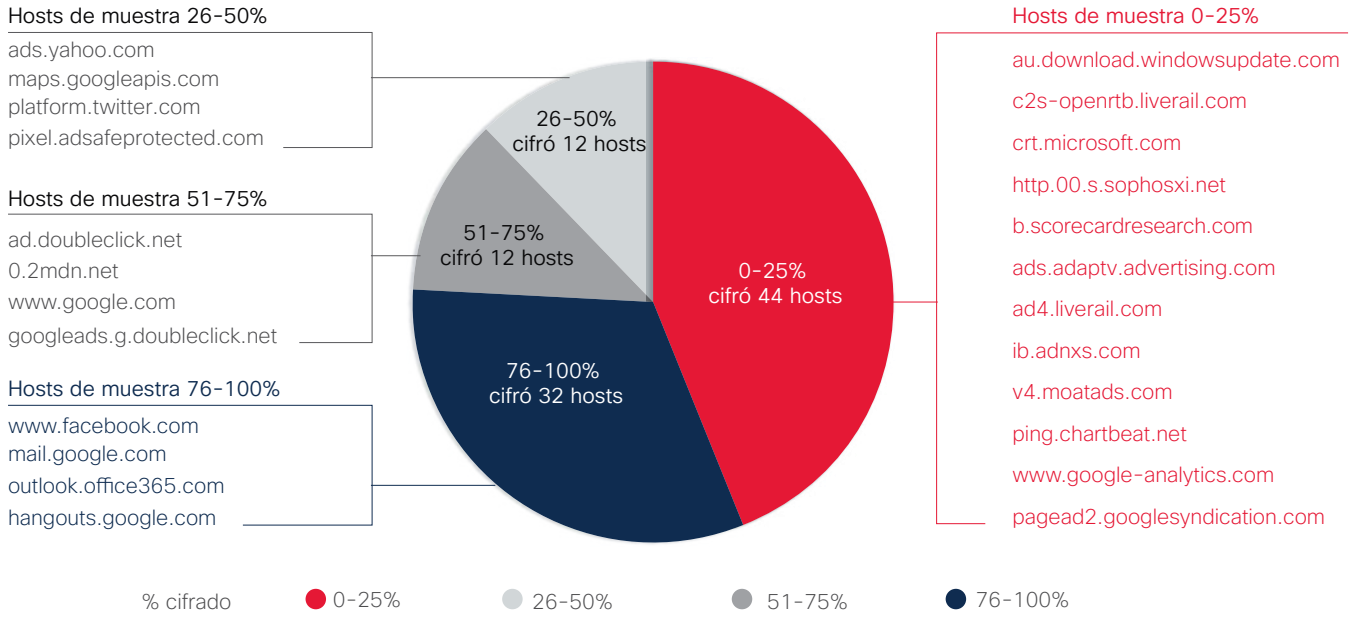
Figura 26. Solicitudes HTTPS: los cambios más grandes de enero a septiembre de 2015



Fuente: grupo de investigaciones de seguridad de Cisco

COMPARTIR

Figura 27. Principales hosts que cifran tráfico HTTPS



Fuente: grupo de investigaciones de seguridad de Cisco

Observando los principales dominios por solicitudes (figura 27), vemos que muchas de las páginas de contenido principales de Google y Facebook están cifradas. Normalmente, solo el 10 por ciento del tráfico de publicidad está cifrado.

Independientemente de los retos, el cifrado de datos es un requisito en el panorama de amenazas actual. Los atacantes son demasiado expertos en eludir el control de acceso de los usuarios para dejar desprotegida la información crítica en cualquier fase del almacenamiento o de la transferencia.

Esta es la razón por la que es fundamental que los equipos de seguridad controlen los patrones de tráfico web para garantizar que las solicitudes HTTPS no provengan ni se dirijan a ubicaciones sospechosas. Precaución: No busque tráfico cifrado en un conjunto predefinido de puertos. Como se explica en la siguiente sección, nuestro estudio muestra que es probable que el malware inicie comunicaciones cifradas en un conjunto de varios puertos.

EL FACTOR DE LA ENTROPÍA

La alta entropía es una buena indicación de comunicaciones o transferencias de archivos comprimidas o cifradas.[6] La buena noticia para los equipos de seguridad es que la entropía es relativamente fácil de supervisar porque no requiere conocer los protocolos de cifrado subyacentes.

Durante un período de tres meses, desde el 1 de junio de 2015, los investigadores de seguridad de Cisco observaron 7 480 178 flujos de los cuales 598.138 ejemplos de malware se enviaron con una "puntuación de amenaza: 100". Entre ellos, había 958 851 flujos de alta entropía durante este período, es decir, el 12,82 por ciento.

También se identificaron 917 052 flujos sobre el protocolo Seguridad de la capa de transporte (TLS) (el 12,26 por ciento). Además, 8419 flujos TLS eran sobre un puerto distinto de 443, el puerto predeterminado para HTTP seguro. Algunos de los puertos en los que se ha observado el malware usado para comunicaciones eran los puertos 21, 53, 80 y 500.

A medida que el nivel del tráfico de Internet cifrado sigue aumentando, será cada vez más importante que las organizaciones adopten una arquitectura integrada de defensa contra amenazas (consulte "Los seis aspectos de la defensa integrada contra amenazas" en la **página 62**). Las soluciones diseñadas para momentos específicos no resultan eficaces en la identificación de amenazas potenciales de tráfico cifrado. Las plataformas de seguridad integradas proporcionan a los equipos de seguridad mayor visibilidad de todo lo que sucede en los dispositivos o las redes, para que así puedan identificar más fácilmente los patrones de actividades sospechosas.

[6] Entropía: en informática, la entropía (es decir, la falta de orden o de previsión) es la aleatoriedad recopilada por un sistema operativo o una aplicación para su uso en el cifrado o para otros usos que requieren datos aleatorios.

El cambio hacia el cifrado: datos del caso

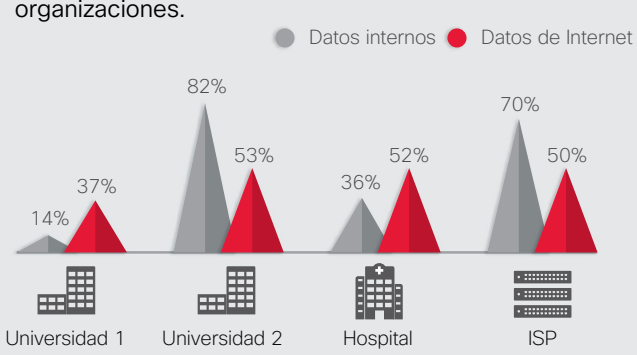
Lancope, una empresa de Cisco, examinó las tasas de cifrado de tráfico de Internet e interno en tres sectores empresariales (dos universidades, un hospital y un proveedor ISP, todos ubicados en Estados Unidos).

En una de las universidades, Lancope descubrió que casi todo el tráfico interno estaba cifrado (el 82 por ciento). Además, el 53 por ciento del tráfico de Internet de la universidad estaba cifrado. Estos resultados estaban a la par con las tendencias que Lancope había observado en otros sectores industriales.

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

En el proveedor ISP líder, el 70 del tráfico interno estaba cifrado y el 50 por ciento del tráfico de Internet estaba cifrado.

El estudio de Lancope cuenta la historia de una amplia adopción del cifrado de datos que se mueven entre diferentes sectores. Cisco recomienda que ahora debe aplicarse un enfoque similar en el cifrado de datos al resto para limitar los efectos de los riesgos en las organizaciones.



Fuente: Lancope Threat Research Labs

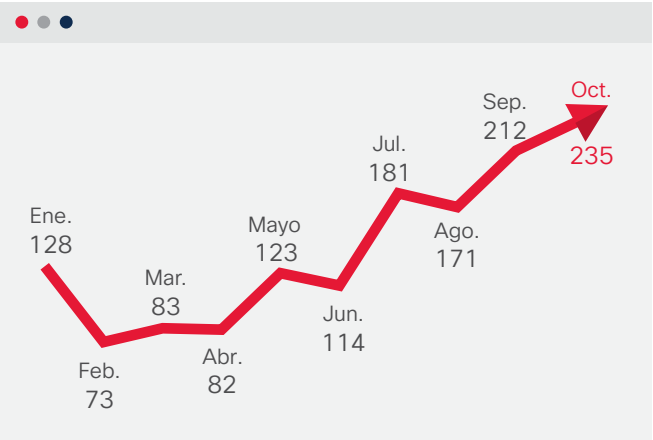
Los ciberdelincuentes aumentan la actividad del servidor en WordPress

Como se ha explicado en la introducción de este informe, los ciberdelincuentes buscan constantemente métodos para aportar eficacia y ahorro de costes a sus operaciones, además de nuevas formas de evitar su detección. Cada vez más, los ciberdelincuentes encuentran esta eficacia en sitios web creados con WordPress, la conocida plataforma de desarrollo de blogs y Webs. En las Webs creadas con WordPress, los atacantes pueden controlar un flujo constante de servidores en riesgo para crear una infraestructura que propicie el ransomware, el fraude bancario o los ataques de suplantación de identidad. Internet está lleno de sitios abandonados creados con WordPress que no se mantienen desde el punto de vista de la seguridad; a medida que surgen nuevos problemas de seguridad, estos sitios se ven a menudo comprometidos y se incorporan a campañas de ataques.

Al analizar los sistemas utilizados para propiciar el ranso mware y otro malware, los investigadores de seguridad de Cisco observaron que muchos ciberdelincuentes están derivando la actividad online a servidores WordPress comprometidos. El número de dominios WordPress usados por los delincuentes ha crecido un 221 por ciento entre febrero y octubre de 2015 (consulte la figura 28).

Los investigadores de Cisco creen que este cambio de escenario se ha producido por una serie de motivos. Cuando el ransomware utiliza otras herramientas para comunicar claves de cifrado u otra información de control y mando, las comunicaciones pueden detectarse o bloquearse, lo que impide que se complete el proceso de cifrado. Sin embargo, las comunicaciones que retransmiten claves de cifrado entre servidores WordPress comprometidos pueden parecer normales, lo que aumenta las posibilidades de que de se complete el cifrado del archivo. En otras palabras, las Webs creadas con WordPress actúan como agentes de retransmisión.

Figura 28. Número de dominios WordPress usados por creadores de malware



Fuente: grupo de investigaciones de seguridad de Cisco

Para evitar los inconvenientes de otras tecnologías, los delincuentes han cambiado a WordPress, que utilizan para alojar cargas de malware y servidores de control y mando. Las Webs creadas con WordPress ofrecen numerosas ventajas. Por ejemplo, muchos sitios web abandonados ofrecen a los delincuentes más oportunidades para comprometer sitios dotados de una protección de seguridad débil.

El riesgo de utilizar sistemas comprometidos para ejecutar una operación de malware es que uno de los servidores pirateados puede desactivarse cuando se detecta el ataque. Si esto se produce en medio de una campaña, el descargador de malware no puede recuperar su carga o es posible que el malware no pueda comunicarse con los servidores de "control y mando". Los investigadores de seguridad de Cisco han observado que el malware sobrecarga esto usando más de un servidor WordPress; Cisco incluso descubrió listas de servidores WordPress comprometidos almacenadas en sitios de datos compartidos como Pastebin.

El malware usaba estas listas para encontrar servidores operativos de "control y mando", lo que permitía que el malware actuara incluso si un servidor comprometido fallaba. Los investigadores también identificaron descargadores de malware que contenían una lista de sitios web creados con WordPress que almacenaban cargas. Si un sitio de descarga no funcionaba, el malware iba al siguiente y descargaba cargas maliciosas del servidor WordPress operativo.

Con frecuencia, los sitios WordPress comprometidos no funcionaban con la última versión de WordPress, tenían a menudo contraseñas de administrador débiles y usaban plugins al los que les faltaban parches de seguridad.

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

Los investigadores de Cisco han identificado algunos tipos de archivos y software alojados en Webs creadas con WordPress comprometidas:

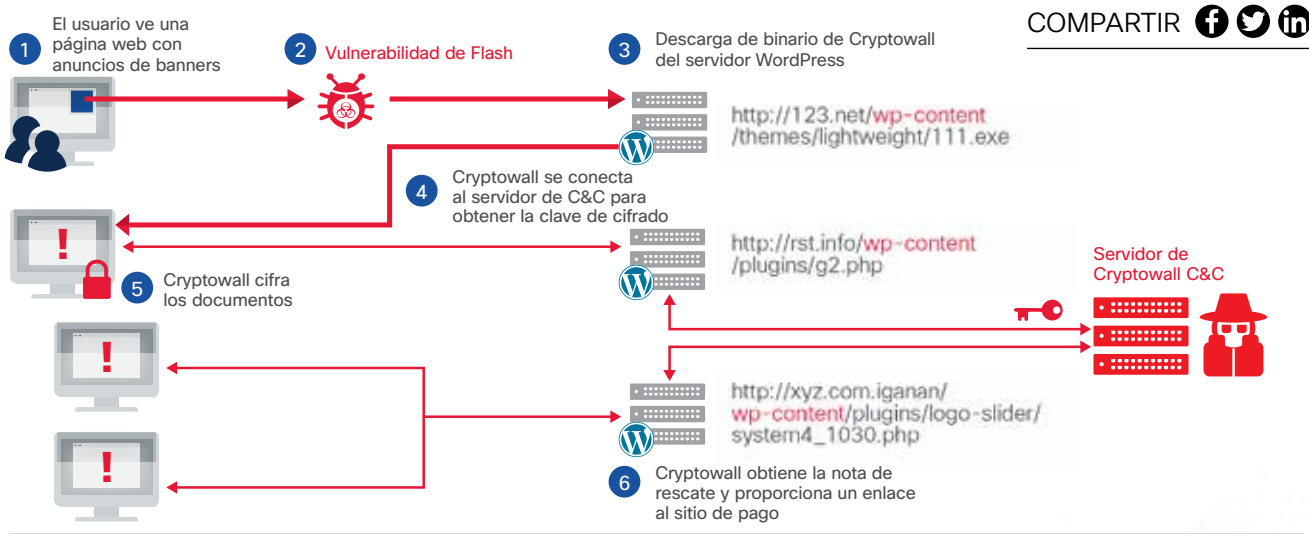
- Archivos ejecutables que son cargas para aprovecharse de ataques del kit
- Archivos de configuración de malware como Dridex y Dyre
- Código proxy que retransmite comunicación de "control y mando" para ocultar infraestructura de "control y mando"
- Páginas web de suplantación de identidad para recopilar nombres de usuario y contraseñas
- Scripts de HTML que redirigen tráfico para aprovecharse de servidores del kit

Además, los investigadores de Cisco han identificado muchas familias de malware que utilizan sitios web creados con WordPress comprometidos para infraestructura:

- Ladrón de información Dridex
- Ladrón de contraseñas Pony
- Ransomware TeslaCrypt
- Ransomware Cryptowall 3.0
- Ransomware TorrentLocker
- Botnet de spam Andromeda
- Difusor de troyanos Bartallex
- Ladrón de información Necurs
- Páginas de inicio de sesión falsas

Figura 29. Cómo se comprometen los sitios creados con WordPress

COMPARTIR



Fuente: grupo de investigaciones de seguridad de Cisco

Los profesionales de la seguridad preocupados por las amenazas de que plantea WordPress deben buscar tecnología de seguridad web que examine el contenido de los sitios creados con WordPress. Este tráfico puede considerarse inusual si la red descarga programas de sitios creados con WordPress en lugar de simplemente páginas web e imágenes (aunque las Webs creadas con WordPress pueden alojar también programas legítimos).

Infraestructura antigua: un problema de 10 años

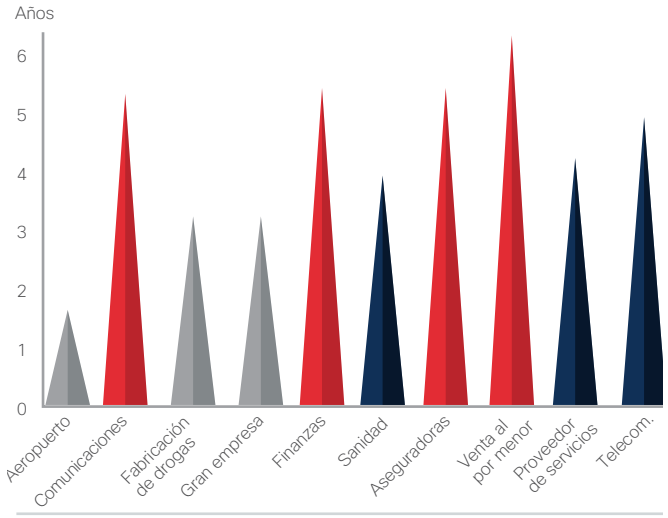
Todas las empresas actuales son empresas de TI hasta cierto punto, ya que dependen de su infraestructura de TI y de TO (tecnología operativa) para estar conectados, estar informatizados y tener éxito. Esto significa que necesitan que la seguridad de la TI sea una prioridad. Sin embargo, muchas organizaciones confían en las infraestructuras de red integradas de componentes antiguos, obsoletos, que ejecutan sistemas operativos vulnerables y que no son tecnológicamente flexibles.

Hemos analizado recientemente 115 000 dispositivos de Cisco en Internet y en entornos de clientes como una forma de atraer la atención sobre los riesgos de seguridad que plantea la presente infraestructura antigua y que carece de atención para solucionar problemas de vulnerabilidad.

Hemos identificado los 115 000 dispositivos en nuestro ejemplo de un día buscando en Internet y, después, analizando los dispositivos desde "fuera hacia adentro" (desde el punto de vista de Internet y dentro de la empresa). En nuestro análisis, descubrimos que 106 000 de los 115 000 dispositivos tenían vulnerabilidades conocidas en el software que ejecutaban. Esto significa que el 92 por ciento de los dispositivos de Cisco presente en Internet de nuestro ejemplo es susceptible de vulnerabilidades conocidas.

Cisco también ha descubierto que la versión del software con la que funcionaban estos dispositivos tenía de media 26 vulnerabilidades. Además, hemos detectado que muchas organizaciones tenían software desactualizado funcionando en su infraestructura de red (figura 30). Descubrimos que algunos clientes de los mercados verticales financieros, sanitarios y minoristas usaban versiones de nuestro software con más de 6 años de antigüedad.

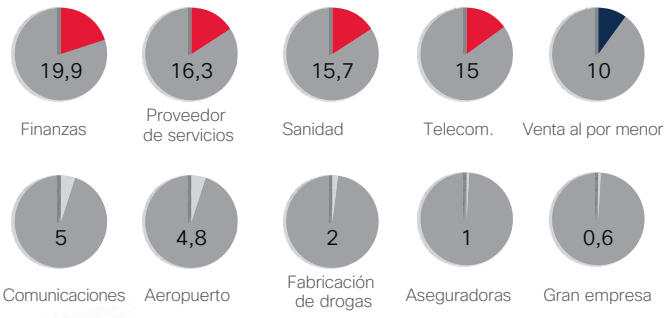
Figura 30. Edad media del software en años



Source: Cisco Security Research

También hemos detectado 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 hacerse más seguros (figura 31). Estos dispositivos ni siquiera reciben parches para las vulnerabilidades conocidas, por lo que no se les proporciona información sobre nuevas amenazas. Se ha avisado a los clientes del problema.

Figura 31. Porcentaje de LDoS para dispositivos de infraestructura



Fuente: grupo de investigaciones de seguridad de Cisco

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

"Seguridad de TI: cuando se sobrestima la madurez"

"Evolución de los ataques en dispositivos Cisco IOS"

"Golpe de SYNful: detectar y mitigar ataques al software Cisco IOS"

Además, el 8 por ciento de los 115 000 dispositivos analizados en nuestro ejemplo ha alcanzado su fin de vida y otro 31 por ciento alcanzará el fin de soporte técnico en un plazo de entre uno y cuatro años.

La infraestructura de TI anticuada y desactualizada es una vulnerabilidad para las organizaciones. A medida que nos acercamos a Internet of Things (IoT) y a Internet of Everything (IoE), cada vez es más importante para las empresas asegurarse de que confían en una infraestructura de red que es segura, lo que garantiza la integridad de los datos y las comunicaciones que abarcan toda la red. Esto es fundamental para el éxito del IoE que acaba de emerger.

Muchos clientes de Cisco crearon su infraestructura de red hace una década. En ese momento, muchas empresas no solo contaban con el hecho de que la infraestructura sería fiable al 100 por cien. Ni siquiera anticiparon que su infraestructura se convertiría en un objetivo prioritario para los adversarios.

Las organizaciones suelen evitar realizar actualizaciones de infraestructuras porque es algo costoso y que requiere tiempo de inactividad en la red. En algunos casos, una simple actualización no sería suficiente. Algunos productos son tan antiguos que no se pueden actualizar para incorporar las últimas soluciones de seguridad necesarias para proteger la empresa.

Estos simples hechos hablan de la importancia del mantenimiento de la infraestructura. Las organizaciones tienen que planificar actualizaciones periódicas y reconocer el valor de controlar su infraestructura crítica de una forma proactiva antes de que lo haga un adversario.

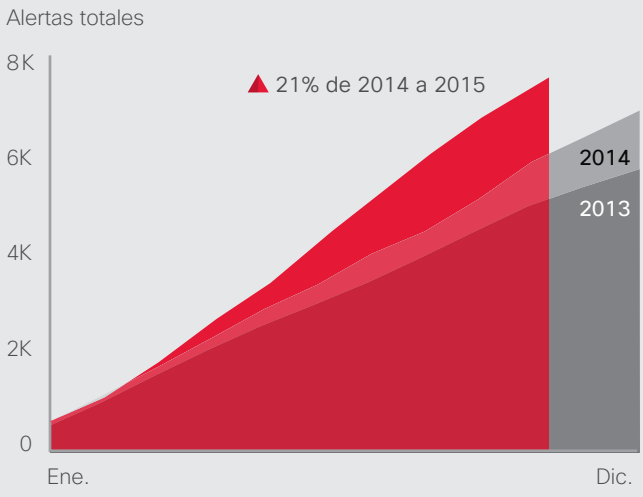
El número total de alertas acumuladas muestra el crecimiento del riesgo a vulnerabilidades de gestión

La dependencia de infraestructuras antiguas abre la puerta a los atacantes. Sin embargo, el aumento de alertas acumuladas, que incluyen vulnerabilidades de productos en soluciones de código abierto y propietarias, es un indicio positivo de que el sector tecnológico presta mucha atención a la eliminación de oportunidades para los atacantes.

El número total de alertas acumuladas aumentó un 21 por ciento de 2014 a 2015. De julio a septiembre de 2015, el aumento fue notablemente alto. Este aumento se puede atribuir en gran parte a importantes actualizaciones de software de proveedores como Microsoft y Apple, ya que las actualizaciones de productos derivan en más informes de vulnerabilidades de software.

Los principales proveedores de software ahora ofrecen un mayor volumen de parches y actualizaciones y son más transparentes sobre esta actividad. El creciente volumen es fundamental para las organizaciones que automatizan la gestión de vulnerabilidades mediante el uso de inteligencia de seguridad y plataformas de gestión que ayudan a administrar el volumen del inventario del sistema y de software, de vulnerabilidades y de información de amenazas. Estos sistemas e interfaces de programación de aplicaciones (API) permiten una gestión de la seguridad más eficaz y puntual en organizaciones de cualquier tamaño.

Figura 32. Número total de alertas acumuladas anuales



Fuente: grupo de investigaciones de seguridad de Cisco

COMPARTIR

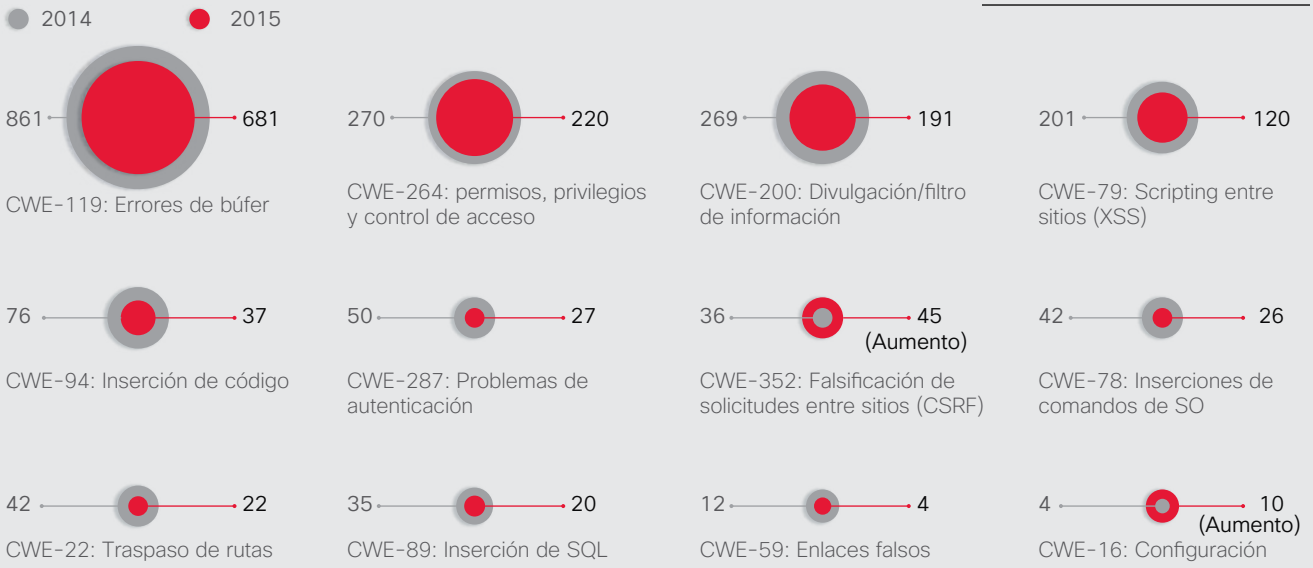
Categorías de amenazas: reducción de errores de búfer, filtraciones y divulgaciones de información

Al examinar las categorías comunes de vulnerabilidades, las vulnerabilidades de scripts entre sitios (XSS) disminuyeron un 47 por ciento de 2014 a 2015 (figura 33). La reducción puede ser resultado de una mayor atención prestada a las pruebas de vulnerabilidad. Los proveedores se han hecho más expertos en la identificación de estas vulnerabilidades concretas y su resolución antes de que sus productos lleguen al mercado.

Las vulnerabilidades de filtración o de divulgación de información descendieron un 15 por ciento en 2015. Estas vulnerabilidades implican divulgaciones involuntarias a terceros que no cuentan con un acceso explícito. Los proveedores han estado atentos a controles que permiten o no permiten el acceso a datos, haciendo que esta vulnerabilidad habitual se repita con menor frecuencia.

Figura 33. Número de vulnerabilidades en categorías comunes

COMPARTIR



Fuente: grupo de investigaciones de seguridad de Cisco

¿Las PYMES son el punto débil para la seguridad de la empresa?

Las PYMES desempeñan un papel fundamental en las economías nacionales. Cuando se les confía datos de sus clientes, las PYMES también tienen la responsabilidad de proteger esta información contra atacantes online. Sin embargo, como se detalla en el estudio comparativo sobre capacidades de seguridad de Cisco 2015 (consulte la **página 41**), las PYMES muestran signos de que sus defensas contra atacantes son más débiles de lo que les exigen sus retos. A su vez, estos puntos débiles pueden poner en riesgo a los clientes empresariales de las PYMES. Los atacantes que pueden vulnerar la red de una PYME, también podrían encontrar una puerta de entrada en una red empresarial.

Según los resultados del Estudio comparativo sobre capacidades de seguridad de Cisco 2014, las PYMES utilizan menos procesos para analizar riesgos y menos herramientas de defensa contra amenazas de las que utilizaban el año pasado. Por ejemplo, el 48 por ciento de las PYMES afirmaron en 2015 que usaban seguridad web; el 59% afirmó que lo hacía en 2014. Solo el 29% ha dicho que usaban parches y configuración en 2015, en comparación con el 39% en 2014.

Además, de los encuestados de PYMES que no tienen un responsable ejecutivo de seguridad, aproximadamente una cuarta parte no cree que sus empresas sean objetivos de gran valor para los ciberdelincuentes. Esta opinión indica un exceso de confianza en la capacidad de su empresa para evitar los sofisticados ataques online actuales o bien que los ataques nunca ocurrirán en su empresa.

LAS PYMES SON MENOS PROPENSAS A UTILIZAR EQUIPOS DE RESPUESTA ANTE INCIDENTES

En muchos casos, es menos probable que las PYMES tengan equipos de inteligencia de amenazas y de respuesta ante incidentes que las grandes empresas. Esto puede deberse a limitaciones de presupuesto; los encuestados declararon que los problemas de presupuesto eran uno de los obstáculos más importantes para adoptar procesos y tecnología de seguridad avanzados. El setenta y dos por ciento de las grandes empresas (con más de 1000 empleados) posee estos dos tipos de equipos, en comparación con el 67 por ciento 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 niveles previos al incidente (figura 35). Por ejemplo, el 53 por ciento de las empresas con más de 10 000 empleados utilizan análisis de flujo de red para analizar los sistemas en riesgo, en comparación con el 43 por ciento de las empresas con menos de 500 empleados. El sesenta por ciento de las empresas con más de 10 000 empleados usaron parches y actualizaciones en aquellas aplicaciones consideradas vulnerables, en comparación con el 51 por ciento de las empresas con menos de 500 empleados.

El uso por parte de las PYMES de determinadas defensas frente a amenazas parece disminuir. Por ejemplo, en 2014, el 52 por ciento de las PYMES usaban seguridad para la movilidad, pero solo el 42 por ciento lo hizo en 2015. Además, en 2014, el 48 por ciento de las PYMES utilizó el análisis de vulnerabilidades, en comparación con el 40 por ciento en 2015 (consulte la figura 36).

Figura 34. Los mayores obstáculos de las PYMES

¿Cuáles de los siguientes considera que son los principales obstáculos para la adopción de procesos y tecnologías de seguridad avanzados?

Tamaño de la empresa	250-499	500-999	1 000-9 999	10 000+
Restricciones presupuestarias	40%	39%	39%	41%
Problemas de compatibilidad con sistemas heredados	34%	30%	32%	34%
Prioridades competitivas	25%	25%	24%	24%

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 36. Las defensas de las PYMES disminuyen en 2015

¿Cuáles de los siguientes tipos de defensas frente a amenazas de seguridad utiliza actualmente su organización?	2014	2015
Seguridad móvil	52%	42%
Conexión inalámbrica segura	51%	41%
Análisis de vulnerabilidades	48%	40%
VPN	46%	36%
Información de seguridad y gestión de eventos (SIEM)	42%	35%
Pruebas de penetración	38%	32%
Diagnóstico de red	41%	29%
Configuración y aplicación de parches	39%	29%
Diagnóstico de terminales	31%	23%

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 35. Las PYMES utilizan menos procesos de seguridad que las grandes empresas

¿Cuáles de estos procesos utiliza su organización para analizar los sistemas en peligro?

Tamaño de la empresa	250-499	500-999	1 000-9 999	10 000+
Diagnóstico de memoria	36%	36%	35%	34%
Análisis del flujo de la red	43%	47%	52%	53%
Análisis de registros/eventos correlacionados	34%	34%	40%	42%
Equipos de análisis/respuestas de incidentes externos (de terceros)	40%	32%	34%	39%
Análisis de registros del sistema	47%	51%	55%	59%
Análisis del registro	43%	47%	52%	53%
Detección de IOC	31%	34%	37%	36%
¿Qué procesos utiliza su organización para restaurar los sistemas afectados a su nivel operativo previo al incidente?				
Aplicación de parches y actualizaciones a aplicaciones que se consideren vulnerables	51%	53%	57%	60%
Implementación de detecciones y controles nuevos o adicionales	49%	55%	57%	61%

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

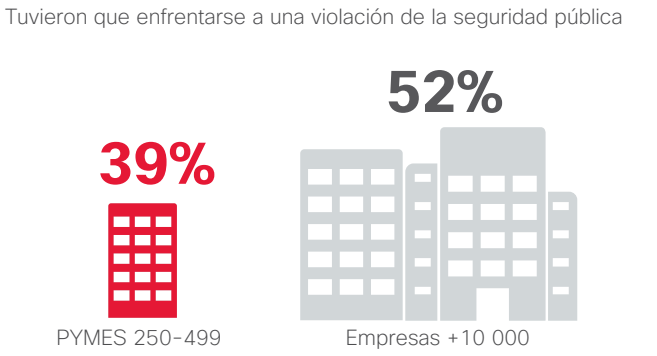
¿Por qué es importante que las PYMES tiendan a utilizar menos defensas que sus homólogos más grandes? En un entorno de seguridad en el que los atacantes desarrollan tácticas más sofisticadas para entrar en las redes y no ser detectados, ninguna empresa puede permitirse dejar sus redes sin proteger o desactivar procesos que pueden ofrecer información sobre cómo se produjo un riesgo para que se pueda evitar en el futuro.

Además, las PYMES pueden no darse cuenta de que su propia vulnerabilidad se puede traducir en riesgos para clientes empresariales más grandes y sus redes. Los delincuentes actuales a menudo acceden a una red como un medio para encontrar un punto de entrada a otra red más rentable y las PYMES pueden ser el punto de partida para dicho ataque.

ES MENOS PROBABLE QUE HAYAN EXPERIMENTADO BRECHAS DE DATOS PÚBLICOS

Es menos probable que las PYMES, en vez de las grandes empresas, se hayan enfrentado a una brecha de seguridad pública, probablemente como resultado de su menor tamaño desde el punto de vista de la red. Mientras que el 52 por ciento de las empresas con más de 10 000 empleados se han enfrentado a las consecuencias de una brecha en la seguridad pública, solo el 39 por ciento de las empresas con menos de 500 empleados lo ha hecho.

Figura 37. Las PYMES notifican menos brechas públicas

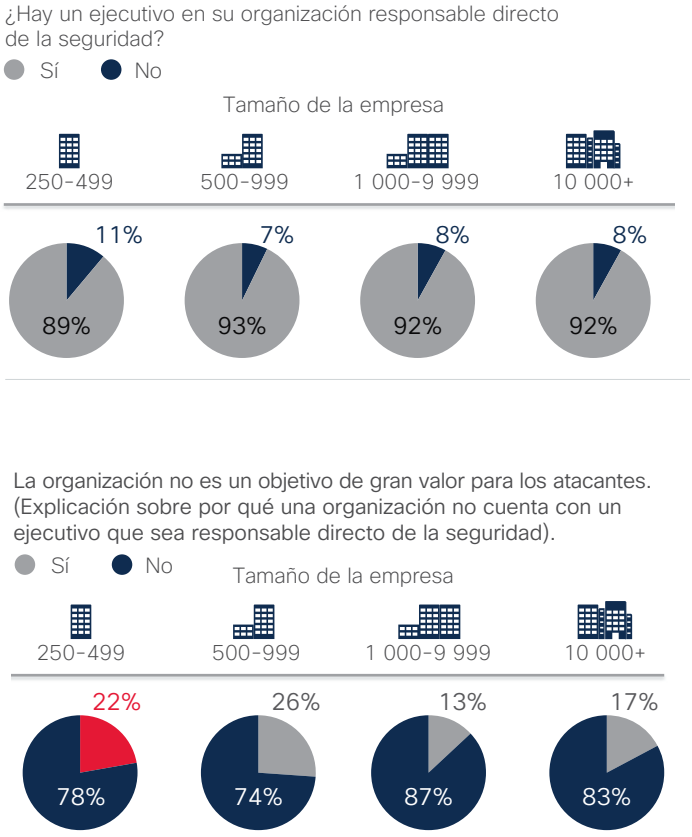


Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

COMPARTIR

Las brechas de seguridad públicas son obviamente perjudiciales y dañinas para una empresa, pero ofrecen una ventaja: con frecuencia animan a las empresas a echar un vistazo a sus protecciones de seguridad y a considerar fortalecerlas. Los datos de la encuesta de Cisco (consulte la **página 74**) muestran que cuando las grandes empresas experimentan una brecha en datos públicos, actualizan de forma significativa la tecnología de seguridad e implementan procesos más sólidos.

Figura 38. Las PYMES no se ven a ellas mismas como objetivos de gran valor



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

La imagen que tienen las PYMES de sus negocios como objetivos de ciberdelincuentes puede demostrar una deficiencia en su percepción del panorama de amenazas. Como se mostraba anteriormente en la figura 38, el 22 por ciento de las empresas con menos de 500 empleados afirmaba que no tenían un ejecutivo con responsabilidad directa sobre la seguridad porque no se consideran objetivos de gran valor.

Las PYMES FUERON MÁS PROPENSAS A SUBCONTRATAR FUNCIONES DE SEGURIDAD EN 2015

Aunque la encuesta muestra que lo más habitual en las PYMES es subcontratar algunas de sus funciones de seguridad, es menos probable que las PYMES, en comparación con las grandes empresas, subcontraten determinados servicios, como el asesoramiento y la consultoría. Por ejemplo, el 55 por ciento de las grandes empresas subcontratan los servicios de asesoramiento y consultoría, en comparación con el 46 por ciento de las empresas con menos de 500 empleados. El cincuenta seis por ciento de las grandes empresas subcontratan las auditorías de seguridad, en comparación con el 42 por ciento de las empresas con menos de 500 empleados (consulte la figura 39).

Sin embargo, en 2015, cada vez más PYMES han subcontratado algunos servicios de seguridad. En 2014, el 24 por ciento de las PYMES con menos de 499 empleados afirmó que no subcontrató ningún servicio. En 2015, solo el 18 por ciento de las PYMES indicó lo mismo.

El hecho de que cada vez más PYMES adopten la subcontratación como una forma de gestionar la seguridad es una buena noticia. Indica que las PYMES buscan herramientas flexibles para proteger las redes que no supongan una carga para su menor número de empleados o para presupuestos más conservadores. Sin embargo, las PYMES pueden creer de manera equivocada que los procesos de subcontratación de seguridad reducirán considerablemente la posibilidad de que se produzca una brecha en la red. O pueden trasladar la responsabilidad de la seguridad a un tercero. Este punto de vista sería una ilusión, ya que solo un sistema de defensa contra amenazas verdaderamente integrado, que analice y mitigue los ataques al mismo tiempo que los evite, puede ofrecer una protección de seguridad de nivel empresarial.

Figura 39. En 2015 fue mayor el número de PYMES que subcontrató servicios de seguridad

Por lo que respecta a la seguridad, ¿cuáles de los siguientes tipos de servicios se obtienen total o parcialmente de terceros?

Tamaño de la empresa	250-499	500-999	1 000-9 999	10 000+
Asesoría y consultoría	46%	51%	54%	55%
Monitorización	45%	46%	42%	44%
Auditoría	42%	46%	46%	56%
Respuesta ante incidentes	39%	44%	44%	40%
Inteligencia de amenazas	35%	37%	42%	41%
Remediación	33%	38%	36%	36%
Ninguna	18%	12%	11%	10%

¿Por qué su organización (PYMES 250-499) decidió subcontratar estos servicios?

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

COMPARTIR

Estudio comparativo sobre capacidades de seguridad de Cisco

Estudio comparativo sobre capacidades de seguridad de Cisco

Para medir la percepción de los profesionales de la seguridad sobre el estado de la seguridad en sus organizaciones, Cisco preguntó a los jefes de seguridad (CSO) y a los directores de operaciones de seguridad (SecOp) de varios países y en organizaciones de diversos tamaños sobre sus percepciones de los recursos y los procedimientos de seguridad. El estudio comparativo sobre capacidades de seguridad de Cisco 2015 ofrece información sobre el nivel de madurez de las operaciones y las prácticas de seguridad que se usan actualmente y también compara estos resultados con los del estudio inaugural de 2014.

Reducción de la confianza en medio de señales del estado de preparación

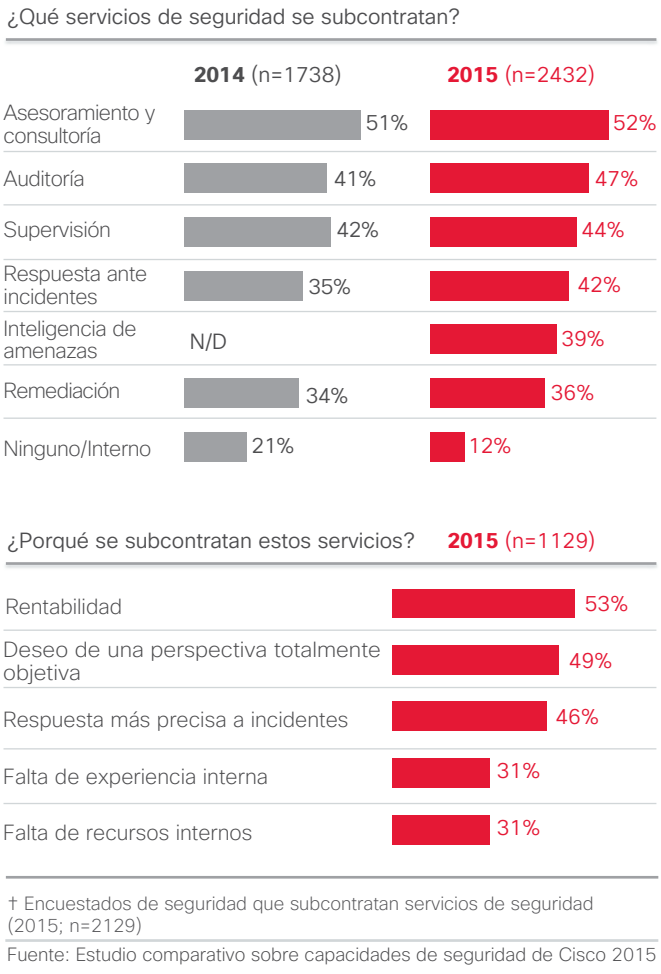
Frente a las amenazas más sofisticadas, el estudio de Cisco sugiere que la confianza de los profesionales de la seguridad parece decaer. Además, la creciente preocupación por la seguridad está cambiando la forma en que estos profesionales protegen las redes. Por ejemplo, se ve más formación en seguridad, un aumento de las políticas formales y redactadas, y más subcontratación de tareas como auditorías de seguridad, asesoramiento y respuesta a incidentes. En resumen, los profesionales de la seguridad muestran señales de que están dando pasos para combatir las amenazas que surgen en sus redes.

Los movimientos hacia la formación y la subcontratación son positivos, pero el sector de la seguridad no se puede permitir detenerse ahí. Debe seguir aumentando el uso de herramientas y procesos para mejorar la detección, la contención y la solución de problemas de amenazas. Dadas las barreras que suponen las restricciones de presupuesto y la compatibilidad de las soluciones, el sector también debe analizar soluciones eficaces que proporcionen una defensa integrada frente a las amenazas. El sector también debe hacer un mejor trabajo de colaboración con otras organizaciones cuando se producen brechas públicas (por ejemplo, con la botnet SSHPsychos; consulte la **página 14**) ya que el uso compartido de conocimientos puede ayudar a evitar futuros ataques.

RECURSOS: ORGANIZACIONES MÁS PROPENSAS A SUBCONTRATAR

Aunque los profesionales de la seguridad están más atentos a las amenazas, pueden buscar formas de mejorar su defensa; por ejemplo, subcontratar tareas de seguridad que se pueden gestionar de manera más eficaz mediante consultores o proveedores. En 2015, el 47 por ciento de las empresas encuestadas subcontrató auditorías de seguridad; un aumento del 41 por ciento respecto a 2014. También en 2015, el 42 por ciento subcontrató procesos de respuesta ante incidentes, en comparación con el 35 por ciento en 2014 (figura 40).

Figura 40. Descripción general de servicios subcontratados



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

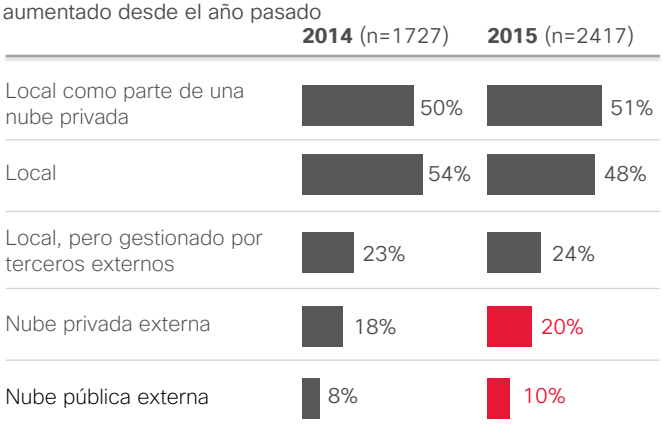
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Además, hay más profesionales de la seguridad que subcontratan algunas funciones de seguridad. En 2014, el 21 por ciento de los encuestados afirmó que no subcontrató ningún servicio de seguridad. En 2015, el número cayó significativamente al 12 por ciento. El cincuenta tres por ciento afirmó que subcontrató servicios porque hacerlo era más rentable, mientras que el 49 por ciento indicó que subcontrató servicios para obtener información de un tercero que fuese imparcial.

Para aportar protección a las redes y a los datos, los profesionales de la seguridad indicaron que son receptivos al concepto de alojar redes fuera de sus instalaciones. Aunque el alojamiento local es la opción destacada, ha aumentado el número de profesionales que utilizan soluciones externas. En 2015, un 20 por ciento utilizó soluciones privadas en la nube fuera de las instalaciones en comparación con el 18 por ciento en 2014 (figura 41).

Figura 41. Alojamiento fuera de las instalaciones

El alojamiento local de las redes de la organización sigue siendo el más habitual; sin embargo, el alojamiento fuera de ellas ha aumentado desde el año pasado



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 42. Las restricciones de presupuesto es la principal barrera para las actualizaciones de seguridad

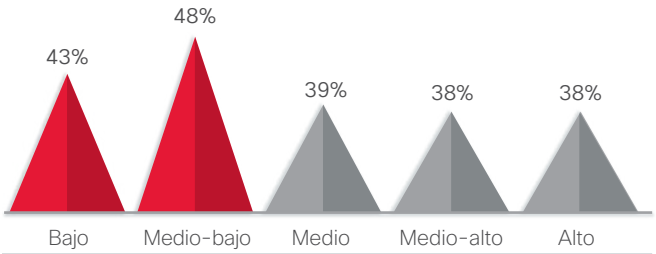
Las principales barreras para adoptar seguridad avanzada		Procesos y tecnología	**2015** (n=2432)
Restricciones de presupuesto $	39%	Falta de conocimientos	23%
Problemas de compatibilidad	32%	Cultura/actitud de la organización	23%
Requisitos de certificación	25%	Falta de personal formado	22%
Prioridades en competencia	24%	Reacio a comprar hasta que no se prueba	22%
Carga de trabajo actual demasiado grande	24%	Compra cuando así lo ordena el equipo de dirección	20%

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Los equipos de seguridad entrevistados por Cisco están más interesados en proteger sus redes de manera más efectiva, pero pueden estar limitados en su capacidad para llevar a cabo sus planes. Los profesionales de la seguridad afirmaron que las restricciones de presupuesto (el 39 por ciento) es el motivo principal en la lista de motivos probables para elegir o rechazar servicios y herramientas de seguridad, seguido de problemas de compatibilidad de la tecnología (el 32 por ciento; consulte la figura 42). Las restricciones de presupuesto se convierten en algo más que un problema para las empresas que están en el intervalo de madurez baja o media baja (consulte la figura 43). En las respuestas de todos los profesionales de la seguridad, el 39 por ciento citan las restricciones presupuestarias como un obstáculo para adoptar procesos de seguridad avanzados. Esa cifra corresponde al 43 por ciento de empresas en el intervalo de madurez baja, y un 48 por ciento en el intervalo de madurez media baja.

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

Porcentaje de encuestados que ven las restricciones de presupuesto como los mayores obstáculos (n=2432)



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Un dato que indica que algunas organizaciones piensan más en sus recursos de seguridad es cómo estructuran su presupuesto de seguridad. La encuesta muestra un ligero aumento en el número de organizaciones que separan el presupuesto de seguridad del presupuesto global de TI. En 2014, el 6 por ciento de los profesionales afirmaban que habían separado completamente los presupuestos de TI y de seguridad; en el año 2015, la cifra alcanzó el 9 por ciento (consulte la figura 44).

Figura 44. Sensible aumento en las organizaciones con presupuestos de seguridad separados

¿El presupuesto de seguridad forma parte del presupuesto de TI?
2014 (n=1720) **2015** (n=2417)

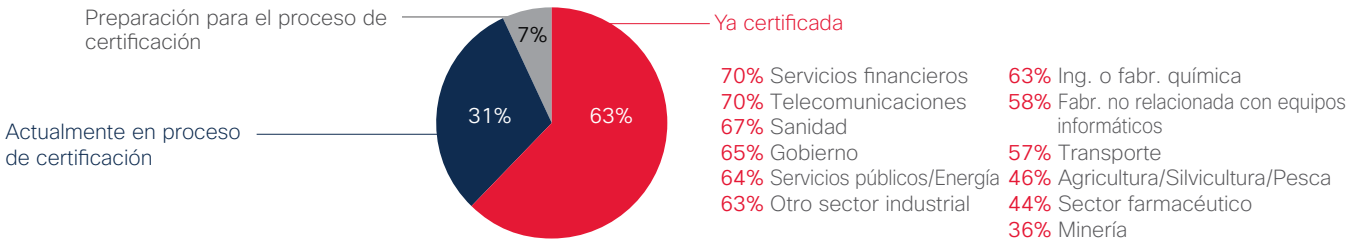
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

COMPARTIR

Cuando las organizaciones estandarizan las políticas de seguridad o buscan una certificación, muestran un compromiso con la mejora de la seguridad. Casi dos tercios de los profesionales de la seguridad afirmaron que sus organizaciones están certificadas en políticas o en prácticas de seguridad estandarizadas o que están en proceso de obtener dichas certificaciones (figura 45). Esta es una señal positiva de que las empresas ven un valor en la mejora del conocimiento de la seguridad y la respuesta a las amenazas.

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

La organización sigue prácticas y políticas de seguridad de la información estandarizadas (**2015** n=1265)



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Al examinar el uso de defensas de seguridad, observamos que los firewalls son las herramientas de seguridad más usadas en las empresas (el 65 por ciento), seguidas por las herramientas de prevención de pérdida de datos (el 56 por ciento) y de autenticación (el 53 por ciento; consulte la figura 46). En 2015, las empresas confiaron menos en las herramientas basadas en la nube. Aunque los profesionales de la seguridad han mostrado su disposición a subcontratar servicios de seguridad (consulte la **página 43**), pueden tender hacia una implementación interna de herramientas. (Consulte la **página 71** para obtener la lista completa).

Figura 46. Los firewalls y la prevención de pérdida de datos son las herramientas de seguridad más utilizadas

Defensas frente a amenazas de seguridad que emplea cada organización	**2014** (n=1738)	**2015** (n=2432)	Las defensas gestionadas por servicios basados en la nube (encuestados de seguridad que utilizan defensas frente a amenazas a la seguridad) **2014** (n=1646)	**2015** (n=2268)
Firewall*	N/D	65%		31%
Prevención de la pérdida de datos	55%	56%		
Autenticación	52%	53%		
Cifrado/Privacidad/Protección de datos	53%	53%		
Seguridad de correo electrónico y mensajería	56%	52%	37%	34%
Seguridad web	59%	51%	37%	31%
Red, seguridad, firewalls y prevención de intrusiones*	60%	N/A	35%	

*Firewall y prevención de intrusiones eran un código en 2014. " Red, seguridad, firewalls y prevención de intrusiones"

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

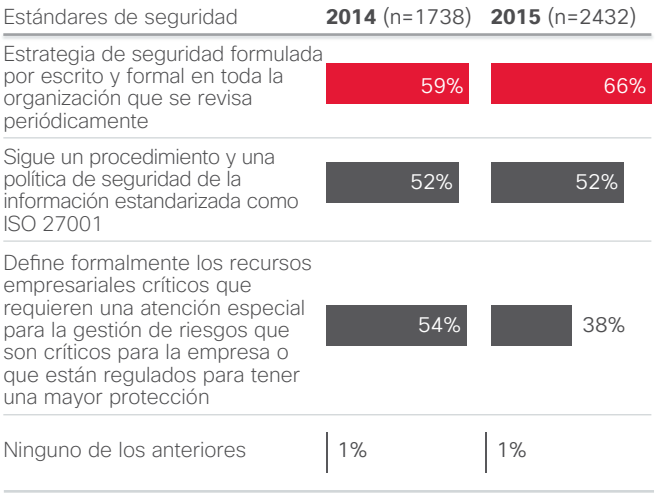
CAPACIDAD: LA CONFIANZA HA DESCENDIDO

En 2015, los profesionales de la seguridad estaban menos seguros que en 2014 de que su infraestructura de seguridad estuviera actualizada. Este descenso de confianza se debe, sin duda, al goteo constante de ataques de alto perfil en las principales empresas, al correspondiente robo de datos privados y a las disculpas públicas de las compañías cuyas redes han sido atacadas.

Sin embargo, est descenso de confianza va acompañado de un interés cada vez mayor en el desarrollo de políticas más sólidas. Como se muestra en la figura 47, hay más empresas (el 66 por ciento) que poseen una estrategia de seguridad oficial y por escrito en 2015 que en 2014 (el 59 por ciento).

Figura 47. Muchas organizaciones crean políticas de seguridad oficiales

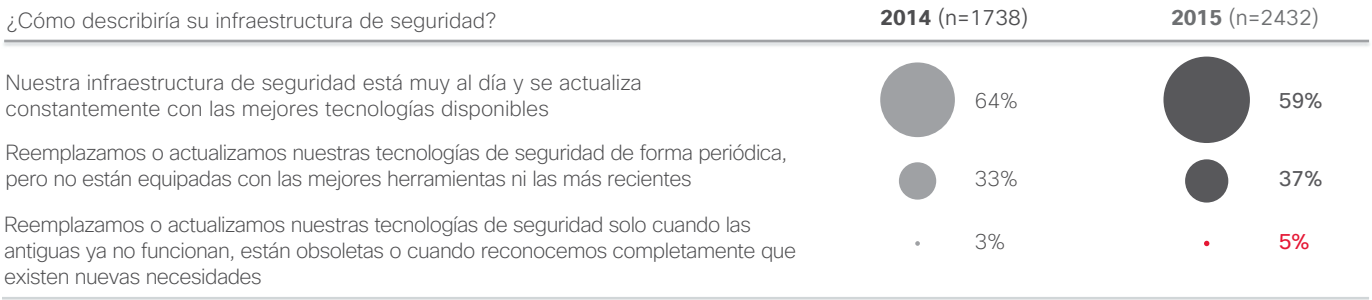
Casi dos tercios ya están certificados en una directiva de seguridad o una práctica estandarizada.



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

COMPARTIR

Figura 48. La confianza es menor en 2015

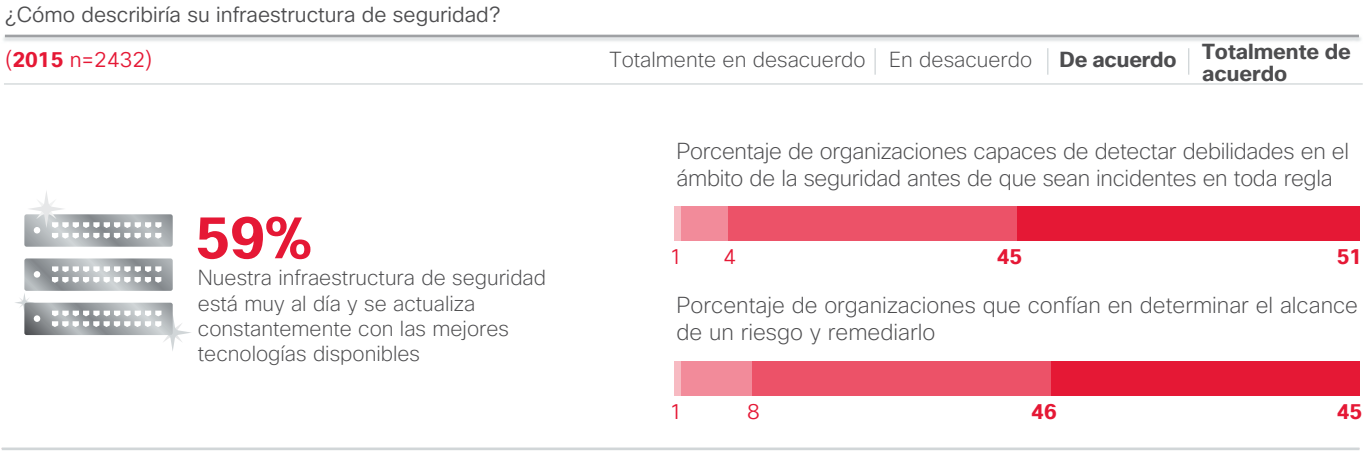


Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Como señal de que la confianza desciende, los profesionales de la seguridad muestran menos confianza en sus tecnologías. En 2014, el 64 por ciento afirmó que su infraestructura de seguridad estaba al día y en constante actualización. En 2015, el número cayó al 59 por ciento (figura 48). Además, en 2014, el 33 por ciento declaró que sus organizaciones no estaban equipadas con las herramientas de seguridad más recientes; el número subió al 37 por ciento en 2015.

La confianza es algo mayor entre los CSO, que son más optimistas que los directores de operaciones de seguridad: el 65 por ciento de CSO cree que su infraestructura de seguridad está actualizada, en comparación con el 54 por ciento de los directores de SecOp. La confianza para los directores de SecOp probablemente es inferior ya que responde a los incidentes de seguridad diarios, lo que les proporciona una visión menos positiva de su preparación para la seguridad.

Figura 49. Confianza relativa en la capacidad para detectar riesgos

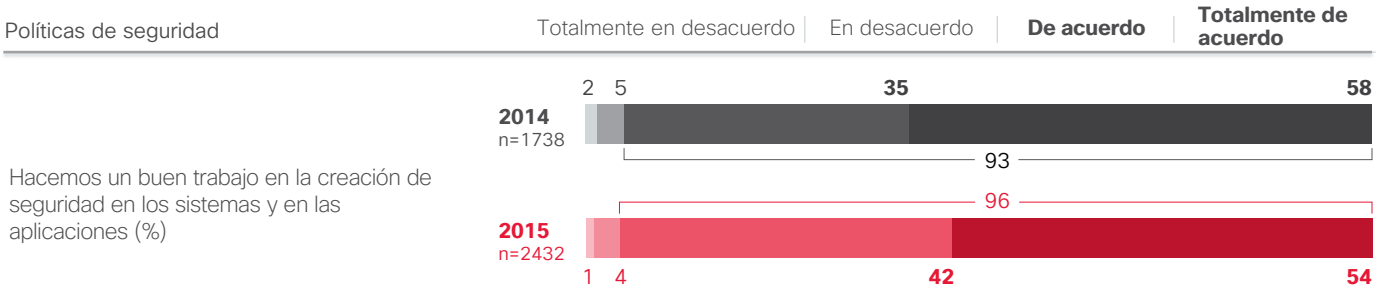


Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Los profesionales de la seguridad también muestran varios niveles de confianza en términos de capacidad para evitar a los atacantes. El cincuenta y uno por ciento cree firmemente en que pueden detectar puntos débiles en la seguridad antes de que se conviertan en incidentes reales; solo el 45 por ciento confían en su capacidad para determinar el alcance de un riesgo de red y remediar el daño (consulte la figura 49).

Los profesionales de la seguridad también muestran niveles de confianza más débiles en su capacidad para defender sus redes contra ataques. Por ejemplo, en 2015, fue menor el número de profesionales que creyeron firmemente que hacían un buen trabajo a la hora de aportar seguridad en los procedimientos para adquirir, desarrollar y mantener sistemas (el 54 por ciento en 2015, en comparación con el 58 por ciento en 2014; consulte la figura 50). (Consulte la **página 76** para obtener la lista completa).

Figura 50. Menor confianza en la capacidad de crear seguridad dentro de los sistemas



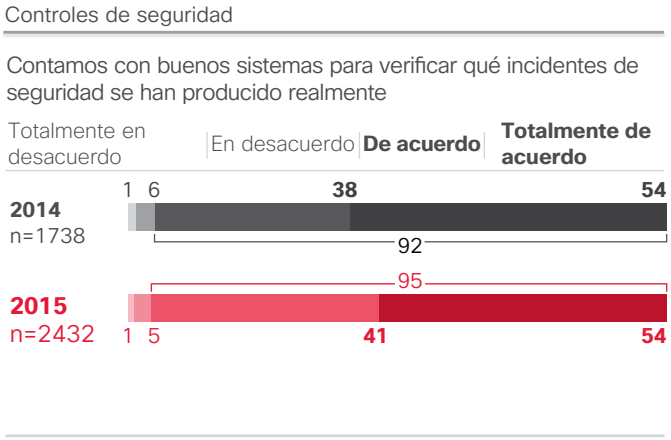
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

COMPARTIR

En algunas áreas, los niveles de confianza en las capacidades de seguridad no son muy altos. Por ejemplo, en 2015, solo el 54 de los encuestados afirmó que creía que tenían un buen sistema para verificar que los incidentes de seguridad realmente se habían producido (consulte la figura 51). (Consulte la **página 77** para obtener la lista completa).

Los encuestados tampoco confiaban totalmente en que sus sistemas pudieran alcanzar y contener dichos riesgos. El cincuenta y seis por ciento afirmó que revisaban y mejoraban las prácticas de seguridad con regularidad, oficial y estratégicamente; el 52 por ciento pensaba que las tecnologías de seguridad están bien integradas y funcionan juntas de una forma eficaz (consulte la figura 52). (Consulte la **página 79** para obtener la lista completa).

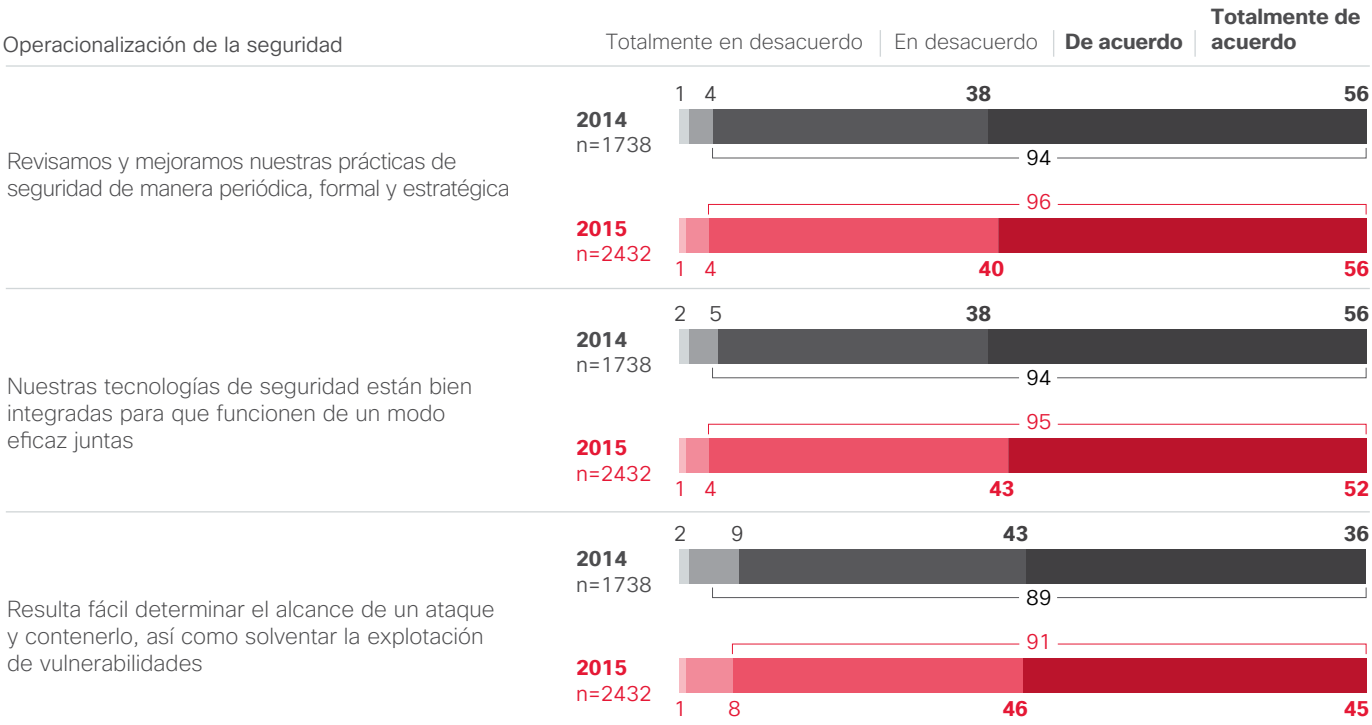
Figura 51. Las empresas consideran que cuentan con buenos controles de seguridad



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

COMPARTIR

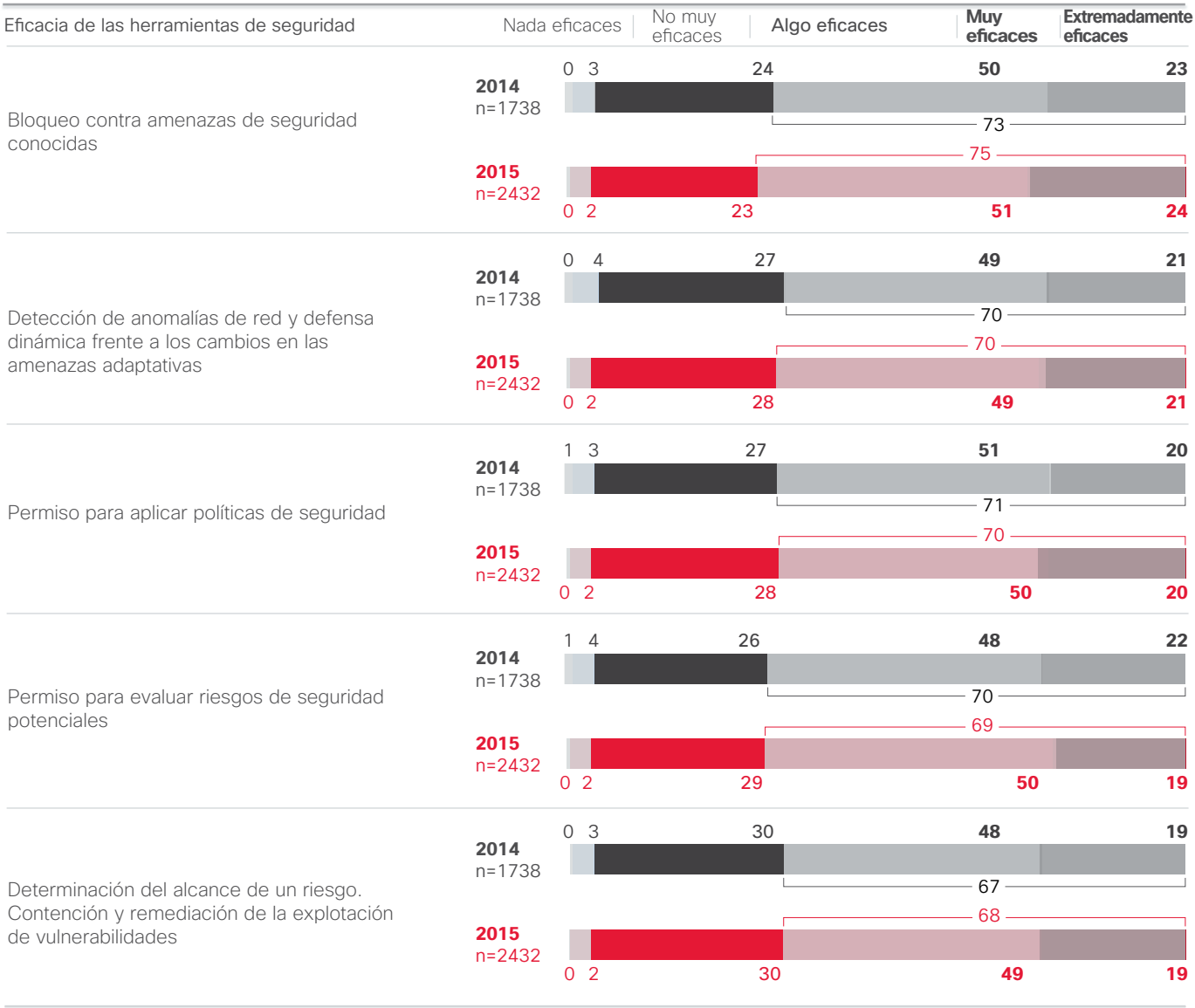
Figura 52. Las empresas expresan una confianza relativa en la capacidad para contener el riesgo



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 53. Una cuarta parte de empresas cree que las herramientas de seguridad solo son un poco eficaces

De una manera similar al año pasado, aproximadamente una cuarta parte percibían que sus herramientas de seguridad eran solo "un poco" en vez de "muy" o "extremadamente" eficaces



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

De un modo similar a los encuestados en 2014, más de una cuarta parte de los profesionales de la seguridad en 2015 afirmaron que creían que sus herramientas de seguridad solo eran un poco eficaces (figura 53).

Las brechas de seguridad públicas tienden a ser algo decisivo para las organizaciones. Cuando se producen, las organizaciones parecen ser más conscientes de la necesidad de evitar futuras brechas. Sin embargo, en 2015, menos profesionales de la seguridad afirmaron que sus organizaciones tenían que hacer frente a brechas de seguridad públicas: eran el 53 por ciento de los profesionales en 2014 y el 48 por ciento en 2015 (figura 54).

Los profesionales reconocen el valor que las brechas tienen en términos de ofrecer una llamada de atención sobre la importancia de fortalecer los procesos de seguridad: el 47 por ciento de los profesionales de la seguridad afectados por las brechas públicas afirmó que las brechas propiciaron mejores políticas y procedimientos. Por ejemplo, el 43 por ciento de los encuestados afirmó que la formación en seguridad aumentó después de una brecha pública, y el 42 por ciento dijo que aumentaron las inversiones en tecnologías de defensa y seguridad.

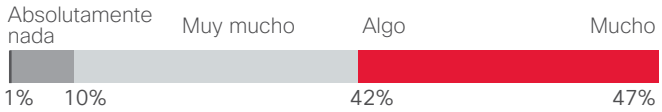
La buena noticia es que las organizaciones que han sufrido una brecha pública tienen cada vez más a fortalecer sus procesos de seguridad. En 2015, el 97 de los profesionales de la seguridad afirmó que realizaban formación en seguridad al menos una vez al año, un aumento considerable del 82 por ciento en 2014 (consulte la figura 90 en la **página 82**).

COMPARTIR

Figura 54. Los brechas públicas pueden mejorar la seguridad

¿Su organización ha tenido que enfrentarse alguna vez al escrutinio público que ocasiona un fallo en la seguridad? (n=1701) (n=1347)

¿Cuánto afectó la brecha a las mejoras en sus políticas, procedimientos o tecnologías que usa para defenderse frente a amenazas de seguridad? (n=1134)



Fuente: estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 55. Cada vez más organizaciones realizan formación en seguridad

En 2015, el 43% de los encuestados afirmó que había aumentado la formación tras una brecha en la seguridad.

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

MADUREZ: LAS ESTRICCIONES DE PRESUPUESTO PESAN MUCHO EN TODOS LOS NIVELES

A medida que las organizaciones implementan políticas y prácticas de seguridad más sofisticadas, las percepciones sobre su preparación para la seguridad puede cambiar. El estudio comparativo sobre capacidades de seguridad de Cisco 2015 sitúa a los encuestados y a sus organizaciones en cinco categorías de madurez, en función de sus respuestas sobre sus procesos de seguridad (figura 56). El estudio examina la forma en que diferentes características como las capacidades, los sectores industriales y los países pueden afectar a los niveles de madurez.

Curiosamente, organizaciones con diferentes niveles de madurez parecen compartir algunos de los obstáculos para la implementación de procesos y herramientas de seguridad más sofisticados. Aunque los porcentajes pueden variar, el reto de las restricciones de presupuesto se encuentra en la parte superior de la lista en todos los niveles de madurez (figura 57).

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

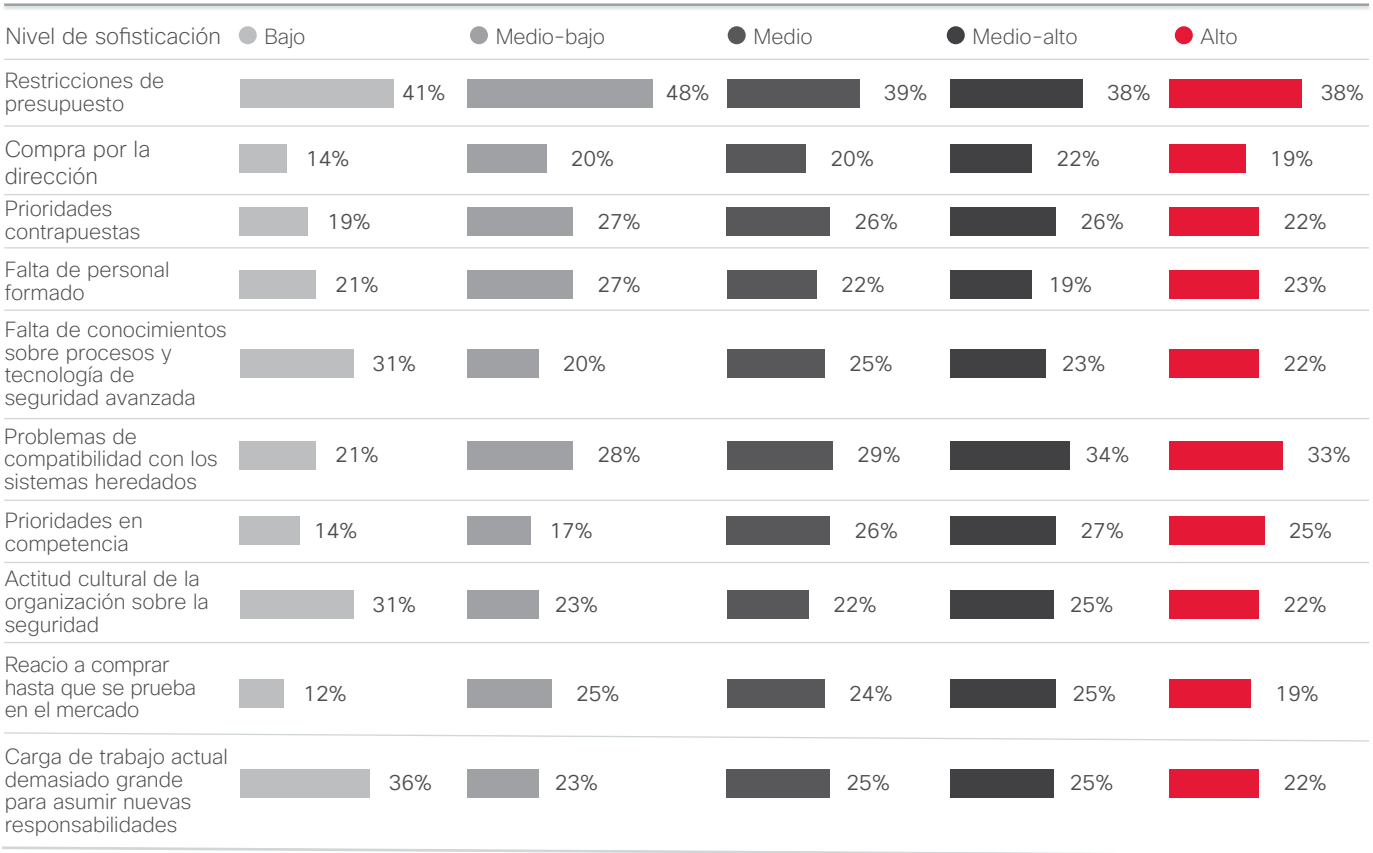
Cisco barajó varias opciones para segmentar la muestra antes de seleccionar una solución de cinco segmentos basada en una serie de preguntas relativas a los procesos de seguridad. La solución de cinco segmentos se corresponde muy estrechamente con el modelo de integración de modelos de madurez de capacidades (CMMI).

	Nivel	Solución basada en 5 segmentos	
Optimización	1	El objetivo principal es la mejora de los procesos	Alto
Gestionado cuantitativamente	2	Procesos medidos y controlados cuantitativamente	Medio-alto
Definido	3	Procesos caracterizados para organizaciones frecuentemente proactivas	Medio
Repetible	4	Procesos caracterizados para proyectos: a menudo reactivos	Medio-bajo
Initial	5	Los procesos son ad hoc e impredecibles	Bajo

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

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

¿Cuáles de los siguientes considera que son los mayores obstáculos para la adopción de procesos y tecnologías de seguridad avanzada?

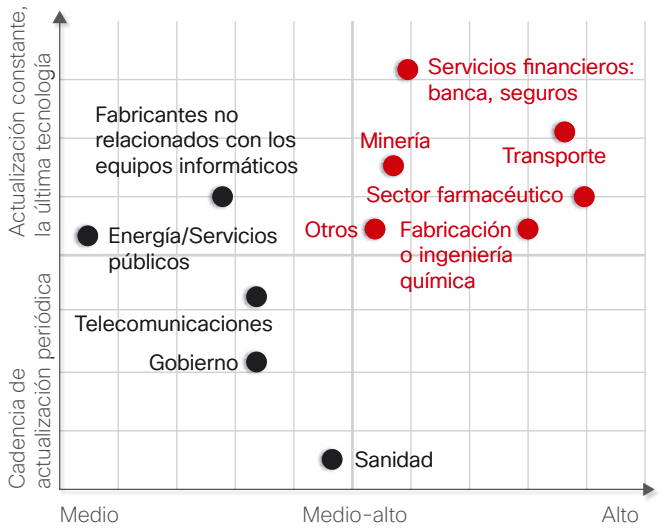


Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

El gráfico de la derecha asigna la calidad de los niveles de madurez e infraestructura de seguridad de diversos sectores industriales. Se basa en la percepción de los encuestados de sus procesos de seguridad. Los sectores industriales que aparecen en el cuadrante superior derecho muestran los niveles más altos de madurez así como de calidad de la infraestructura.

El gráfico siguiente muestra la ubicación de los niveles de madurez de Cisco por sector industrial. En 2015, casi la mitad de las organizaciones farmacéuticas y transportistas encuestados estaban en el segmento de mayor madurez. Las organizaciones de telecomunicaciones y energéticas es menos probable encontrarlas en el segmento de mayor madurez en 2015, en comparación con 2014. Los resultados se basan en la percepción que tienen los encuestados sobre sus procesos de seguridad.

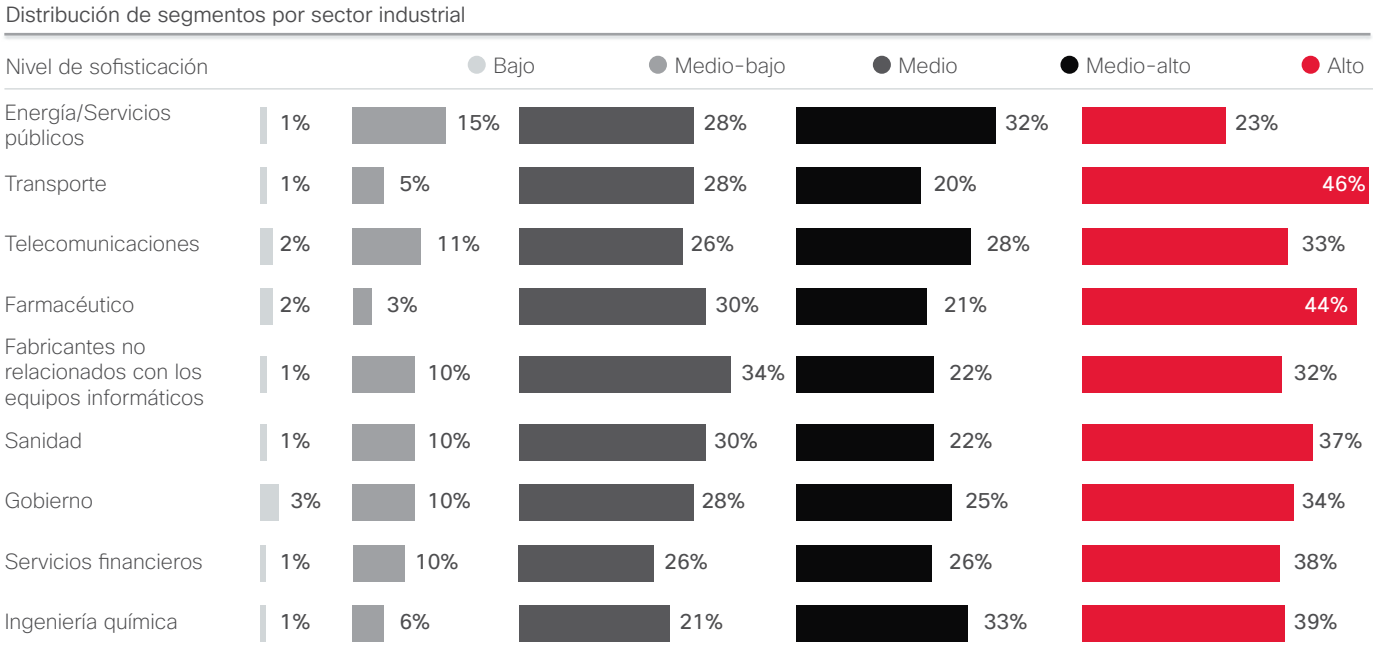
Figura 58. Medición de madurez de seguridad por infraestructura y sector industrial



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

COMPARTIR

Figura 59. Niveles de madurez por sector industrial



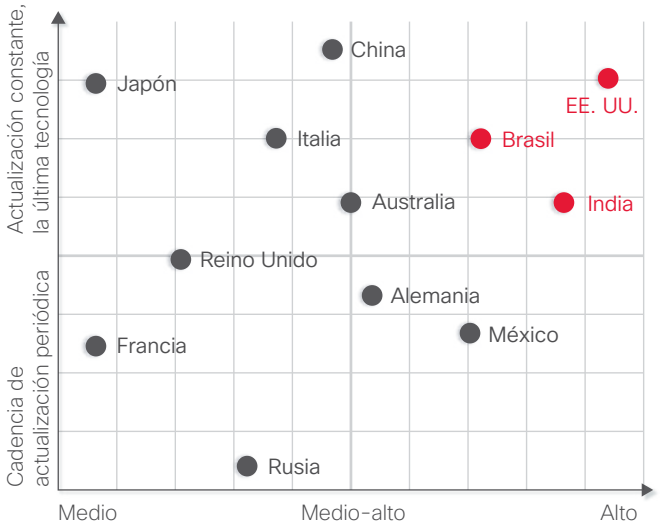
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

El gráfico de la derecha asigna la calidad de los niveles de madurez e infraestructura de seguridad de diversos países. Los países que aparecen en el cuadrante superior derecho muestran los niveles más altos de madurez así como de calidad de infraestructura. Es importante señalar que estos resultados se basan en la percepción de los profesionales de la seguridad de su preparación para la seguridad.

El gráfico siguiente muestra la ubicación de los niveles de madurez de Cisco por país. Los resultados se basan en la percepción que tienen los encuestados sobre sus procesos de seguridad.

COMPARTIR

Figura 60. Medición de madurez de seguridad por infraestructura y país



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

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 de Cisco 2015

RECOMENDACIONES: RESPUESTA A UNA COMPROBACIÓN DE LA REALIDAD

Como muestra nuestro Estudio comparativo sobre capacidades de seguridad, la realidad se ha establecido en los profesionales de la seguridad. La confianza de los profesionales de la seguridad en su preparación para bloquear a atacantes está en entredicho. Sin embargo, las comprobaciones con la realidad proporcionadas por las vulnerabilidades de altos perfiles han tenido efectos positivos en el sector industrial, a juzgar por el aumento en la formación de seguridad y en el desarrollo de políticas oficiales. Además, la cada vez más frecuente subcontratación de servicios de respuesta ante incidentes y auditorías indica que los responsables de seguridad buscan la ayuda de expertos.

Las empresas deben seguir preocupándose por su preparación ante la seguridad, y los profesionales de la seguridad deben defender el aumento de los presupuestos para poder así contar con una mejor tecnología y un mejor personal. Además, la confianza aumentará cuando los profesionales de la seguridad implementen herramientas que no solo puedan detectar amenazas, sino que también contengan su impacto y aporten más formas de evitar futuros ataques.

Una mirada al futuro

Una mirada al futuro

Los expertos en geopolítica de Cisco ofrecen sus perspectivas sobre el cambiante panorama de la gobernanza de Internet, incluidos los cambios en la legislación sobre transferencia de datos y el debate acerca del uso del cifrado. Esta sección incluye también algunas conclusiones de dos estudios de Cisco. Uno examina la preocupación de los ejecutivos acerca de la ciberseguridad. El otro se centra en la percepción de los responsables de la toma de decisiones de TI en cuanto al riesgo para la seguridad y la fiabilidad. También se proporciona una descripción general del valor de una arquitectura de defensa integrada contra amenazas y se informa de los avances de Cisco en la reducción del tiempo de detección (TTD).

Perspectiva geopolítica: incertidumbre sobre el panorama de la gobernanza de Internet

En la era posterior a Edward Snowden, el panorama geopolítico de la gobernanza de Internet ha cambiado de forma drástica. El flujo de información libre a través de las fronteras está rodeado de una gran incertidumbre. El mayor impacto fue probablemente el caso emblemático del activista austriaco en favor de la privacidad Max Schrems contra el gigante Facebook, que llevó al Tribunal de Justicia de la Unión Europea (TJEU) a revocar el 6 de octubre de 2015 el acuerdo de Puerto seguro con EE. UU.[7]

Como consecuencia, ahora las empresas se ven obligadas a emplear otros mecanismos y medidas de protección legales distintas de las de Puerto seguro para la transferencia de datos de la Unión Europea a los Estados Unidos, que, además, ahora están siendo objeto de una investigación. Las empresas de datos aún están valorando las consecuencias de esta decisión y, aunque las autoridades de ambas partes llevan dos años trabajando en un acuerdo que sustituya al revocado, existe preocupación acerca de este nuevo y esperado mecanismo. Dicho acuerdo podría no materializarse en la fecha prevista, enero de 2016, o, lo que es más probable, podría no restaurar la confianza de los mercados si no responde completamente a las preocupaciones del TJEU, por lo que sería susceptible de una nueva anulación.[8]

Los expertos en protección de datos auguran que el acuerdo Puerto seguro 2.0 será, como mínimo, tan polémico como su predecesor. Podría incluso seguir el mismo camino y terminar siendo declarado no válido en los tribunales.[9]

El cifrado de extremo a extremo (cómo beneficia a los consumidores y organizaciones, y los retos que plantea para los organismos de seguridad en la investigación de actividades criminales y terroristas) será otro importante tema de debate entre gobiernos e industria en los años venideros. Tras los atentados de París en noviembre de 2015, algunos legisladores han redoblado su presión para permitir a los investigadores acceder al contenido de las comunicaciones cifradas.[10] Esto podría acelerar el desarrollo del Puerto seguro 2.0, ya que la preocupación por la seguridad se impone a la defensa de los derechos civiles.

---

[7] "El Tribunal de Justicia declara no válida la decisión de la comisión que declaró que Estados Unidos garantiza un nivel de protección adecuado de los datos personales transferidos", TJUE, 6 de octubre de 2015: **http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf.**

[8] "Safe Harbor 2.0 framework begins to capsize as January deadline nears", 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", 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", 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 este escenario incierto, ¿qué deberían pedir las organizaciones a los proveedores de datos para asegurarse de que sus negocios cumplen la normativa de transferencia de datos? A corto plazo, deberían solicitarles una garantía de que en las transferencias de datos desde la Unión Europea emplean modelos de cláusulas contractuales aplicables en la Unión Europea o normativa corporativa vinculante, y no solo el acuerdo de Puerto seguro.

Otro importante problema geopolítico al que las organizaciones deben prestar atención es el de las vulnerabilidades. Algunos gobiernos han expresado gran preocupación por el auge del mercado de vulnerabilidades sin parche, las llamadas "software armado". Estas herramientas son esenciales para la comunidad de estudio de la seguridad, que busca maneras de proteger las redes de todo el mundo. Sin embargo, en malas manos, especialmente las de regímenes represivos, esta tecnología pensada para el bien podría emplearse para cometer delitos financieros, robar secretos nacionales o comerciales, reprimir la disensión política o incapacitar una infraestructura esencial.

Cómo limitar el acceso a las vulnerabilidades sin parche sin atar las manos de quienes desarrollan una investigación vital será uno de los quebraderos de cabeza de los gobiernos en los próximos meses y años. Al afrontar este espinoso asunto, los legisladores deberán valorar cuidadosamente el efecto que sus decisiones tendrán sobre la seguridad. Por ejemplo, la incertidumbre respecto a la legislación relativa a la transmisión de información sobre vulnerabilidades no publicadas podría detener el avance del estudio de amenazas o fomentar la publicación de vulnerabilidades antes de que los proveedores tengan ocasión de ofrecer un parche. Cualquier estrategia de resolución de dicha incertidumbre debería ser aplicable en todo el mundo.

La preocupación de los ejecutivos por la ciberseguridad

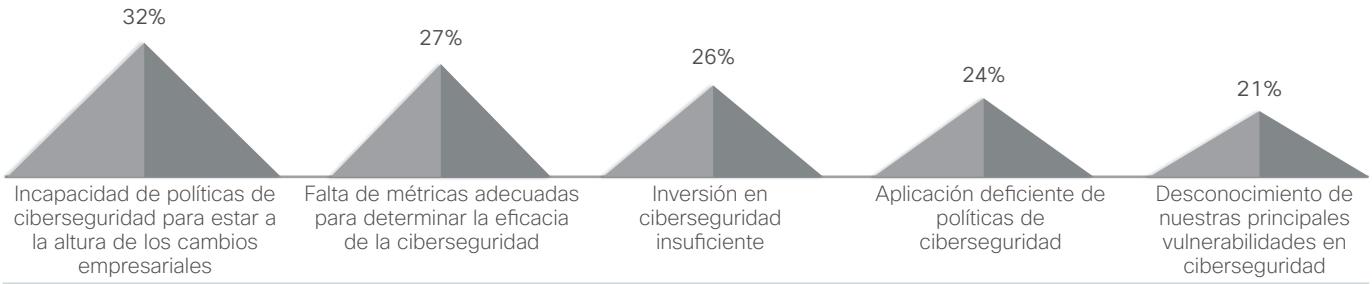
Obviamente, una seguridad exhaustiva puede ayudar a las empresas a evitar ataques y brechas calamitosas de la seguridad. Sin embargo, ¿mejora la probabilidad de una empresa de alcanzar el éxito? Según un estudio de octubre de 2015 realizado por Cisco con ejecutivos de finanzas y líneas de negocio respecto al papel de la ciberseguridad en la estrategia empresarial y digital, los ejecutivos comprenden que el éxito o el fracaso pueden depender de la protección del negocio frente a estas amenazas. A medida que las organizaciones se digitalizan, su crecimiento depende de la capacidad para proteger la plataforma digital.

Como muestra la encuesta, la ciberseguridad es una preocupación cada vez mayor para los ejecutivos: el 48% dice sentirse muy preocupado y el 39% moderadamente preocupado por las brechas en la ciberseguridad. Esta preocupación va en aumento: el 41 % dice sentirse mucho más preocupado por esta cuestión que hace tres años, mientras que el porcentaje de ejecutivos un poco más preocupados es del 42 %.

Los líderes empresariales también creen que los inversores y reguladores realizarán preguntas cada vez más complejas acerca de los procesos de seguridad, como ya hacen acerca de otras funciones empresariales. El 92% de los participantes coincide en que los reguladores e inversores querrán que, en el futuro, las empresas proporcionen más información sobre exposición y ciberriesgo.

Las empresas también parecen tener una idea muy clara de los retos que afrontan a este respecto. La incapacidad de las políticas de ciberseguridad para mantenerse al día de los cambios empresariales fue el más citado, seguido por la falta de métricas con las que determinar la eficacia de la seguridad (figura 62).

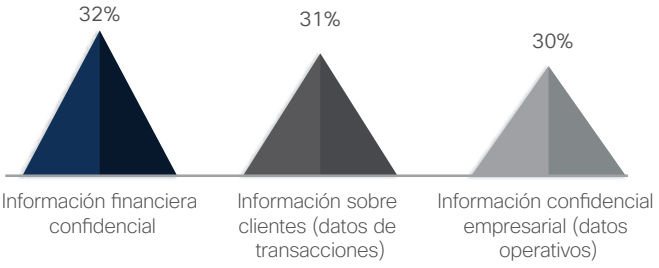
Figura 62. Las empresas se enfrentan a unos retos complejos en el ámbito de la ciberseguridad



Fuente: Investigación de seguridad de Cisco

A un tercio aproximadamente de los ejecutivos también les preocupa su capacidad para salvaguardar datos críticos. Cuando se les pide que nombren los tipos de información más difíciles de proteger, el 32% elige "Información financiera confidencial". Los encuestados indican "Información del cliente" e "Información empresarial confidencial" como los dos tipos de datos más difíciles de proteger (consulte la figura 63).

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



Fuente: Investigación de seguridad de Cisco

Estudio de fiabilidad: algo de luz acerca de los riesgos y retos para las empresas

El aumento constante de las brechas de seguridad de la información subraya la profunda necesidad que las empresas tienen de que sus sistemas, datos, socios comerciales, clientes y empleados estén seguros. Se ve claramente cómo la confianza se convierte en un factor cada vez más importante a la hora de decantarse por una infraestructura de TI y networking. De hecho, son muchos los que exigen ya que la seguridad y la fiabilidad estén integradas en el ciclo de vida completo de los productos de su infraestructura.

En octubre de 2015, Cisco realizó un estudio con el fin de valorar la percepción que los responsables de la toma de decisiones de TI tienen de los riesgos y retos para la seguridad, y para determinar qué papel juega en sus inversiones de TI la confianza en un proveedor. Participaron responsables de la toma de decisiones sobre seguridad de la información y seguridad de diversos países. (Consulte el **Apéndice** para obtener más información acerca del Estudio sobre riesgos de seguridad y fiabilidad, incluida nuestra metodología).

A CONTINUACIÓN SE EXPONEN ALGUNAS DE LAS CONCLUSIONES DEL ESTUDIO:

Se observó que el 65% de los encuestados cree que su organización afronta un riesgo para la seguridad significativo, en concreto por el uso de soluciones basadas en la nube y soluciones de movilidad y seguridad de TI (figura 64).

Figura 64. Percepción del riesgo para la seguridad

Fuente: Estudio sobre riesgos de seguridad y fiabilidad, Cisco

COMPARTIR

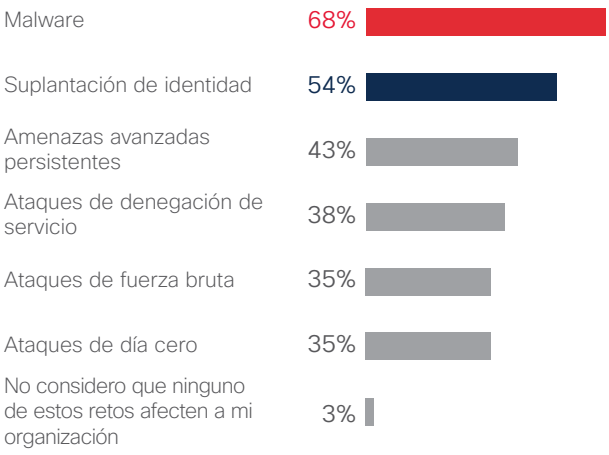
El 68 % de los participantes en el estudio identificó el malware como el principal reto externo de seguridad para sus organizaciones. Le acompañaron la suplantación de identidad y las amenazas persistentes avanzadas, con el 54% y el 43% respectivamente (consulte la figura 65).

En cuanto a los retos de seguridad internos (consulte la figura 66), más de la mitad de los encuestados (54%) citó las descargas de software malicioso como principal amenaza, seguida por las brechas de seguridad internas por parte de los empleados (47%) y las vulnerabilidades de hardware y software (46 %).

También se comprobó que la mayoría de las empresas (92%) emplea un equipo de seguridad dedicado dentro de la organización. El 88% de los participantes indicó que sus organizaciones disponen de una estrategia global de seguridad que se renueva con regularidad. Sin embargo, solo el 59% dispone de políticas y procedimientos estandarizados para validar la fiabilidad de los proveedores de TI (consulte la figura 67).

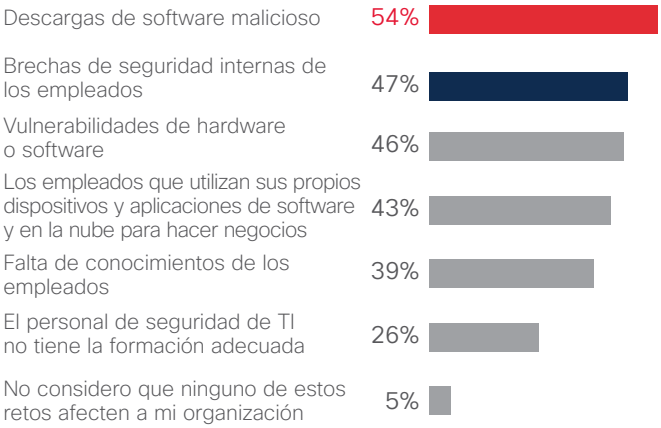
Además, aproximadamente la mitad de las grandes empresas (49%) mantiene su seguridad actualizada con las tecnologías más actuales, y la mayoría mejora la infraestructura con regularidad. Según el estudio, muy pocos esperan a que una tecnología quede obsoleta para actualizarla.

Figura 65. Retos externos (total de encuestados)



Fuente: Estudio sobre riesgos de seguridad y fiabilidad, Cisco

Figura 66. Retos de seguridad internos (total de encuestados)



Fuente: Estudio sobre riesgos de seguridad y fiabilidad, Cisco

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

Fuente: Estudio sobre riesgos de seguridad y fiabilidad, Cisco

COMPARTIR

Cómo pueden demostrar fiabilidad los proveedores

En el entorno actual centrado en las amenazas, la confianza en los procesos, políticas, tecnologías y personal de un proveedor, así como la capacidad para comprobarlos, son fundamentales a la hora de crear una relación duradera y de confianza entre proveedores y empresas.

Los proveedores de tecnología demuestran fiabilidad:

- Integrando la seguridad en sus soluciones y su cadena de valor desde la misma concepción
- Implementando y cumpliendo políticas y procesos que reducen los riesgos
- Creando una cultura de concienciación de seguridad
- Respondiendo a las brechas de seguridad de forma rápida y transparente
- Ofreciendo remediación rápida y vigilancia constante tras un incidente

Sin duda, actualizar la infraestructura es una práctica recomendable. Las organizaciones de todos los tamaños deben implementar una infraestructura fiable en la que la seguridad esté integrada en todas las facetas. Sin embargo, también pueden reducir su vulnerabilidad fomentando una cultura abierta en la que exista sensibilización por la seguridad.

Esto requiere la implementación de políticas y procesos globales y coherentes que garanticen que la seguridad queda integrada en todos los aspectos de la empresa. A continuación, deben esforzarse por extender esta mentalidad de seguridad a sus partners y proveedores, y demostrar constantemente transparencia y capacidad para asumir responsabilidades ante los clientes, partners y otras partes interesadas.

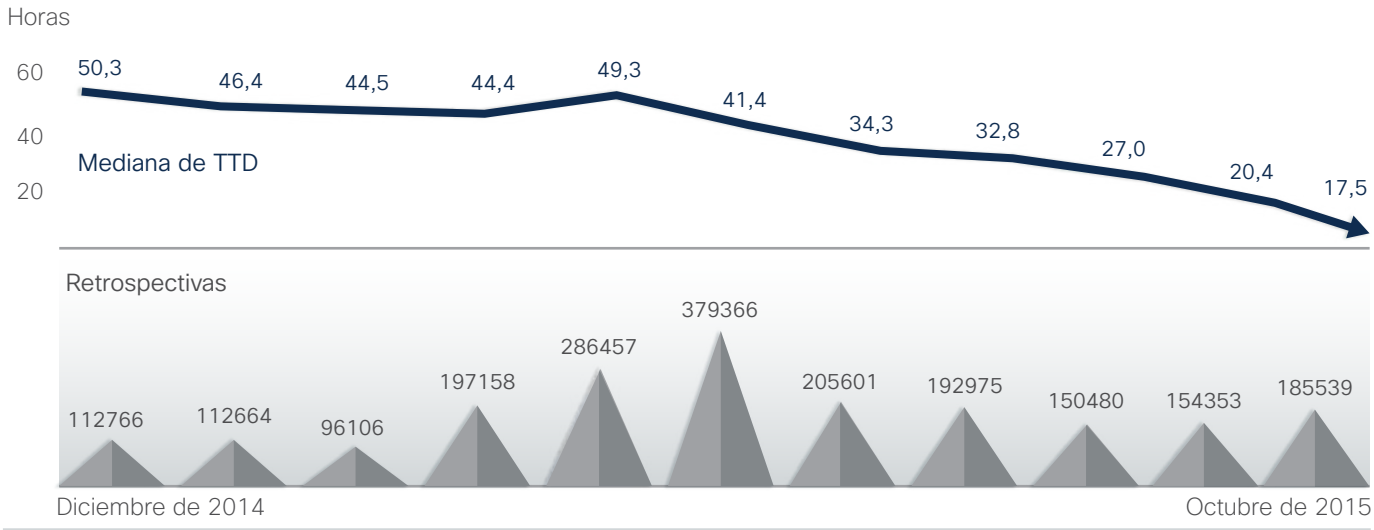
Tiempo de detección: la carrera por reducir los plazos

"Tiempo de detección" se define como el intervalo transcurrido entre la primera observación de un archivo desconocido y la detección de una amenaza. Este intervalo de tiempo se calcula usando telemetría de seguridad opcional recopilada a partir de los productos de seguridad de Cisco implementados en todo el mundo.

La categoría "Retrospectivas" de la figura 68 muestra el número de archivos que Cisco clasificó inicialmente como "desconocidos" y más tarde convirtió en "amenazas conocidas".

Tal y como se indicó en el Informe de seguridad semestral de Cisco 2015, el TTD medio fue de dos días aproximadamente (50 horas).

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



Fuente: Investigación de seguridad de Cisco

De enero a marzo, el TTD no sufrió muchas variaciones y fue de entre 44 y 46 horas, aunque con una leve tendencia descendente. En abril, este valor subió levemente hasta 49 horas. Sin embargo, a finales de mayo, el valor de TTD para Cisco disminuyó hasta 41 horas.

Desde entonces, el TTD medio ha descendido rápidamente. En octubre, Cisco había reducido el TTD medio a 17 horas, menos de un día. Esta cifra mejora muchísimo la estimación actual del TTD del sector (entre 100 y 200 días). Esta velocidad se debe a la inclusión de información más detallada acerca de la mitigación de infecciones breves.

La industrialización de la piratería informática y el mayor uso de malware de consumo han tenido un importante papel en nuestra capacidad para reducir el plazo del TTD. Tan pronto como una amenaza se industrializa, se extiende y se hace más fácil de detectar.

Sin embargo, también sugerimos que la combinación de defensas sofisticadas y la estrecha colaboración entre investigadores de seguridad expertos puede haber sido aún más decisiva en nuestra capacidad para reducir de forma constante y significativa el TTD medio a lo largo de 2015.

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

Fuente: Investigación de seguridad de Cisco

COMPARTIR

La comparación de TTD en la figura 69 muestra que, en junio, muchas amenazas fueron detectadas en una media de 35,3 horas. En septiembre, las amenazas se detenían en unas 17,5 horas. Como se ha dicho, parte de la reducción del TTD medio se atribuye a una identificación más rápida del malware de consumo, como Cryptowall 3,0, Upatre y Dyre. Otro factor es la integración de nuevas tecnologías, como las de ThreatGRID, una empresa de Cisco.

No obstante, pese a la reducción del TTD, algunas amenazas siguen siendo más difíciles de detectar que otras. Las aplicaciones de descarga que atacan a los usuarios de Microsoft Word suelen ser las más fáciles de detectar (menos de 20 horas). Entre las amenazas más escurridizas están el adware y las inyecciones en el navegador (menos de 200 horas).

Un motivo por el que estas amenazas son difíciles de detectar es que los equipos de seguridad suelen asignarles una prioridad menor, de modo que a menudo se las pasa por alto en la carrera por rechazar los feroces ataques de día cero (consulte "Infecciones del navegador: una importante y extendida causa de filtración de datos" en la **página 16**).

La figura 70 muestra los tipos de amenazas que suelen aparecer en un plazo de 100 días.

Figura 70. Nube de etiquetas durante 100 días

Fuente: Investigación de seguridad de Cisco

Los seis aspectos de defensa integrada contra amenazas

En el Informe de seguridad semestral de Cisco 2015, los expertos en seguridad afirmaron que la necesidad de soluciones flexibles e integradas provocará cambios importantes en el sector de la seguridad en los próximos cinco años. Los resultados serán la consolidación del sector y un movimiento unificado hacia una arquitectura escalable de defensa integrada contra amenazas. Esta arquitectura proporcionará visibilidad, control, inteligencia y contexto para numerosas soluciones.

Este marco de "detección y respuesta" permitirá actuar más rápidamente ante amenazas conocidas y emergentes. En el centro de esta nueva arquitectura habrá una plataforma de visibilidad con identificación del entorno que se actualice constantemente para valorar amenazas, relacionar la información local y global, y optimizar las defensas. La intención de esta plataforma es crear una base en la que todos los proveedores puedan operar y a la que todos puedan contribuir. La visibilidad se traduce en un mayor control, y este en una mejor protección ante más vectores de amenazas, y en la capacidad para frustrar más ataques.

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

1. **Es necesaria una arquitectura de red y seguridad con más posibilidades para abordar el volumen y la cada vez mayor sofisticación de los responsables de las amenazas.**

   Durante los últimos 25 años, el modelo tradicional de seguridad ha sido "si ves un problema, compra un aparato". Sin embargo, estas soluciones, que a menudo son una colección de tecnologías procedentes de diversos proveedores de seguridad, no se comunican entre ellas de un modo significativo. Producen información acerca de eventos de seguridad, que se integran en una plataforma de eventos para su posterior análisis por parte del personal de seguridad.

   Una arquitectura de defensa integrada contra amenazas es un marco de detección y respuesta que ofrece más capacidades y permite una respuesta más rápida ante amenazas por medio de la obtención automatizada y eficaz de información sobre la infraestructura implementada. Este marco observa el entorno de seguridad con mayor inteligencia. En lugar de limitarse a alertar a los equipos de seguridad de eventos sospechosos y violaciones de la política, puede proporcionar una imagen clara de la red y de lo que sucede en ella, para así tomar mejores decisiones de seguridad.

2. **La tecnología más avanzada no puede por sí sola afrontar el panorama actual (o futuro) de amenazas; simplemente aumenta la complejidad del entorno de red.**

   Las organizaciones invierten en las mejores tecnologías de seguridad, pero ¿cómo saben si estas soluciones funcionan realmente? Las noticias del año pasado acerca de grandes brechas de seguridad son una prueba de que muchas de estas tecnologías no funcionan bien. Y cuando fallan, lo hacen estrepitosamente.

   La proliferación de proveedores de seguridad que dicen ofrecer la mejor solución posible no ayuda a mejorar el entorno de seguridad, salvo que proporcionen soluciones radicalmente (no solo un poco) diferentes a las de la competencia. Sin embargo, hoy en día no existen grandes diferencias en las principales áreas de seguridad de los principales proveedores.

3. **El aumento del tráfico cifrado requiere una defensa integrada contra amenazas que pueda actuar contra actividades maliciosas cifradas que hacen ineficaces determinados productos.**

   Como se indica en este informe, el tráfico web cifrado está creciendo. Sin duda, existen buenas razones para emplear el cifrado, pero al mismo tiempo esto dificulta a los equipos de seguridad realizar un seguimiento de las amenazas.

   La respuesta al "problema" del cifrado es tener una mayor visibilidad de lo que sucede en dispositivos y redes. Las plataformas de seguridad integradas pueden ayudar en este aspecto.

4. **Las API abiertas son fundamentales en una arquitectura de defensa integrada contra amenazas.**

   Los entornos de varios proveedores necesitan una plataforma común que proporcione mayor visibilidad, contexto y control. La creación de una plataforma frontal de integración puede propiciar una mejor automatización y aumentar el conocimiento de los propios productos de seguridad.

5. **Una arquitectura integrada de defensa contra amenazas requiere menos dispositivos y software que no hay que instalar y administrar.**

   Los proveedores de seguridad deberían tratar de proporcionar plataformas con el mayor número de características y que ofrezcan una amplia funcionalidad en una plataforma. Esto ayudará a reducir la complejidad y la fragmentación del entorno de seguridad, lo que ofrece a los adversarios demasiadas oportunidades para acceder y ocultarse con facilidad.

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

   La reducción de falsos positivos ayuda a los equipos de seguridad a centrarse en lo más importante. La contextualización admite un análisis de primera línea de eventos en marcha, ayuda a los equipos a valorar si estos eventos requieren atención inmediata y puede terminar produciendo respuestas automatizadas y análisis más profundos.

La eficacia en cifras: el valor de la colaboración en el sector

La colaboración del sector es fundamental no solo para desarrollar una futura arquitectura para la defensa integrada contra amenazas que permita responder más rápido, sino también para no perder el paso a una comunidad global de creadores de amenazas cada vez más audaz, innovadora y persistente. Los adversarios son cada vez más hábiles implementando campañas de alta rentabilidad y difíciles de detectar. Muchos emplean ahora recursos legítimos de la infraestructura para propiciar estas campañas, y con gran éxito.

Con este panorama, no es de extrañar que los responsables de seguridad entrevistados para el Estudio comparativo sobre capacidades de seguridad 2015 de Cisco tengan menos confianza en su capacidad para proteger la organización. Sugerimos que estos responsables consideren el enorme impacto que una colaboración proactiva y continua del sector puede tener en el desenmascaramiento de la ciberdelincuencia, el socavamiento de la capacidad del rival para generar ingresos y la reducción de las oportunidades para lanzar futuros ataques.

Como se ha tratado anteriormente en este informe (consulte "Historias destacadas" a partir de la **página 10**), la cooperación entre un colaborador partner de Cisco, el ecosistema Collective Security Intelligence (CSI) y proveedores de servicios fue un factor decisivo en la capacidad de Cisco para desvelar, verificar y desarticular operaciones globales centradas en el kit de aprovechamiento de vulnerabilidades Angler, así como en el debilitamiento de una de las mayores botnets DDoS que nuestros investigadores han observado nunca, SSHPsychos.

Acerca de Cisco

Acerca de Cisco

Cisco proporciona ciberseguridad inteligente para el mundo real, ya que ofrece una de las carteras de soluciones de protección contra amenazas más amplia del sector para el conjunto más grande de vectores de ataque. El enfoque sobre la seguridad implementado y centrado en las amenazas de Cisco reduce la complejidad y la fragmentación mientras proporciona una visibilidad superior, control uniforme y protección avanzada contra amenazas antes, durante y después de un ataque.

Los investigadores de amenazas del ecosistema de inteligencia de seguridad colectiva de Cisco (CSI) aportan, bajo un mismo marco, la inteligencia de amenazas líder del sector mediante el uso de datos de telemetría extraídos de la amplia gama de dispositivos y sensores, de fuentes públicas y privadas, y de la comunidad de código abierto de Cisco. Gracias a esto, se registran diariamente datos de miles de millones de solicitudes web y millones de correos electrónicos, así como muestras de malware e intrusiones en la red.

Nuestra infraestructura y nuestros sistemas sofisticados emplean estos datos de telemetría para ayudar a los investigadores y los sistemas de aprendizaje mediante máquinas a llevar a cabo un seguimiento de las amenazas en las redes, los Data Centers, los terminales, los dispositivos móviles, los sistemas virtuales, la Web, los correos electrónicos y la nube con el fin de identificar las causas principales y determinar el alcance de los brotes. La información que se obtiene se convierte en protección en tiempo real para nuestras ofertas de servicios y productos, que se presta de inmediato a clientes de Cisco en todo el mundo.

Para obtener más información acerca del enfoque de Cisco centrado en las amenazas, visite **www.cisco.com/go/security.**

Colaboradores del Informe de seguridad anual de Cisco 2016

TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

Talos es la organización de inteligencia de amenazas de Cisco, un grupo de élite de expertos en seguridad dedicados a proporcionar la mejor protección para los clientes, productos y servicios de Cisco. El grupo está compuesto por importantes investigadores y cuenta con sofisticados sistemas para crear para los productos de Cisco una inteligencia capaz de detectar, analizar y proteger contra las amenazas conocidas y emergentes. Talos cumple el conjunto de normas oficiales de Snort.org, ClamAV, SenderBase.org y SpamCop. Además, es el principal equipo que aporta información sobre amenazas al ecosistema de Cisco CSI.

SERVICIOS AVANZADOS EN LA NUBE Y TRANSFORMACIÓN DE TI, EQUIPO DE OPTIMIZACIÓN

El equipo proporciona recomendaciones y optimiza redes, Data Centers y soluciones basadas en la nube para los principales proveedores de servicios y empresas del mundo. Esta oferta de asesoramiento se centra en maximizar la disponibilidad, el rendimiento y la seguridad de las soluciones esenciales de los clientes. Este servicio de optimización se ofrece a más del 75% de las empresas de la lista Fortune 500.

EQUIPO ACTIVE THREAT ANALYTICS

El equipo Cisco Active Threat Analytics (ATA) ayuda a las organizaciones a defenderse contra intrusiones conocidas, ataques de día cero y amenazas persistentes avanzadas al aprovechar las tecnologías avanzadas de Big Data. 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. Proporciona vigilancia constante y análisis a demanda las 24 horas del día, los 7 días de la semana.

ORGANIZACIÓN CISCO THOUGHT LEADERSHIP

La organización Cisco Thought Leadership ilumina las oportunidades globales, las transiciones del mercado y las soluciones clave que transforman organizaciones, industrias y experiencias. La organización proporciona una mirada incisiva que predice lo que una empresa puede esperar en un mundo en rápida transformación e indica cuál es el mejor modo de competir. Buena parte del liderazgo del equipo se centra en ayudar a las organizaciones a digitalizarse, y para ello tiende sólidos puentes entre los entornos físico y virtual con el fin de acelerar la innovación y lograr los resultados comerciales deseados.

COGNITIVE THREAT ANALYTICS

Cognitive Threat Analytics de Cisco es un servicio basado en la nube que detecta infracciones, malware que se ejecuta dentro de redes protegidas y otras amenazas de seguridad por medio de análisis estadísticos de los datos del tráfico de red. Hace frente a los puntos débiles de las defensas perimetrales mediante la identificación de los síntomas de la infección de malware o de la infracción de datos. Para ello, emplea análisis de comportamiento y capacidades de detección de anomalías. Cognitive Threat Analytics se basa en un aprendizaje automatizado y en modelos estadísticos avanzados para detectar nuevas amenazas de forma independiente, aprender de lo que ve y adaptarse con el tiempo.

GLOBAL GOVERNMENT AFFAIRS

Cisco se relaciona con los gobiernos en muchos y distintos niveles para ayudar a dar forma a las políticas y leyes relativas al sector tecnológico, así como para ayudar a los gobiernos a alcanzar sus objetivos. El equipo Global Government Affairs desarrolla e influye en las políticas y leyes favorables a la tecnología. Trabaja en colaboración con partes interesadas del sector y partners, y establece relaciones con líderes gubernamentales para influir en las políticas que afectan a los negocios de Cisco y a la adopción general de ICT, siempre con vistas a ayudar a dar forma a las decisiones políticas en los ámbitos global, nacional y local. El equipo está compuesto por antiguos cargos públicos, parlamentarios, reguladores, funcionarios estadounidenses de alto nivel y profesionales de asuntos administrativos que ayudan a Cisco a promover y proteger el uso de la tecnología en todo el mundo.

EQUIPO INTELLISHIELD

El equipo de IntelliShield realiza investigaciones sobre vulnerabilidades y amenazas, además de análisis, integración y correlación de datos e información procedentes de las operaciones e investigaciones de seguridad de Cisco y las fuentes externas para generar el servicio IntelliShield Security Intelligence Service, que es compatible con numerosos productos y servicios de Cisco.

LANCOPE

Lancope, una empresa de Cisco, es uno de los principales proveedores de visibilidad de red e inteligencia de seguridad, y su fin es proteger a las empresas de las mayores amenazas de hoy en día. Mediante el análisis de NetFlow, IPFIX y otros tipos de telemetría de la red, el StealthWatch® System de Lancope proporciona análisis con identificación del entorno para detectar rápidamente un amplio abanico de ataques, desde APT y DDoS hasta malware de día cero y amenazas de trabajadores internos. Mediante la combinación de supervisión lateral continua en las redes empresariales y detección de usuarios, dispositivos y aplicaciones, Lancope acelera la respuesta ante incidentes, mejora los diagnósticos y reduce el riesgo empresarial.

OPENDNS

OpenDNS, una empresa de Cisco, es la plataforma de seguridad en la nube más grande del mundo y sirve diariamente a más de 65 millones de usuarios repartidos por más de 160 países. OpenDNS Labs es el equipo de investigación de seguridad de OpenDNS y está encargado de la plataforma de seguridad. Para obtener más información, visite **www.opendns.com** o **https://labs.opendns.com**.

SECURITY AND TRUST ORGANIZATION

La Security and Trust Organization subraya el compromiso de Cisco con la resolución de dos de los problemas que más preocupan a juntas directivas y líderes mundiales por igual. Entre los principales objetivos de la organización están la protección de los clientes públicos y privados de Cisco, la habilitación e implantación de los sistemas Secure Development Lifecycle y Trustworthy Systems de Cisco en todo su catálogo de productos y servicios, y la protección de la empresa ante unas ciberamenazas en constante evolución. Cisco adopta un enfoque integral de la seguridad generalizada y la confianza, lo que incluye personas, políticas, procesos y tecnología. La Security and Trust Organization busca la excelencia operativa y para ello se centra en las áreas de seguridad de la información, ingeniería fiable, protección de datos y privacidad, seguridad de la nube, transparencia y validación, e investigación y administración de seguridad avanzada. Para obtener más información, visite **http://trust.cisco.com.**

SECURITY RESEARCH AND OPERATIONS (SR&O)

La función de Security Research and Operations (SR&O) es gestionar las amenazas y vulnerabilidades de todos los productos y servicios de Cisco, y cuenta con el equipo de élite Product Security Incident Response Team (PSIRT). SR&O ayuda a los clientes a entender el cambiante panorama de amenazas en eventos como Cisco Live and Black Hat y mediante la colaboración con otros grupos de Cisco y del sector. Además, SR&O innova para ofrecer nuevos servicios, como Custom Threat Intelligence (CTI), que es capaz de identificar indicadores de compromiso que las infraestructuras de seguridad existentes no han podido detectar o mitigar.

Colaborador partner de Cisco

LEVEL 3 THREAT RESEARCH LABS

Level 3 Communications es un importante proveedor de comunicaciones globales con sede en Broomfield, Colorado, y ofrece servicios de comunicación para empresas, gobiernos y operadoras. Nuestra plataforma de servicios dispone de extensas redes de fibra en tres continentes conectadas por instalaciones submarinas y ofrece recursos subterráneos que llegan a más de 500 mercados en más de 60 países. La red de Level 3 proporciona una amplia vista del panorama de amenazas global.

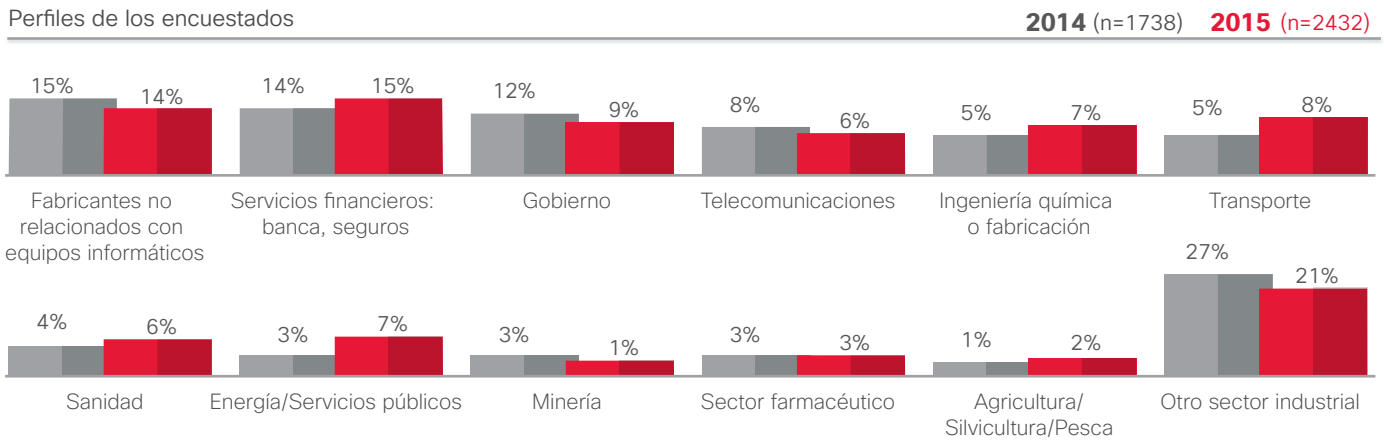
Level 3 Threat Research Labs es el grupo de seguridad que analiza de forma proactiva el panorama global de amenazas y relaciona la información con fuentes internas y externas para ayudar a proteger a los clientes de Level 3, su red e Internet. El grupo se asocia con regularidad con líderes del sector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

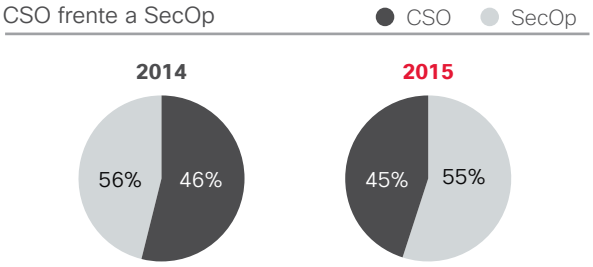
Apéndice

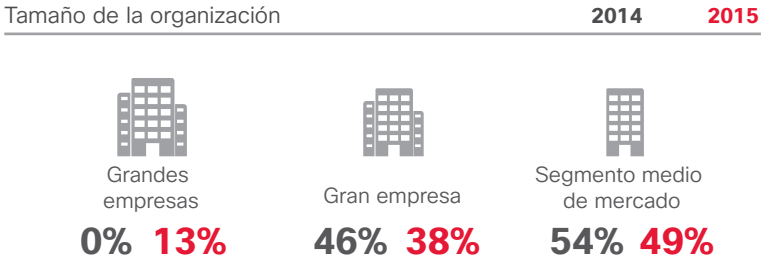
Apéndice

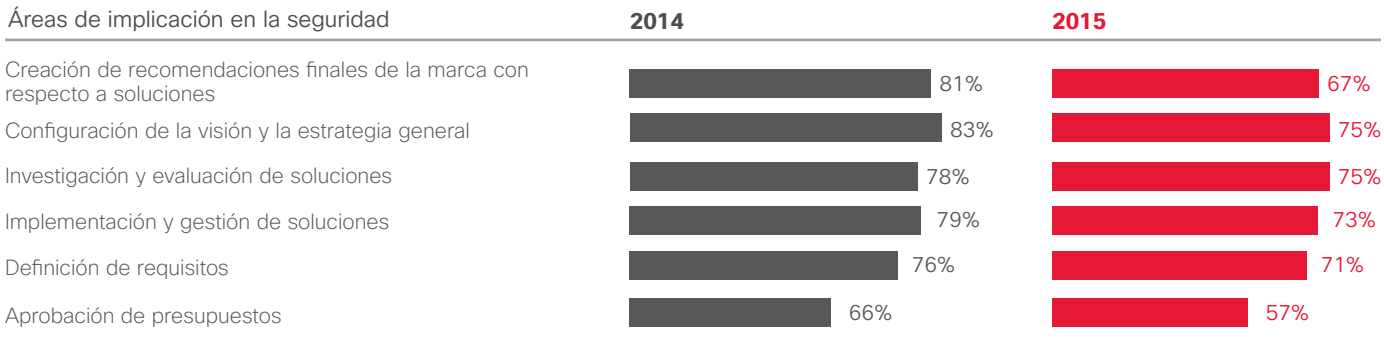
Estudio comparativo sobre capacidades de seguridad 2015 de Cisco: perfil y recursos de los encuestados

Figura 71. Perfiles de los encuestados





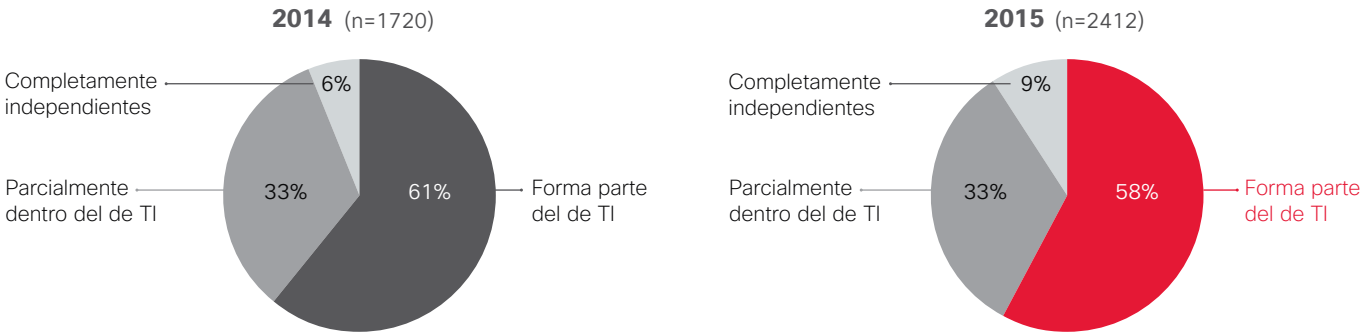




Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

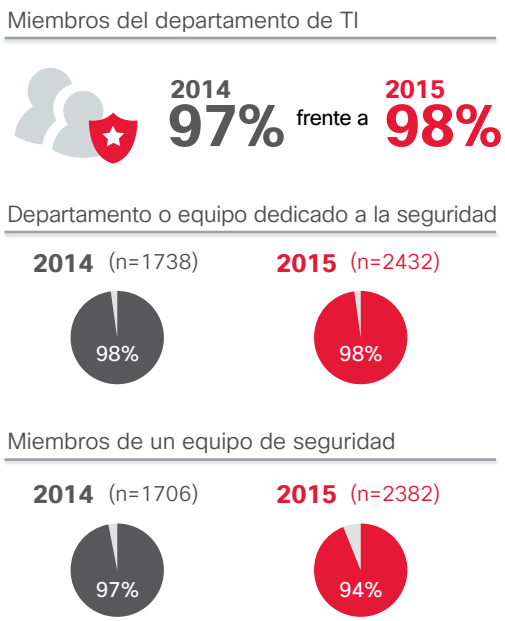
Figura 72. Aunque solo el 9% tiene el presupuesto de seguridad separado del presupuesto de TI, esta cifra ha aumentado de forma significativa respecto a 2014

¿El presupuesto de seguridad forma parte del presupuesto de TI? (Miembros del departamento de TI)



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 73. Cargos: encuestados y sus supervisores



Cargo		Cargo de gerente	
Director de seguridad	22%	Director ejecutivo	34%
Director de tecnología	18%	Presidente/Propietario	18%
Director de TI	16%	Director de seguridad	6%
Director de información	13%	Director de información	6%
Director de operaciones de seguridad	7%	Director de tecnología	6%
Vicepresidente de seguridad de TI	5%	Director de TI	4%
Director de riesgos y cumplimiento de normativas	4%	Vicepresidente de seguridad de TI	4%
Director de operaciones de seguridad	4%	Vicepresidente de TI	2%
Arquitecto de seguridad	4%	Consejo de dirección	2%
Vicepresidente de TI	3%	Director de operaciones	1%
Director de operaciones	3%	Director financiero	1%
Otro cargo	2%	Otro cargo	0%

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 74. El firewall es la herramienta más habitual de defensa contra las amenazas para la seguridad; en 2015 se administraron menos defensas mediante servicios basados en la nube que en 2014

Defensas frente a amenazas de seguridad que emplea cada organización	**2014** (n=1738)	**2015** (n=2432)	Las defensas administradas por servicios basados en la nube (encuestados de seguridad que utilizan defensas frente a amenazas a la seguridad) **2014** (n=1646)	**2015** (n=2268)
Firewall*	N/D	65%		31%
Prevención de la pérdida de datos	55%	56%		
Autenticación	52%	53%		
Cifrado/Privacidad/Protección de datos	53%	53%		
Seguridad de correo electrónico y mensajería	56%	52%	37%	34%
Seguridad web	59%	51%	37%	31%
Protección de terminales/Antimalware	49%	49%	25%	25%
Control de acceso/Autorización	53%	48%		
Administración de identidades/Aprovisionamiento de usuario	45%	45%		
Prevención de intrusiones*	N/D	44%		20%
Seguridad de la movilidad	51%	44%	28%	24%
Red inalámbrica segura	50%	41%	26%	19%
Análisis de vulnerabilidades	48%	41%	25%	21%
VPN	48%	40%	26%	21%
Información de seguridad y gestión de eventos	43%	38%		
Defensa ante DDoS	36%	37%		
Pruebas de penetración	38%	34%	20%	17%
Parches y configuración	39%	32%		
Diagnósticos de red	42%	31%		
Diagnósticos de terminales	31%	26%		
Red, seguridad, firewalls y prevención de intrusiones*	60%	N/A	35%	
Ninguno de los anteriores	1%	1%	13%	11%

*Firewall y prevención de intrusiones eran un código en 2014 "Red, seguridad, firewalls y prevención de intrusiones"

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

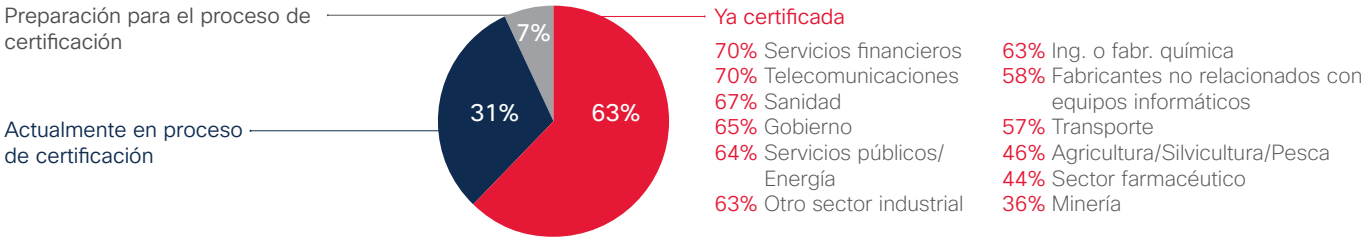
Contratación externa

Figura 75. Asesamiento y consultoría siguen siendo los principales servicios de seguridad externalizados

Se han detectado aumentos importantes en la subcontratación de auditorías y respuestas ante incidentes. Se observa que la subcontratación es más rentable.

La mitad (el 52%) sigue prácticas y políticas de seguridad estandarizadas como ISO 27001; la misma que el año pasado. De estos, la mayoría ya están certificadas o están en proceso de certificación.

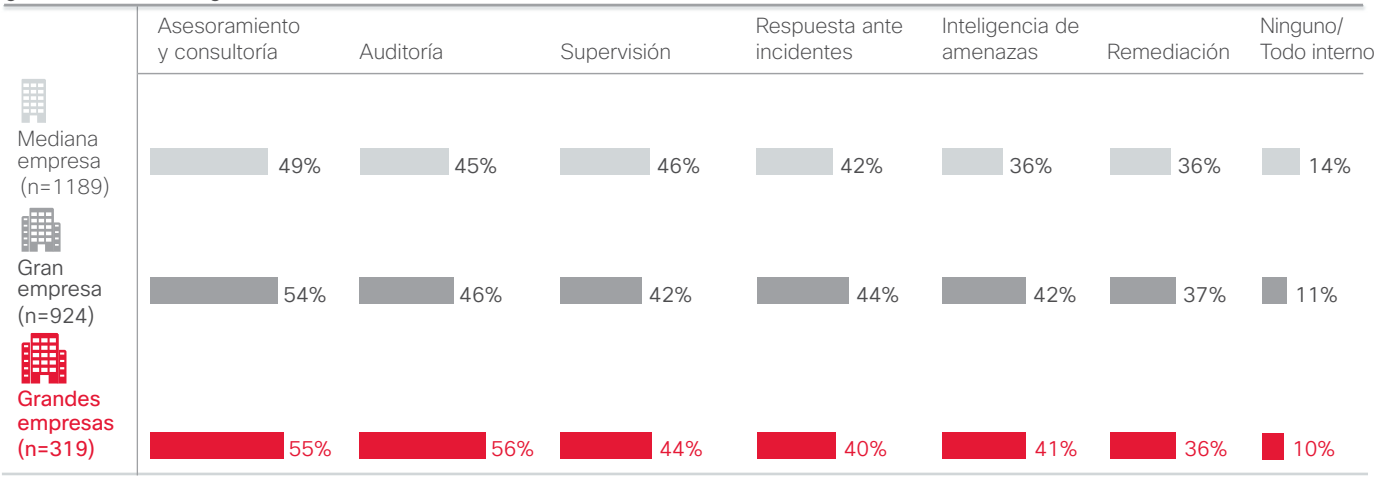
Práctica de la política de seguridad estandarizada
La organización sigue la práctica de la política de seguridad de información estandarizada (**2015**: n=1265)



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 76. Vista de empresa de servicios externalizados: las grandes empresas son mucho más propensas a externalizar las auditorías, el asesoramiento y la consultoría

¿Qué servicios de seguridad se subcontratan?



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

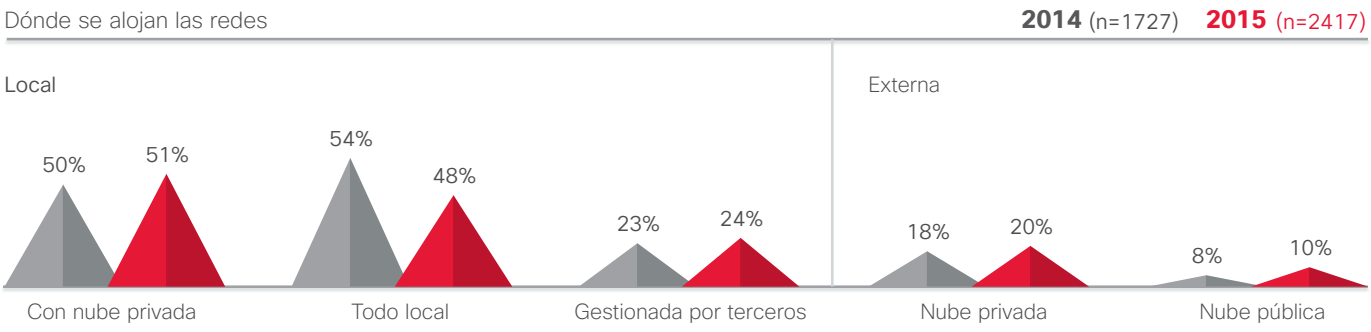
Figura 77. Vista de país de servicios externalizados: Japón es mucho más propenso a externalizar el asesoramiento y la consultoría

¿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 ante incidentes	42%	46%	39%	32%	38%	43%	53%	34%	49%	53%	45%	27%	54%
Inteligencia de amenazas	39%	42%	40%	37%	46%	36%	16%	36%	48%	47%	44%	42%	39%
Remediación	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 de Cisco 2015

Figura 78. El alojamiento local de redes sigue siendo lo más común. Sin embargo, el alojamiento externo ha aumentado respecto al año pasado



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Brecha de seguridad pública

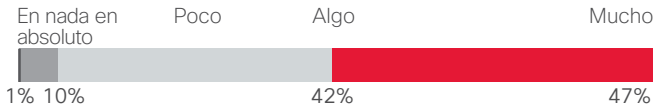
Figura 79. Menos organizaciones indicaron en 2015 que habían tenido que afrontar el escrutinio público que acarrean las brechas de seguridad

Las brechas de seguridad son factores importantes que impulsan las mejoras:

En **2015** fue menor el número de organizaciones que tuvo que afrontar el escrutinio público que acarrean las brechas de seguridad en comparación con **2014**.

2014 **53%** frente al 2015 **48%**

¿En qué medida impulsó una brecha de seguridad mejoras en las políticas, los procedimientos o las tecnologías de defensa ante amenazas? (n=1134)



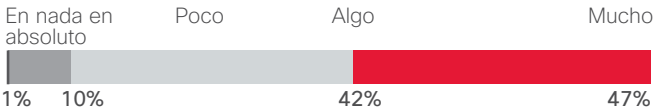
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 80. Las brechas públicas pueden mejorar la seguridad

Las brechas de seguridad son factores importantes que impulsan las mejoras: Participantes dedicados a la seguridad. **2014** (n=1701) **2015** (n=1347)

2014 **53%** Sí frente al 2015 **48%** Sí

¿En qué medida impulsó una brecha de seguridad mejoras en las políticas, los procedimientos o las tecnologías de defensa ante amenazas? (n=1134)



Los CSO mencionan más mejoras tras una brecha de seguridad que los directores de seguridad.

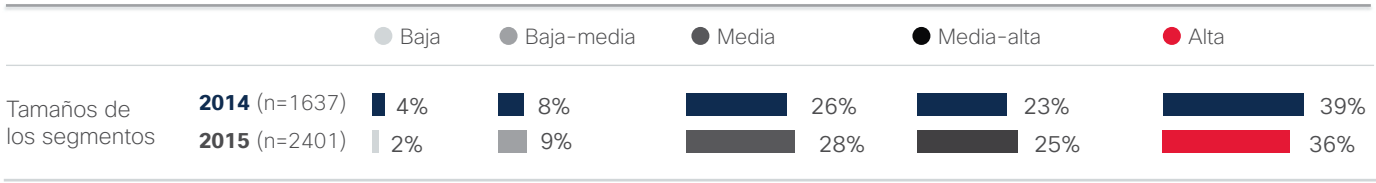
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Liderazgo y madurez

Figura 81. El modelo de cinco segmentos se adapta estrechamente al modelo de madurez de la capacidad de seguridad (CMM).

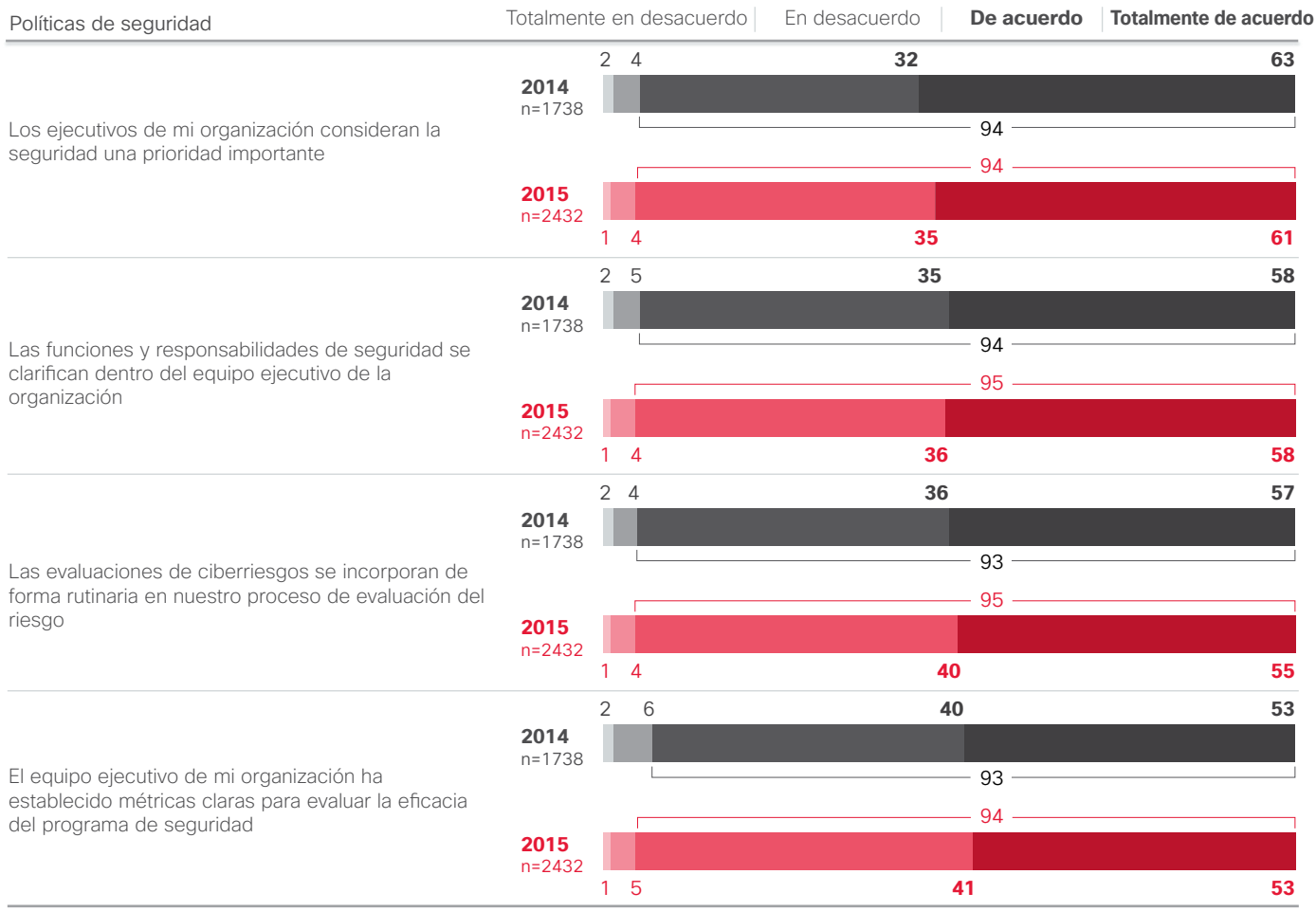
Los segmentos reflejan un patrón similar al estudio del año pasado en cuanto a la madurez en la prioridad de la seguridad y cómo esto se traduce en procesos y procedimientos.

60% o más encaja en perfiles de más seguridad-madurez. Se cumple en general en todos los países y sectores.



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 82. Como en 2014, casi todos están de acuerdo o muy de acuerdo con que los altos ejecutivos consideran la seguridad una alta prioridad.



Los encuestados del sector farmacéutico están de acuerdo con la declaración "El equipo ejecutivo mi organización ha establecido métricas claras para evaluar la eficacia del programa de seguridad" en un porcentaje significativamente mayor que los de otros sectores.

Bastantes más CSO que directores de seguridad están de acuerdo con todas las afirmaciones relativas a la participación de los ejecutivos.

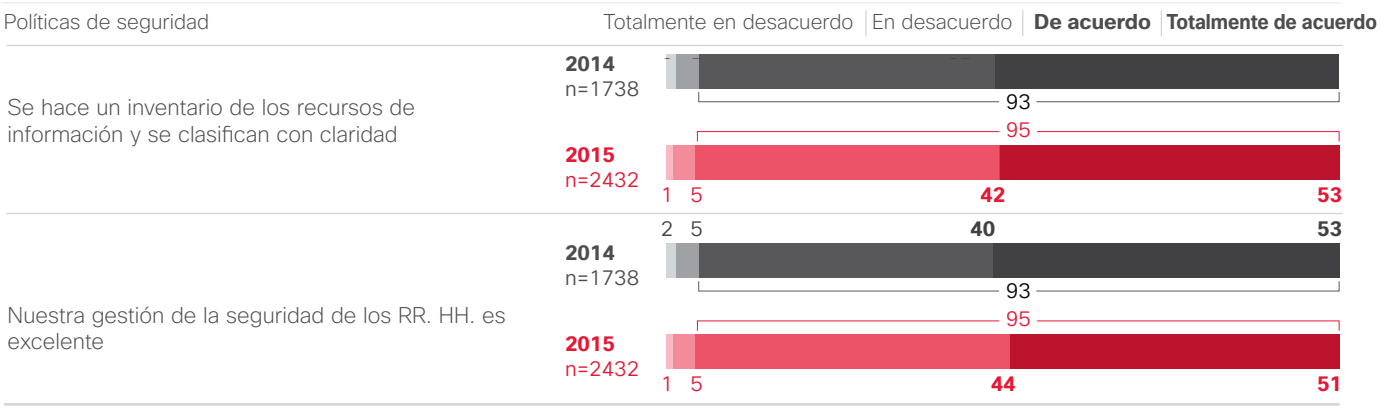
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Procesos

Figura 83. Confianza dividida en la capacidad para dotar a los sistemas de seguridad

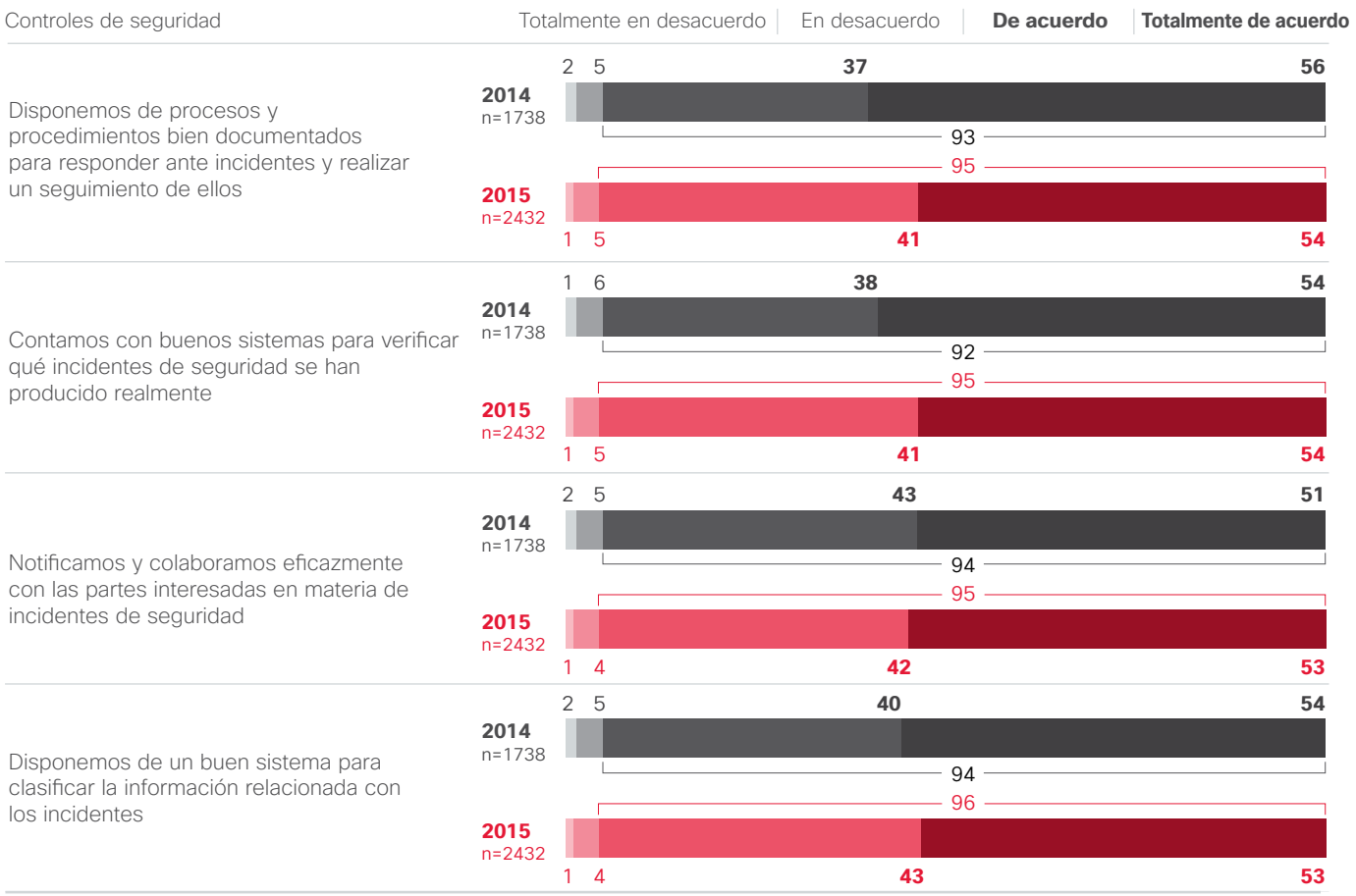
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 83. Confianza dividida en la capacidad para dotar a los sistemas de seguridad (continuación)



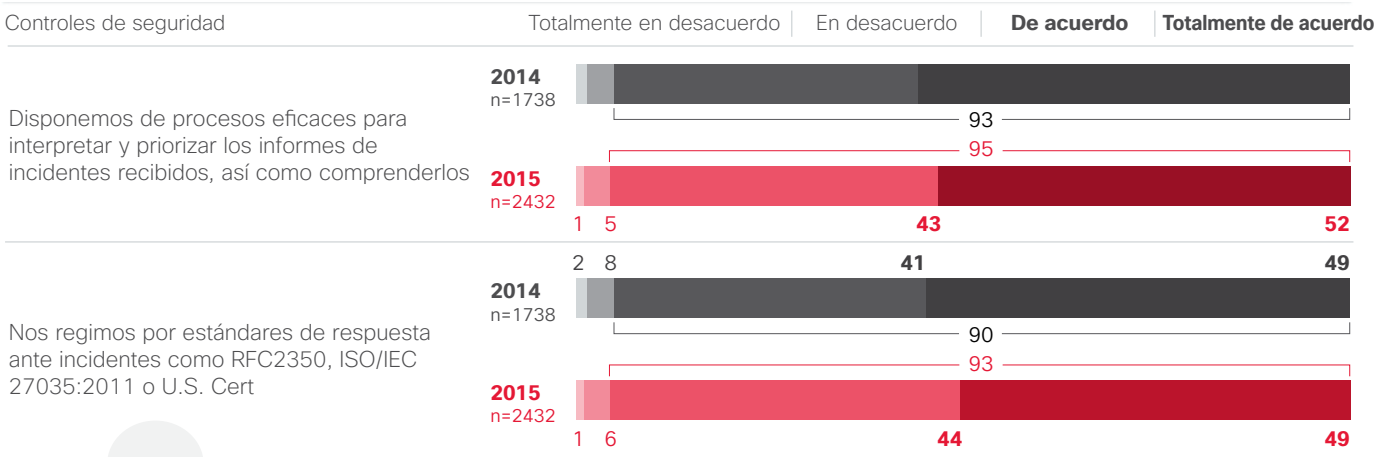
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 84. Las empresas consideran que cuentan con buenos controles de seguridad



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 84. Las empresas consideran que cuentan con buenos controles de seguridad (continuación)



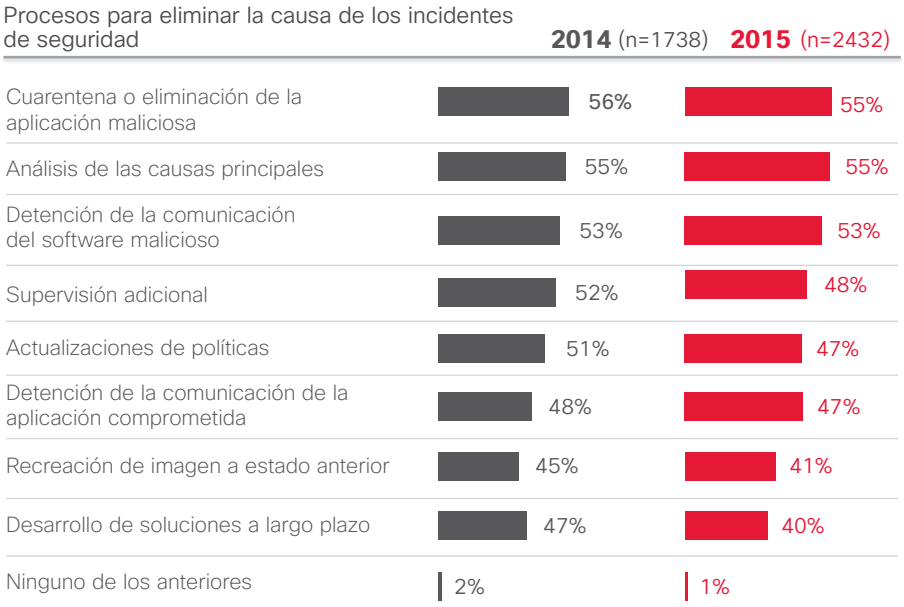
Los encuestados de servicios financieros están totalmente de acuerdo con la afirmación "Disponemos de un buen sistema para clasificar la información relacionada con los incidentes" más a menudo que los profesionales de la mayoría de los sectores.

A excepción de la afirmación "Notificamos y colaboramos eficazmente con las partes interesadas en materia de incidentes de seguridad", los CSO se muestran más positivos respecto a los controles de seguridad que los directores de seguridad.

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 85. La puesta en cuarentena/eliminación de aplicaciones maliciosas y el análisis de las causas principales siguen siendo los procesos más utilizados

Significativamente más encuestados de EE. UU. mencionan "Ninguna de las opciones anteriores" cuando se les pregunta por procesos para eliminar la causa de un incidente de seguridad en comparación con los encuestados de la mayoría de los demás países.

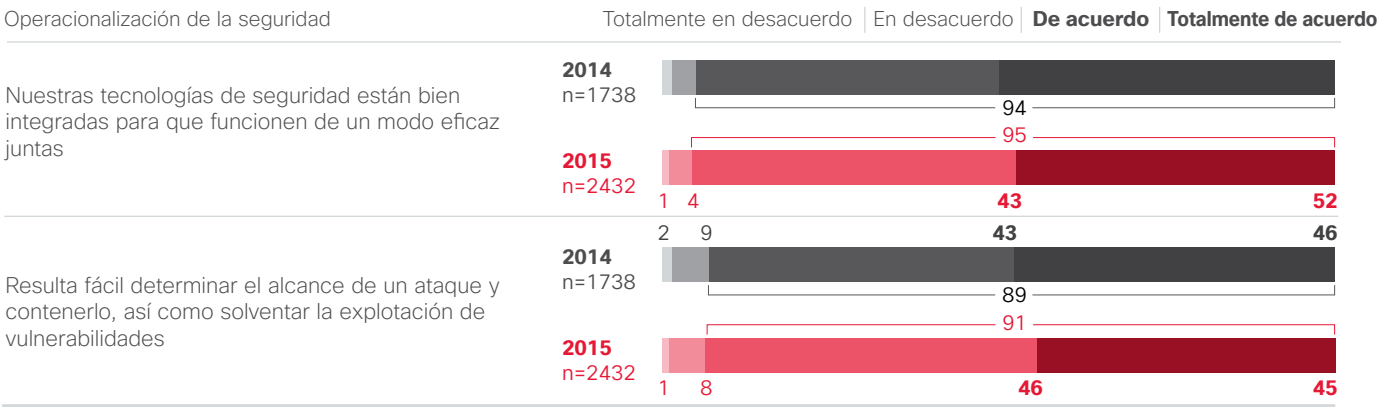


Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 86. Las empresas muestran una confianza dividida respecto a la capacidad para alojar compromisos

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

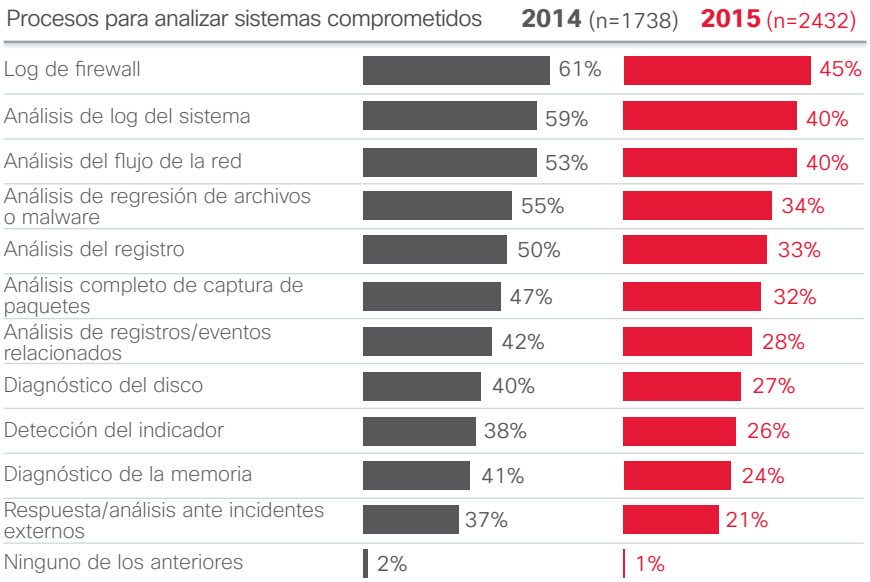
Figura 86. Las empresas muestran una confianza dividida respecto a la capacidad para contener riesgos (continuación)



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 87. El análisis de los registros del firewall y del sistema siguen siendo los procesos más utilizados para analizar sistemas en peligro

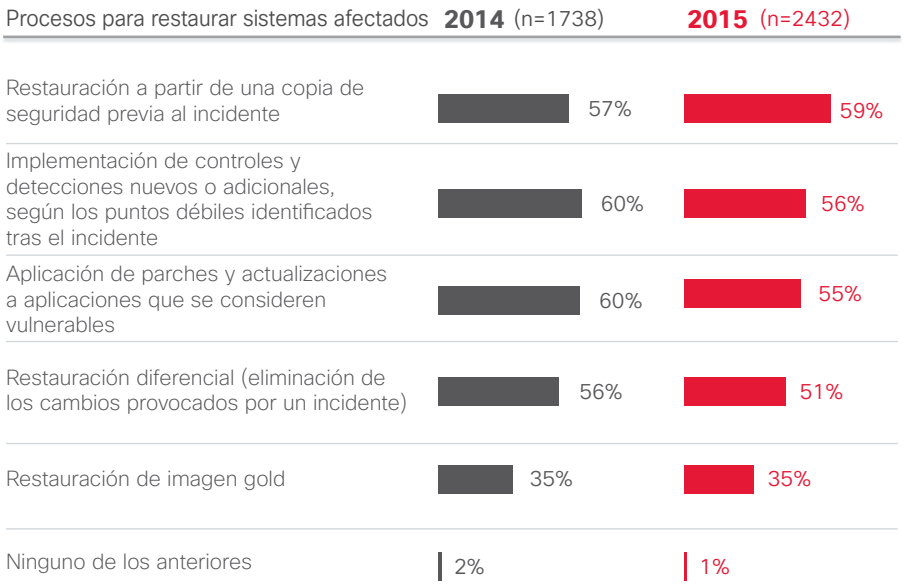
Las empresas medianas y grandes afirman que utilizan más procesos para analizar sistemas en riesgo que las medianas empresas.



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

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

Los encuestados en China dicen actualizar y aplicar parches a las aplicaciones consideradas vulnerables más frecuentemente que los encuestados en otros países analizados.

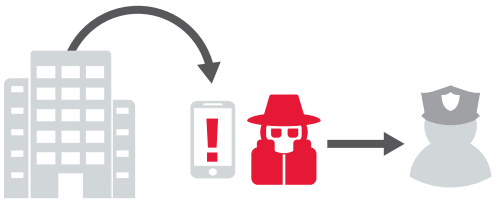


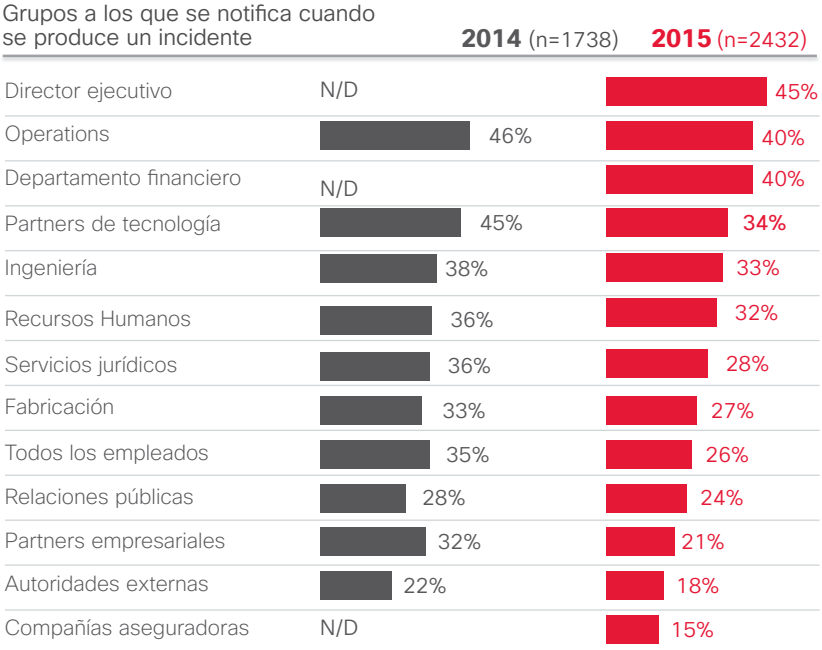
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 89. El director ejecutivo o presidente es el cargo más escogido para recibir la notificación de un incidente de seguridad, seguido por Operaciones y el departamento financiero

Bastante más encuestados pertenecientes a grandes empresas que a empresas de tamaño medio indican que notifican probablemente a autoridades externas en caso de incidentes

Grandes empresas



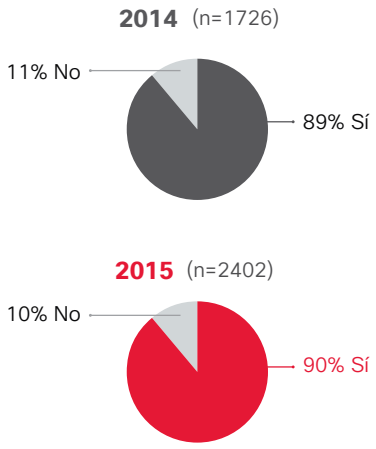


Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

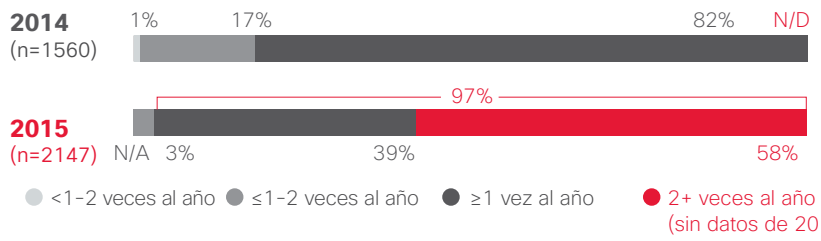
Formación

Figura 90. Casi todas las empresas (97%) proporcionan formación sobre seguridad al menos una vez al año

¿El personal de seguridad asiste a programas de formación o de concienciación sobre la importancia de la seguridad con regularidad? (Encuestados dedicados a la seguridad)



¿Con qué frecuencia se forma a los empleados en seguridad? (Encuestados cuyos equipos de seguridad reciben formación)



Más empresas que han sufrido una brecha en la seguridad imparten con regularidad programas de formación y de concienciación sobre la importancia de la seguridad (96%) que las que no la han sufrido (83%).

Sí **96%** frente al No **83%**

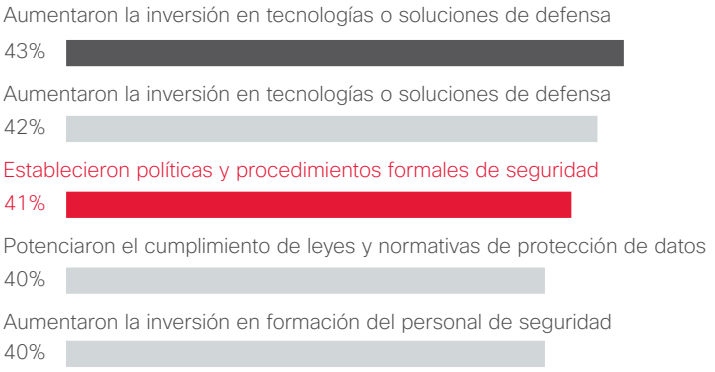
Más grandes empresas afirman que disponen de programas periódicos de formación y de concienciación sobre la importancia de la seguridad (93%) en comparación con las medianas empresas (88%) y las empresas grandes (89%).

Grandes empresas **93%** Segmento de medianas empresas **88%** Gran empresa **89%**

Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 91. La frecuencia de la formación sobre la importancia de la seguridad y la incidencia de las políticas de seguridad formales aumentan desde 2014, lo que evidencia que se está actuando al respecto.

(5 principales menciones) Los encuestados afectados por una brecha de seguridad (**2015** n=1109)



Aumentaron la formación/concienciación sobre la importancia de la seguridad entre los empleados

En 2015, el 43% de los encuestados afirmó que había aumentado la formación tras una brecha de seguridad.

43%

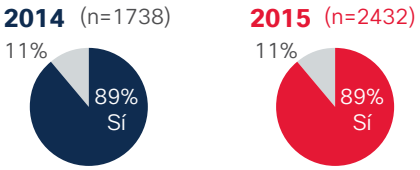
En 2015, el 41% de los encuestados afirmó que había establecido políticas y procedimientos formales de seguridad.

41%

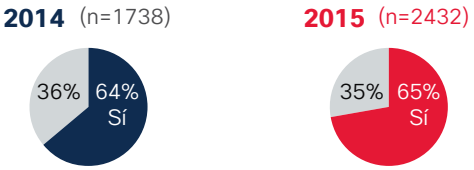
Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Figura 92. Al igual que en 2014, casi 9 de cada 10 indican que su personal de seguridad asiste a conferencias o cursos centrados en la seguridad

¿Los integrantes del personal de seguridad asisten a conferencias o cursos externos para mejorar y no perder sus habilidades?
(Encuestados dedicados a la seguridad)



¿Los empleados participan en comités o consejos del sector de la seguridad?
(Encuestados dedicados a la seguridad)



Fuente: Estudio comparativo sobre capacidades de seguridad de Cisco 2015

Estudio sobre riesgos de seguridad y fiabilidad

Figura 93. Trasfondo y metodología

A Cisco le interesa comprender mejor la percepción que los responsables de la toma de decisiones de TI de empresas y proveedores de servicios tienen respecto a los riesgos y retos en materia de seguridad para sus organizaciones, y el papel que la confianza en los proveedores de TI tiene en la adquisición de soluciones.

Los objetivos específicos incluyen:

- Valorar el nivel de riesgo de las amenazas y vulnerabilidades internas y externas
- Conocer las estrategias, políticas y soluciones que se implementan para mitigar riesgos de seguridad
- Identificar el proceso de compra de soluciones de TI y el papel que la fiabilidad del proveedor de TI tiene en dicho proceso
- Valorar el interés en recibir comunicaciones acerca de la validación de la fiabilidad de los proveedores de TI
- Determinar si hay diferencias por sectores o públicos en la perspectiva o el enfoque de los riesgos de seguridad y su mitigación

Metodología: enfoque cuantitativo y cualitativo

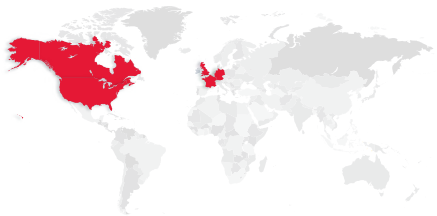
Se emplearon dos métodos para obtener información acerca de estos objetivos de investigación:

(Todos los encuestados son responsables de la decisión de compra de productos de TI = RCTI)

Encuesta cuantitativa en Internet entre **1050 RCTI de empresas**
(402 EE. UU., 282 Reino Unido, 197 Alemania, 169 Francia)

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

La investigación se realizó en EE. UU, Reino Unido, Francia, Alemania, y Canadá (solo IDI)



La recopilación de datos se realizó entre agosto y septiembre de 2015

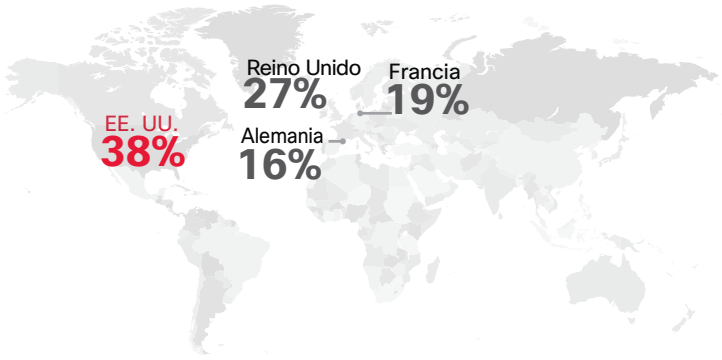
20 **minutos** de encuesta en Internet

45 **minutos** de entrevista a fondo

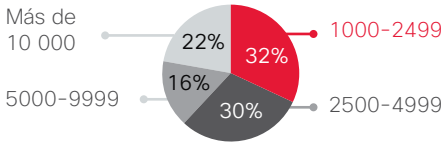
Fuente: Estudio sobre riesgos de seguridad y fiabilidad, Cisco

Figura 94. Perfil de la encuesta para empresas: cuantitativa

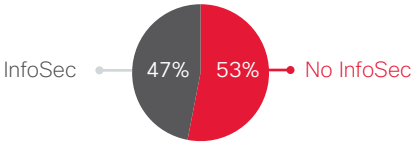
País



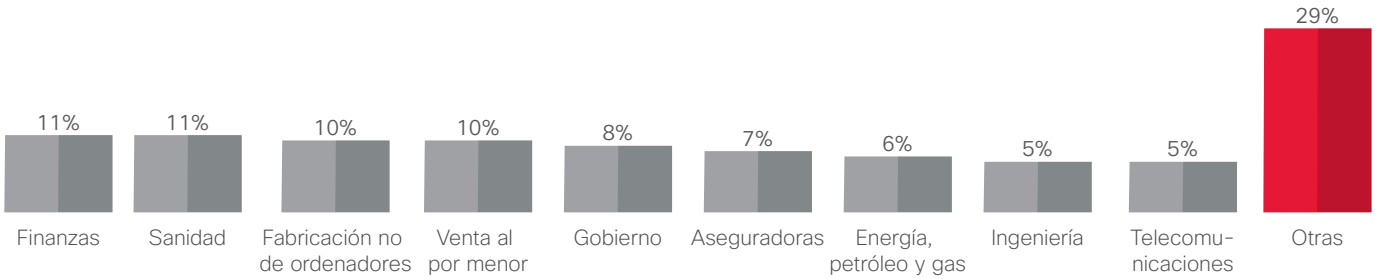
Tamaño de la empresa



Clasificación InfoSec



Sector (si se superó el 5%)



Cargo

Nivel ejecutivo (CIO, CSO, CTO, etc.).	25%
Vicepresidente	9%
Director	30%
Ingeniero o arquitecto Sénior	6%
Ingeniero	3%
Gerente	26%
Servicios jurídicos	2%

Implicaciones de compra

Establecer la visión/estrategia	69%
Asegurar el cumplimiento de normativas	71%
Aprobar las grandes compras	69%
Investigar/evaluar soluciones	77%
Dar la opinión o tomar decisiones finales de marca	80%
Implementar/gestionar soluciones	77%
Autorizar financiación/aprobar presupuesto	53%

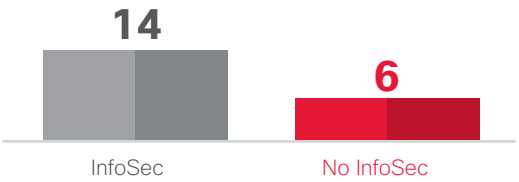
Fuente: Estudio sobre riesgos de seguridad y fiabilidad, Cisco

Figura 95. Perfil de la encuesta para proveedores de servicios: cualitativa

País

Tamaño de la empresa

Clasificación InfoSec



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 Sénior	1%
Ingeniero o arquitecto Sénior	2%
Gerente	1%

Implicaciones de compra

Establecer la visión/estrategia	80%
Asegurar el cumplimiento de normativas	100%
Aprobar las grandes compras	70%
Investigar/evaluar soluciones	95%
Tomar decisiones finales de marca	85%
Implementar/gestionar soluciones	75%
Autorizar financiación/aprobar	60%

Fuente: Estudio sobre riesgos de seguridad y fiabilidad, Cisco

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

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono y fax se encuentran en la Web de Cisco en **www.cisco.com/go/offices.**

Publicado en enero de 2016

© 2016 Cisco y/o sus filiales. Todos los derechos reservados.

Cisco y el logotipo de Cisco son marcas comerciales o marcas registradas de Cisco o de sus filiales en EE. UU. y en otros países. Si desea consultar una lista de las marcas comerciales de Cisco, visite **www.cisco.com/go/trademarks**. Las marcas registradas de terceros que se mencionan aquí son de propiedad exclusiva de sus respectivos propietarios. El uso de la palabra " partner" no implica la existencia de una asociación entre Cisco y cualquier otra empresa. (1110R)

Adobe, Acrobat y Flash son marcas registradas de Adobe Systems Incorporated en Estados Unidos y otros países.