Informe anual de seguridad
de 2015

Resumen ejecutivo

Existen ciertas constantes en el dinámico entorno de amenazas moderno.

Los adversarios se comprometen a desarrollar o mejorar continuamente nuevas técnicas para evadir la detección y ocultar la actividad maliciosa. Mientras tanto, los defensores (principalmente los equipos de seguridad) deben mejorar constantemente su enfoque de protección de la organización y de los usuarios contra estas campañas cada vez más sofisticadas.

Atrapados en el medio se encuentran los usuarios. Pero ahora parece que no solo son ellos el objetivo, sino también los facilitadores cómplices de los ataques.

El *Informe anual de seguridad de 2015 de Cisco*, que presenta la investigación, las perspectivas y los puntos de vista provistos por Cisco® Security Research y otros expertos en seguridad de Cisco, explora la carrera continua entre los atacantes y los defensores, y cómo los usuarios se convierten en enlaces cada vez más débiles dentro de la cadena de seguridad.

La seguridad cibernética es un tema amplio y complejo que tiene un impacto de largo alcance sobre los usuarios, las compañías, los gobiernos y otras entidades en todo el mundo. El *Informe anual de seguridad de 2015 de Cisco* se divide en cuatro áreas de debate. Estas secciones, y los temas explorados, pueden parecer diferentes a primera vista, pero un análisis más detallado revela su interconexión:

Cuatro áreas de debate del *Informe anual de seguridad de 2015 de Cisco:*

1. Inteligencia contra amenazas
2. Estudio comparativo de capacidades de seguridad de Cisco
3. Geopolítica y tendencias de la industria
4. Cambio de actitud frente a la seguridad cibernética: de los usuarios a la sala de reuniones del directorio

1. Inteligencia contra amenazas

Esta sección proporciona una descripción general de la más reciente investigación sobre amenazas de Cisco, que incluye actualizaciones sobre kits de aprovechamiento de vulnerabilidades, spam, amenazas y vulnerabilidades, además de tendencias de publicidad malintencionada (malvertising). También analiza la creciente dependencia de los delincuentes en línea respecto de los usuarios para lanzar sus ataques. A fin de elaborar el análisis de las tendencias observadas en 2014, Cisco Security Research utilizó un conjunto global de datos de telemetría. La inteligencia contra amenazas provista en el informe representa el trabajo realizado por los principales expertos en seguridad de Cisco.

2. Estudio comparativo de capacidades de seguridad

Para evaluar las percepciones de los profesionales de seguridad respecto del estado de la seguridad en las organizaciones, Cisco consultó a jefes de seguridad de la información (CISO) y gerentes de operaciones de seguridad (SecOps) de nueve países y organizaciones de diferente tamaño sobre sus procedimientos y recursos de seguridad. Los resultados del estudio son exclusivos del *Informe anual de seguridad de 2015 de Cisco*.

3. Geopolítica y tendencias de la industria

En esta sección, los expertos en política, geopolítica y seguridad de Cisco identifican tendencias geopolíticas actuales y emergentes que las organizaciones, especialmente las compañías multinacionales, deben controlar. Se centran en cómo prosperan los delitos cibernéticos en áreas de débil gestión. También cubren los desarrollos internacionales recientes relacionados con los temas de soberanía de datos, localización de datos, cifrado y compatibilidad de datos.

4. Cambio de actitud frente a la seguridad cibernética: de los usuarios a la sala de reuniones corporativas

Los expertos en seguridad de Cisco sugieren que ha llegado el momento de que las organizaciones comiencen a ver su enfoque respecto de la seguridad cibernética de manera diferente si desean alcanzar la seguridad del mundo real. Entre las estrategias se incluyen: la adopción de controles de seguridad más sofisticados para proteger contra amenazas antes, durante y después de los ataques; la institución de la seguridad como tema a tratar de la sala de reuniones del directorio; y la implementación del Manifiesto de seguridad de Cisco, un conjunto de principios de seguridad que permite que las organizaciones tengan un enfoque más dinámico de la seguridad y sean más realistas e innovadoras que sus adversarios.

La interconexión de los temas de seguridad cubiertos en el *Informe anual de seguridad de 2015 de Cisco* se reduce a lo siguiente: los atacantes se han vuelto competentes en el aprovechamiento de las brechas de seguridad a fin de ocultar su actividad maliciosa. Tanto los usuarios como los equipos de seguridad forman parte del problema de seguridad. Mientras que muchos defensores creen que sus procesos de seguridad están optimizados y sus herramientas de seguridad son eficaces, la verdad es que su preparación para la seguridad probablemente necesita mejorar. Lo que sucede en el panorama geopolítico, desde la legislación hasta las amenazas de seguridad, puede tener un impacto directo en las operaciones comerciales y la manera en que las organizaciones abordan la seguridad. Tomando en cuenta todos estos factores, nunca ha sido tan importante que las organizaciones de todos los tamaños comprendan que la seguridad es un problema de la gente, que la participación es inevitable y que el momento de adoptar un nuevo enfoque para la seguridad es ahora.

Descubrimientos clave

Los siguientes son descubrimientos clave presentados en el Informe anual de seguridad de 2015 de Cisco.

Los atacantes se han vuelto competentes en el aprovechamiento de las brechas de seguridad a fin de ocultar su actividad maliciosa.

- En 2014, el 1% de las alertas de exposición y vulnerabilidades comunes de extrema urgencia (CVE) fue activamente aprovechado. Esto significa que las organizaciones deben priorizar y revisar inmediatamente ese 1% de las vulnerabilidades. Pero incluso con la tecnología líder en seguridad, se requiere la excelencia en el proceso para abordar las vulnerabilidades.
- Desde que se eliminó el kit de aprovechamiento de vulnerabilidades Blackhole en 2013, ningún otro kit de aprovechamiento de vulnerabilidades ha podido lograr niveles de éxito similares. Sin embargo, es posible que los creadores de kits de aprovechamiento de vulnerabilidades no ansíen tanto los primeros puestos como antes.
- Las vulnerabilidades de seguridad de Java han disminuido un 34%, dado que la seguridad de Java ha mejorado y los adversarios buscan adoptar nuevos vectores de ataque.
- El malware basado en Flash ahora interactúa con JavaScript para ocultar la actividad maliciosa, lo que dificulta su detección y análisis.
- El volumen de spam aumentó un 250% de enero de 2014 a noviembre de 2014.
- El spam tipo raqueta de nieve (snowshoe), que implica el envío de pequeños volúmenes de spam desde un gran conjunto de direcciones IP para evitar ser detectados, es una amenaza emergente.

Los usuarios y equipos de TI se han convertido en piezas involuntarias del problema de seguridad.

- Los delincuentes en línea dependen de los usuarios para instalar malware o aprovechar las brechas de seguridad.
- Heartbleed (hemorragia de corazón), una peligrosa brecha de seguridad, expone críticamente el OpenSSL. Aún así, el 56% de todas las versiones de OpenSSL tiene más de 50 meses y es vulnerable.
- El comportamiento negligente de los usuarios al utilizar Internet, junto con las campañas dirigidas de los adversarios, ponen a muchos sectores de la industria en mayor riesgo de exposición a malware basado en la web. En 2014, la industria química y farmacéutica emergió como el principal sector de mayor riesgo de exposición a malware basado en la web, según Cisco Security Research.
- Los creadores de malware utilizan los complementos de los navegadores web como medio de distribución de malware y aplicaciones no deseadas. Este enfoque de distribución de malware es acertado para los protagonistas malintencionados, dado que muchos usuarios confían inherentemente en los complementos o simplemente los consideran benignos.

El *Estudio comparativo de capacidades de seguridad de Cisco* revela controversia en las percepciones sobre la preparación para la seguridad.

- El 59% de los CISO considera que sus procesos de seguridad están optimizados en comparación con el 46% de los SecOps.
- Aproximadamente el 75% de los CISO considera que sus herramientas de seguridad son muy o extremadamente eficaces, mientras que solo un cuarto percibe las herramientas de seguridad como medianamente eficaces.
- El 91% de los encuestados de las compañías con seguridad sofisticada coincide plenamente en que los ejecutivos de las compañías consideran la seguridad como una alta prioridad.
- Menos del 50% de los encuestados utiliza herramientas estándar, como revisiones y configuraciones para evitar las brechas de seguridad.
- Las organizaciones grandes o medianas son más propensas a adoptar estados de seguridad altamente sofisticada en comparación con las organizaciones de otros tamaños incluidas en el estudio.

Contenido

Atacantes frente a defensores: una carrera continua

Los profesionales de seguridad y los delincuentes en línea se encuentran en una carrera continua para ver quién supera a quién.

Por el lado de la seguridad, las organizaciones parecen haber ganado el juego mediante la adopción de herramientas más sofisticadas para evitar los ataques y reducir el impacto. Han reconocido la necesidad comercial de adoptar una sólida postura de seguridad y confían en la optimización de sus procesos de seguridad. Los proveedores de tecnología también prestan mayor atención a la localización y eliminación de vulnerabilidades de sus productos, lo que brinda a los delincuentes menos oportunidades para aprovecharse.

Pero al mismo tiempo, los adversarios se vuelven más sofisticados no solo en sus enfoques de lanzamiento de ataques, sino también en la evasión de la detección:

- Cambian sus tácticas y herramientas a cada momento, ya sea desapareciendo de la red antes de que los detengan o eligiendo rápidamente un método diferente para obtener acceso.
- Elaboran campañas de spam con cientos de direcciones IP en un intento por eludir los productos de reputación anti-spam basada en IP.
- Diseñan malware basado en las herramientas que los usuarios consideran benignas o de confianza para infectar y ocultarse persistentemente a plena vista en sus máquinas.
- Encuentran nuevas vulnerabilidades para aprovechar cuando los proveedores suprimen las debilidades de otros productos.
- Trabajan con el fin de tener una presencia oculta o combinación en la organización designada; a veces demoran semanas o meses para establecer diversas posiciones iniciales en las infraestructuras y bases de datos de los usuarios. Solo cuando están listos ejecutan su misión principal.

Conforme al nuevo *Estudio comparativo de capacidades de seguridad de Cisco* (consulte la página 24), los profesionales de seguridad son optimistas respecto de su buena preparación para detener a los atacantes en línea. No obstante, los adversarios siguen robando información, ganando dinero mediante estafas o interrumpiendo las redes con objetivos políticos. En definitiva, la seguridad es una cuestión de números: aunque una organización bloquee el 99,99% de los miles de millones de mensajes de spam, alguno se filtrará. No hay manera de garantizar una eficacia del 100%.

Cuando estos mensajes o kits de aprovechamiento de vulnerabilidades llegan a los usuarios, son los mismos usuarios los que se convierten en puntos débiles en la red. Debido a que las empresas se han vuelto más adeptas al uso de soluciones que bloquean las brechas de la red, el malware y el spam, es posible que entonces los protagonistas malintencionados se aprovechen de los usuarios a través de tácticas tales como el envío de solicitudes falsas para restablecer la contraseña.

Con usuarios que se convierten en enlaces cada vez más débiles dentro de la cadena de seguridad, las empresas deben tomar decisiones durante la implementación de políticas y tecnologías de seguridad: mientras los desarrolladores intentan que las aplicaciones y el software sean más intuitivos y fáciles de usar, ¿crean las organizaciones agujeros de seguridad que los delincuentes cibernéticos aprovechan? ¿Eluden las empresas a los usuarios porque asumen que no son confiables ni educables e instalan controles de seguridad más estrictos que obstaculizan el trabajo de los usuarios? ¿Dedican tiempo a educar a los usuarios sobre la implementación de los controles de seguridad y a explicar claramente cómo los usuarios desempeñan un papel vital para ayudar a las organizaciones a alcanzar la seguridad dinámica que respalda a las empresas?

Como sugieren los principios descritos en el Manifiesto de seguridad de Cisco en la página 45: lo segundo. Las soluciones tecnológicas raramente facultan a los usuarios para hacerse cargo de la seguridad como participantes activos. En cambio, los fuerzan a trabajar en torno a herramientas de seguridad que obstaculizan su trabajo diario, lo que deja a las empresas más inseguras. La seguridad ya no es una cuestión de *si* la red estará en riesgo. Todas las redes *estarán* en riesgo en algún momento. ¿Qué harán entonces las organizaciones? Y si el personal de seguridad supiera que la red se podría estar en riesgo, ¿se enfocaría en la seguridad de manera diferente?

El *Informe anual de seguridad de 2015 de Cisco* presenta la más reciente investigación del grupo Cisco Security Research. El equipo examina los avances de la industria de seguridad diseñados para defender las organizaciones y los usuarios de los ataques, y las técnicas y estrategias empleadas por los adversarios que esperan romper dichas defensas. El informe además resalta los descubrimientos clave del *Estudio comparativo de capacidades de seguridad de Cisco,* que examina la postura de seguridad de las empresas y sus percepciones respecto de su preparación para defenderse de los ataques. También analiza las tendencias geopolíticas, los desarrollos globales relacionados con la localización de datos, el valor de controles de acceso seguro más sofisticados, la segmentación en función del acceso basado en funciones y la importancia de hacer de la seguridad cibernética un tema de la sala de reuniones.

1. Inteligencia contra amenazas

Cisco Security Research ha reunido y analizado en este informe los puntos de vista de la seguridad en función de un conjunto global de datos de telemetría. Los expertos en seguridad de Cisco realizan investigaciones y análisis continuos de amenazas descubiertas, como tráfico de malware, que pueden proporcionar perspectivas sobre el posible comportamiento delictivo futuro y ayudar en la detección de amenazas.

Vulnerabilidades de seguridad web: para los creadores de kits de aprovechamiento de vulnerabilidades, ocupar el primer lugar no implica ser los mejores

En el mundo de los negocios, las compañías aspiran a ser reconocidas como líderes en la industria. Pero en el caso de los creadores de kits de aprovechamiento de vulnerabilidades que operan en la denominada "economía en la sombra", mantenerse en el cuarto o quinto puesto entre los líderes de kits de aprovechamiento de vulnerabilidades puede ser incluso un signo más evidente de éxito, según Cisco Security Research.

Como revela el *Informe de seguridad de mitad de año 2014 de Cisco,* no ha habido un líder absoluto entre los kits de aprovechamiento de vulnerabilidades desde fines de 2013.[1] En aquel entonces, las autoridades eliminaron el ampliamente utilizado, bien mantenido yaltamente eficaz kit de aprovechamiento de vulnerabilidades Blackhole después de arrestar a su presunto creador y distribuidor, conocido como "Paunch". Cisco Security Research sugiere que una de las causas principales de que (aún) no exista ningún kit de aprovechamiento de vulnerabilidades dominante es simplemente porque ningún otro kit ha surgido como verdadero líder tecnológico entre los competidores. Otra tendencia observada: desde la deposición de Paunch y Blackhole, más usuarios de kits de aprovechamiento de vulnerabilidades parecen estar invirtiendo en kits técnicamente sofisticados en términos de su capacidad para evadir la detección.

Durante todo el 2014, Angler, Sweet Orange y Goon fueron los kits de aprovechamiento de vulnerabilidades observados con mayor frecuencia "en estado salvaje", según los expertos en seguridad de Cisco. Entre todos los kits de aprovechamiento de vulnerabilidades, Angular se detectó con mayor frecuencia en el campo durante 2014 y, por motivos que no son claros, prevaleció especialmente a fines de agosto. Cisco Security Research atribuye la popularidad de Angular a la decisión de sus creadores de eliminar el requisito de descarga como ejecutable de Windows para distribuir el malware.

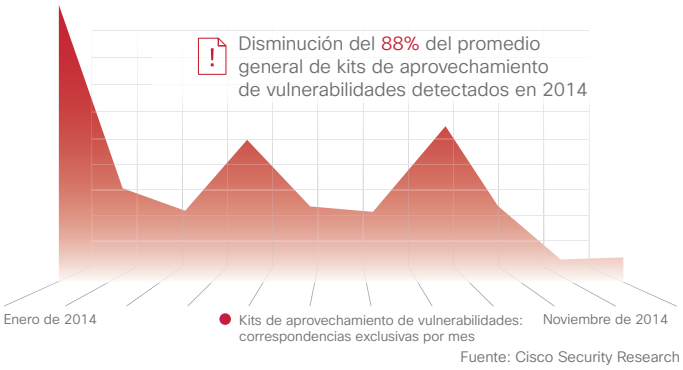
El uso de las vulnerabilidades de Flash, Java, Microsoft Internet Explorer (IE) e incluso Silverlight por parte de Angular hace que "haya que vigilar" este kit de aprovechamiento de vulnerabilidades, dicen los investigadores de Cisco. Una vez desencadenado el aprovechamiento de vulnerabilidades, la carga del malware se escribe directamente en la memoria mediante un proceso como iexplore.exe, en lugar de escribirse en el disco. La carga distribuida por Angular parece un blob de datos cifrados, lo que dificulta su identificación y bloqueo.

Para obtener más información sobre Angler y cómo se utiliza la publicidad malintencionada (malvertising) como modalidad principal de distribución de kits de aprovechamiento de vulnerabilidades a usuarios, consulte la entrada de blog de Cisco Security: "Aprovechamiento de vulnerabilidades de seguridad de Silverlight".

El kit de aprovechamiento de vulnerabilidades Sweet Orange es muy dinámico; sus componentes, puertos y URL de carga cambian constantemente para que Sweet Orange siga siendo eficaz y evite ser detectado. Esto hace que Sweet Orange sea el kit de aprovechamiento de vulnerabilidades "con más posibilidades de éxito", según Cisco Security Research. Sweet Orange distribuye una gama de malware que elimina la revisión de los sistemas de usuarios finales e incluye kits de aprovechamiento de vulnerabilidades de Adobe Flash Player, IE y Java. Los adversarios que utilizan Sweet Orange generalmente dependen de la publicidad malintencionada para redirigir a los usuarios a los sitios web, incluidos sitios legítimos, que alojan el kit de aprovechamiento de vulnerabilidades. Los usuarios son normalmente redirigidos al menos dos veces en el proceso. Los sitios web en riesgo que ejecutan versiones desactualizadas de los sistemas de gestión de contenidos (CMS), como WordPress y Joomla, son otras ubicaciones conocidas oportunas para alojar el kit de aprovechamiento de vulnerabilidades Sweet Orange.[2]

Con respecto al kit de aprovechamiento de vulnerabilidades Goon, Cisco Security Research apunta a su reputación en cuanto a confiabilidad como la principal razón para su modesta pero constante popularidad en 2014; también se ganó la distinción de kit de aprovechamiento de vulnerabilidades "más organizado" en comparación con otros kits. Originalmente descubierto por investigadores de seguridad en 2013, Goon, también conocido como "kit de aprovechamiento de vulnerabilidades Goon/Infinity", es un marco de distribución de malware que genera kits de aprovechamiento de vulnerabilidades del navegador pertenecientes a componentes de Flash, Java o Silverlight en plataformas Windows y Mac.[3]

Figura 1. Tendencias de kits de aprovechamiento de vulnerabilidades: cantidad de correspondencias exclusivas detectadas de enero a noviembre de 2014



Fuente: Cisco Security Research

Aunque la cantidad total de kits de aprovechamiento de vulnerabilidades detectados en el campo cayó un 87% en los meses posteriores a la desaparición del kit de aprovechamiento de vulnerabilidades Blackhole, la cantidad de kits detectados por Cisco Security Research aumentó en el verano de 2014 (consulte la Figura 1). En las últimas dos semanas de agosto, se observó un aumento significativo en la cantidad de detecciones en el campo del kit de aprovechamiento de vulnerabilidades Angular. Sin embargo, en noviembre, la cantidad total de detecciones de kits de aprovechamiento de vulnerabilidades conocidos disminuyó nuevamente, con algunas apariciones frecuentes de Angular y Goon/Infinity. La disminución general promedio de la cantidad de kits de aprovechamiento de vulnerabilidades detectados entre mayo y noviembre de 2014 fue del 88%.

Amenazas y vulnerabilidades: Java deja de ser un vector de ataque

En los últimos años, Java ha desempeñado un papel destacado en las listas de vulnerabilidades más predominantes y severas para aprovechar. No obstante, Java parece estar perdiendo popularidad entre los adversarios que buscan la manera más rápida, más fácil y menos detectable de lanzar kits de aprovechamiento de vulnerabilidades del software, según Cisco Security Research.

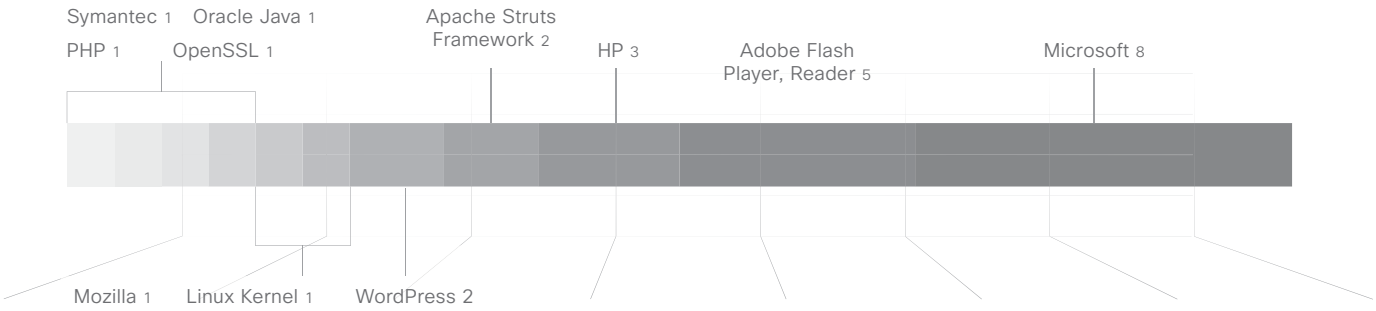
Lea la entrada de blog de Cisco Security: **"El paquete de aprovechamiento de vulnerabilidades Fiesta no es ninguna fiesta para las víctimas de la web"** para descubrir cómo las compañías pueden defenderse contra el kit de aprovechamiento de vulnerabilidades Fiesta. Este kit distribuye malware a través de vectores de ataque, como Silverlight, y utiliza dominios DNS dinámicos (DDNS) como páginas de destino de kits de aprovechamiento de vulnerabilidades.

Para obtener más detalles sobre el kit de aprovechamiento de vulnerabilidades Nuclear y su capacidad para evaluar los sistemas de los usuarios a fin de determinar las vulnerabilidades y distribuir los tipos de malware apropiados, consulte la entrada de blog de Cisco Security: **"Evolución del kit de aprovechamiento de vulnerabilidades Nuclear"**.

De las principales 25 alertas de vulnerabilidad relacionadas con productos y proveedores del 1.º de enero de 2014 al 30 de noviembre de 2014, solo una estuvo relacionada con Java (consulte la Tabla 1. Gráfico del sistema de puntuación de vulnerabilidades comunes [CVSS] en la página 10). En 2013, Cisco Security Research realizó el seguimiento de 54 nuevas vulnerabilidades de Java urgentes; en 2014, la cantidad de vulnerabilidades de Java seguidas disminuyó a 19. Esto no impedirá a los delincuentes en línea de la popularidad y la eficacia de atacar las vulnerabilidades anteriores que aún persisten.

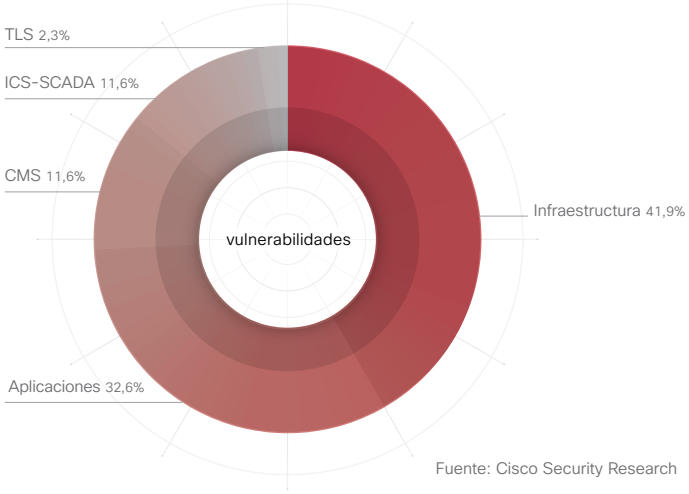
Los datos de la base de datos de vulnerabilidad nacional (NVD) muestran una disminución similar: la NVD informó 309 vulnerabilidades de Java en 2013 y 253 nuevas vulnerabilidades de Java en 2014. (Cisco Security Research sigue las vulnerabilidades importantes que tienen una puntuación alta en la escala del CVSS a partir de la cantidad más baja, mientras que la NVD incluye todas las vulnerabilidades informadas). La Figura 2 describe las principales vulnerabilidades aprovechadas por proveedor y producto de 2014.

Figura 2. Aprovechamiento de principales vulnerabilidades por producto y proveedor



Fuente: Cisco Security Research

Figura 3. Categorías de productos principales aprovechadas



Fuente: Cisco Security Research

El aprovechamiento de las vulnerabilidades de Adobe Flash Player y Microsoft IE por el lado del cliente, junto con los kits de aprovechamiento de vulnerabilidades que apuntan a los servidores (por ejemplo, el aprovechamiento de las vulnerabilidades de Apache Struts Framework, el marco web de fuente abierta), le quitó el liderazgo a Java. La creciente cantidad de aprovechamientos de vulnerabilidades de Apache Struts Framework es un ejemplo de la tendencia de los delincuentes a poner en riesgo la infraestructura en línea como manera de expandir el alcance y capacidad durante los ataques.

Apache Struts Framework es un punto de partida lógico para los kits de aprovechamiento de vulnerabilidades debido a su popularidad.

La Figura 3 resalta las categorías de productos más populares aprovechadas en 2014.

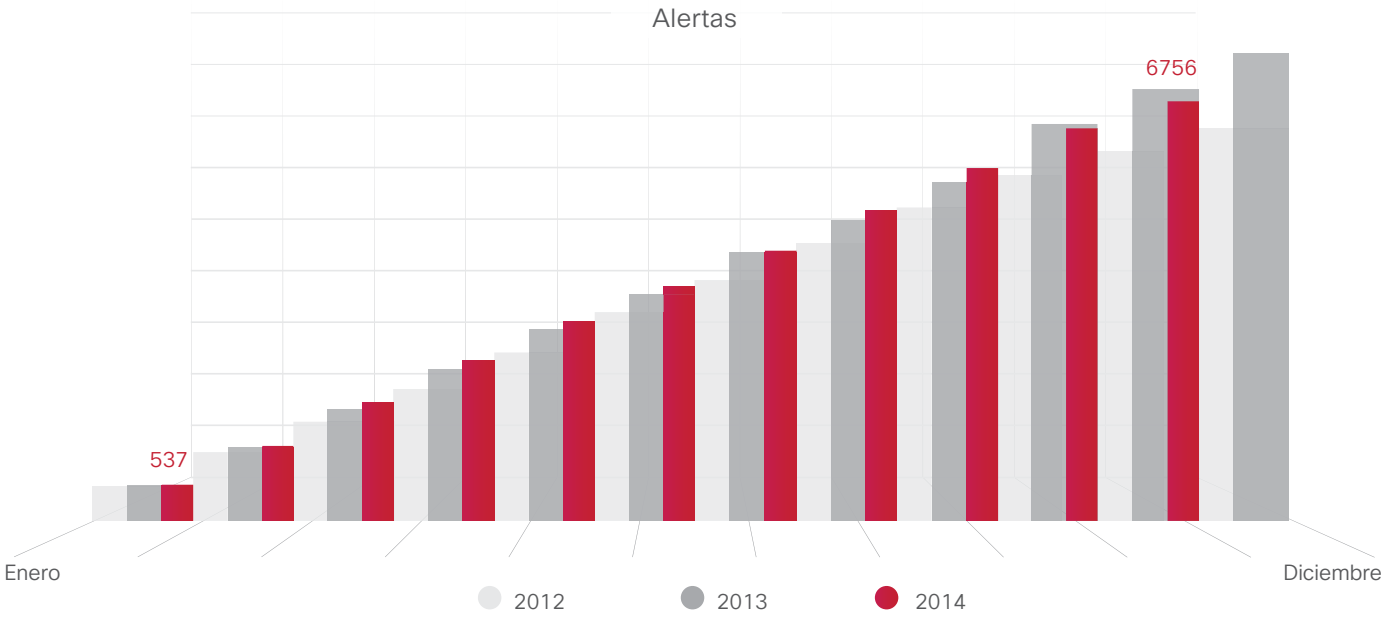
En 2014, las aplicaciones e infraestructuras fueron las más frecuentemente aprovechadas según los datos de Cisco Security Research. Los sistemas de gestión de contenidos (CMS) también son objetivos preferidos; los adversarios dependen de los sitios web que ejecutan versiones obsoletas de los CMS para facilitar la distribución de kits de aprovechamiento de vulnerabilidades.

Alertas anuales acumulativas en disminución

Las alertas anuales totales, las vulnerabilidades acumulativas de productos nuevos y actualizados informadas en 2014 y recopiladas por Cisco Security Research, parecen estar disminuyendo (Figura 4). A partir de noviembre de 2014, las alertas totales cayeron por debajo de los totales de 2013 un 1,8%. Puede que el porcentaje sea pequeño, pero es la primera vez en los últimos años que la cantidad de alertas ha disminuido en comparación con el año anterior.

La razón más probable de la disminución es la creciente atención que prestan los proveedores al desarrollo y la prueba de software. Los ciclos de desarrollo mejorados parecen reducir la cantidad de vulnerabilidades que los delincuentes aprovechan con facilidad.

Figura 4. Alertas anuales totales acumulativas



Fuente: Cisco Security Research

Tabla 1. Vulnerabilidades más comúnmente aprovechadas

Sistema de puntuación de vulnerabilidades comunes (CVSS)

ID de IntelliShield	Título	Urgencia	Credibilidad	Gravedad	Base	Temporal
33695	Vulnerabilidad de la divulgación de información de DTLS Heartbeat/OpenSSL TLS				5,0	5,0
35880	Vulnerabilidad de ejecución de código arbitrario de contenido de variables del entorno de prueba de GNU de procesamiento				10,0	7,4
35879	Vulnerabilidad de ejecución de código arbitrario de definiciones de funciones de variables del entorno de prueba de GNU de procesamiento				10,0	7,4
36121	Vulnerabilidad de inyección de núcleo SQL de Drupal				7,5	6,2
32718	Vulnerabilidad de ejecución de código remoto de Adobe Flash Player				9,3	7,7
33961	Vulnerabilidad de ejecución de código de objeto de memoria eliminado de Microsoft Internet Explorer				9,3	7,7
28462	Vulnerabilidad de ejecución de código arbitrario de derivación de seguridad de Oracle Java SE				9,3	7,7
30128	Productos Struts 2 Action de varios proveedores: vulnerabilidad de inyección de comando de procesamiento de parámetros				10,0	8,3

Fuente: Cisco Security Research

Alertas nuevas frente a alertas actualizadas

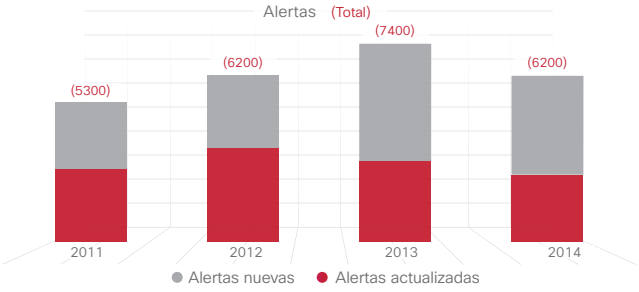
La cantidad de alertas nuevas para 2013 y 2014 indica que se siguen informando más vulnerabilidades nuevas en comparación con años anteriores; esto significa que los proveedores, desarrolladores e investigadores de seguridad descubren, eliminan e informan más vulnerabilidades nuevas en sus productos. Como se muestra en la Figura 5, la cantidad total de alertas nuevas y anuales es la misma o disminuyó ligeramente en 2014 en comparación con 2013.

La Tabla 1 ilustra algunas de las vulnerabilidades más comúnmente aprovechadas según el sistema de puntuación de vulnerabilidades comunes (CVSS). La base de datos de vulnerabilidad nacional (NVD) del Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos proporciona un marco de comunicación de las características y los impactos de las vulnerabilidades de TI que respalda el CVSS. La puntuación de "Urgencia" de la tabla del CVSS indica que estas vulnerabilidades están siendo aprovechadas, lo que se corresponde con la puntuación de "Temporal" que indica actividad de los kits de aprovechamiento de vulnerabilidades. Mediante el análisis de la lista de productos aprovechados, las empresas también pueden determinar cuáles de dichos productos están en uso y, en consecuencia, deben controlarse y revisarse.

La Figura 6 describe los proveedores y productos con las mayores puntuaciones del CVSS. Cisco indica mediante las puntuaciones del CVSS que existe un código de aprovechamiento de vulnerabilidades de prueba de concepto; sin embargo, el código no está públicamente disponible.

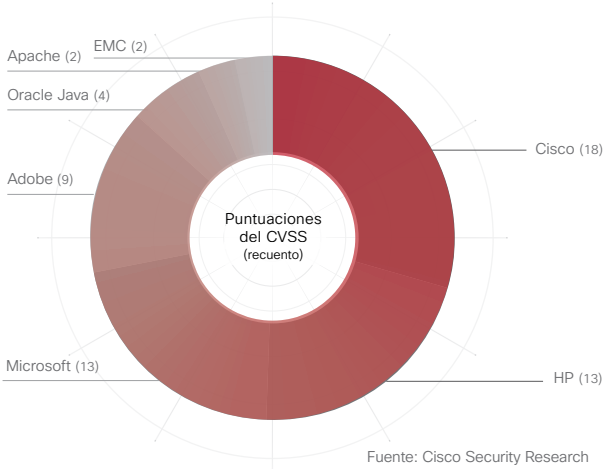
Nota: las vulnerabilidades de la Tabla 1 son las que mostraron signos iniciales de actividad de kits de aprovechamiento de vulnerabilidades durante el período observado. La mayoría de estas vulnerabilidades aún no se había convertido en "corriente principal"; es decir, no había llegado a los kits de aprovechamiento de vulnerabilidades para la venta.

Figura 5. Comparación de alertas nuevas y alertas actualizadas



Fuente: Cisco Security Research

Figura 6. Proveedores y productos con las mayores puntuaciones del CVSS



Fuente: Cisco Security Research

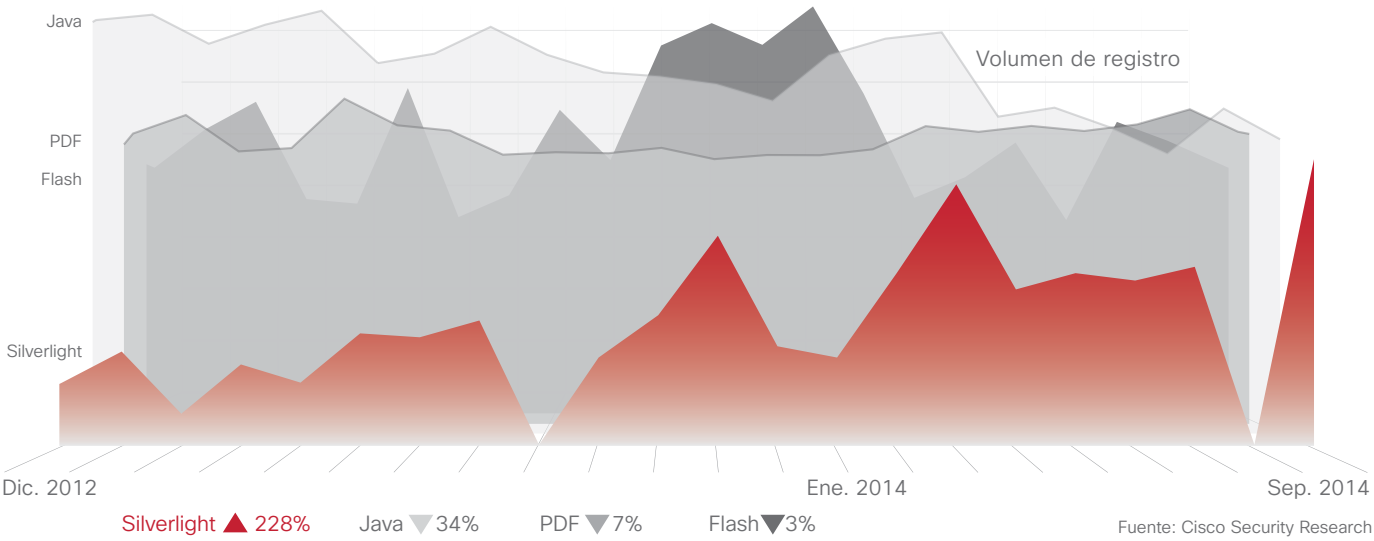
Análisis: factores probables del abandono de las vulnerabilidades de seguridad de Java por parte de los adversarios

Cisco Security Research sugiere que la disminución de las vulnerabilidades de seguridad de Java puede deberse en parte al hecho de que no se divulgaron ni dispusieron nuevas vulnerabilidades de seguridad de Java de día cero para que los adversarios aprovechen en 2014. Las versiones modernas de Java se revisan automáticamente y los proveedores de navegadores bloquean de forma predeterminada las versiones anteriores más vulnerables de Java Runtime Environment. Apple incluso toma la precaución adicional de deshabilitar las versiones obsoletas y vulnerables de Java, y de revisarlas a través de actualizaciones automáticas. Además, el Equipo de Respuesta ante Emergencias Informáticas de los Estados Unidos (US-CERT) recomienda desde enero de 2013 a los usuarios de computadoras que protejan, deshabiliten o eliminen Java.

La última versión de Java, Java 8, tiene controles más potentes que las versiones anteriores. Además, es difícil de vulnerar porque ahora requiere la interacción humana, como firma de código y diálogo de usuario que solicitan al usuario habilitar Java. Los delincuentes en línea han descubierto objetivos más simples y han vuelto su atención hacia vectores que no utilizan Java para obtener un mayor retorno de la inversión. Por ejemplo, muchos usuarios no actualizan periódicamente los navegadores o lectores Adobe Flash y PDF, lo que brinda a los delincuentes una gama más amplia de vulnerabilidades nuevas y viejas para aprovechar. Y, como revela el *Informe de seguridad de mitad de año de 2014 de Cisco,* la cantidad de kits de aprovechamiento de vulnerabilidades, incluido Microsoft Silverlight, sigue creciendo.[4]

La Figura 7 muestra que el reinado de Java como vector de ataque principal ha seguido una tendencia descendente durante más de un año. El uso de Flash para lanzar kits de aprovechamiento de vulnerabilidades ha sido un poco errático; el mayor aumento ocurrió en enero de 2014. El uso de PDF ha sido constante, dado que muchos protagonistas malintencionados parecen seguir enfocados en el lanzamiento de campañas altamente individualizadas a través de correos electrónicos con PDF adjuntos. Los ataques a Silverlight, aunque siguen estando muy por debajo en comparación con vectores más establecidos, siguen aumentando, especialmente desde agosto.

Figura 7. Comparación de tendencias de volúmenes por vector de ataque



Flash y JavaScript: ¿Juntos mejor?

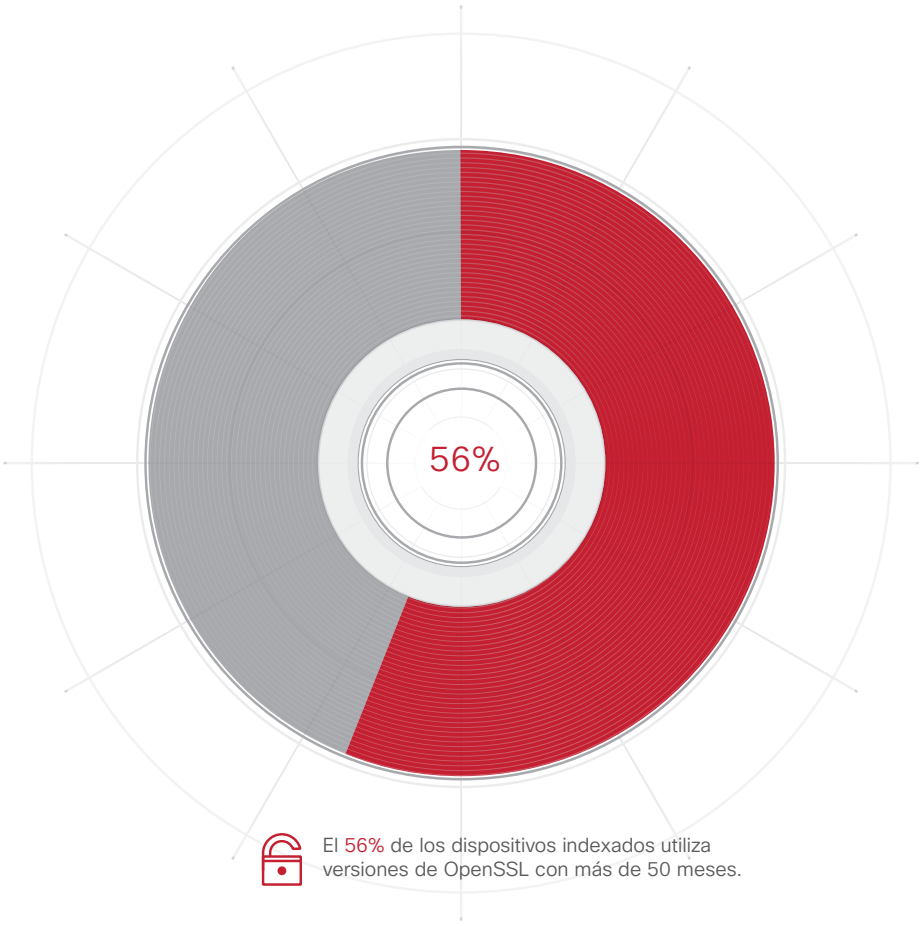
En 2014, Cisco Security Research observó el crecimiento del uso de malware basado en Flash que interactúa con JavaScript. El aprovechamiento de vulnerabilidades se comparte entre dos archivos diferentes: un archivo Flash y un archivo JavaScript. El intercambio del aprovechamiento de vulnerabilidades entre dos formatos y archivos diferentes dificulta la identificación y el bloqueo de los kits de aprovechamiento de vulnerabilidades y el análisis con herramientas de ingeniería inversa de los dispositivos de seguridad. Este enfoque además permite a los adversarios ser más eficientes y eficaces en sus ataques. Por ejemplo, si la primera fase de un ataque se encuentra completamente en JavaScript, la segunda fase, la transmisión de la carga, no ocurrirá hasta después de que JavaScript se ejecute satisfactoriamente. De esta manera, solo los usuarios que pueden ejecutar el archivo malicioso reciben la carga.

Esclarecimiento de la arqueología de las vulnerabilidades: peligros del software obsoleto y por qué la revisión no es la única solución

Como se explicó en el análisis de las vulnerabilidades (consulte la página 8), los adversarios utilizan la ruta más simple disponible para determinar cómo y dónde tendrán éxito los kits de aprovechamiento de vulnerabilidades. Elijen productos que presentan más oportunidades de área de ataque; estas oportunidades generalmente se generan a través del uso de software obsoleto o sin parches. Por ejemplo, la revisión de aplicaciones sigue siendo un desafío dado que hay muchos sistemas que aún son vulnerables a los ataques de SSL Poodle.[5] En función de las tendencias observadas, Cisco Security Research insinúa que la proliferación de versiones obsoletas de software aprovechables seguirá liderando los problemas de seguridad de gran magnitud.

Cisco Security Research utilizó motores de detección para examinar los dispositivos conectados a Internet y el uso de OpenSSL. El equipo determinó que el 56% de los dispositivos sondeados utilizó versiones de OpenSSL con más de 50 meses. Esto significa que, a pesar de la publicidad dada a Heartbleed[6], la brecha de seguridad en el manejo de la seguridad de la capa de transporte (TLS) descubierta en 2014 y la necesidad urgente de actualizar a la última versión el software OpenSSL para evitar dichas vulnerabilidades, las organizaciones no garantizan la ejecución de las versiones más recientes. La Figura 8 muestra el año de las versiones de OpenSSL.

Figura 8. Año de la versión de OpenSSL



Fuente: Cisco Security Research

Posibles soluciones: revisiones y actualizaciones automáticas

El mayor uso de actualizaciones automáticas puede ser una solución para el problema de software desactualizado. Cisco Security Research examinó los datos de los dispositivos conectados en línea que utilizan el navegador Chrome o IE. Los datos revelaron que el 64% de las solicitudes de Chrome se origina a partir de la última versión de dicho navegador. Respecto de los usuarios de IE, solo el 10% de las solicitudes se origina a partir de la última versión.

Cisco Security Research sugiere que es posible que el sistema de actualización automática de Chrome sea más exitoso para garantizar que la mayor cantidad de usuarios posible tenga la versión más reciente del software. (Además, es posible que los usuarios de Chrome sean técnicamente más competentes que los usuarios de IE y, por lo tanto, más propensos a actualizar sus navegadores e instalar actualizaciones).

Cuando se combina con la disminución del aprovechamiento de vulnerabilidades de Java, la investigación indica claramente que el software que instala sus propias actualizaciones de manera automática parece tener una ventaja dado que brinda un marco de seguridad más efectivo. A fin de superar el riesgo eventual garantizado que surge de los procesos de actualización manual, es momento de que las organizaciones acepten la incompatibilidad y la falla ocasional que representan las actualizaciones automáticas.

Informe de riesgo de los sectores de la industria: los objetivos de los adversarios y las prácticas negligentes de los usuarios son una potente combinación para las compañías en sectores de alto riesgo

La industria química y farmacéutica surgió como el principal sector de alto riesgo de exposición a malware basado en la web en 2014. En la primera mitad del año, la industria de las editoriales y los medios de comunicación ocuparon el primer puesto, pero descendió al segundo puesto en noviembre. Completan los cinco primeros puestos las industrias de fabricación, transporte, navegación y aviación, respectivamente. Todos estos sectores se ubicaron en los cinco primeros puestos durante la primera mitad de 2014.

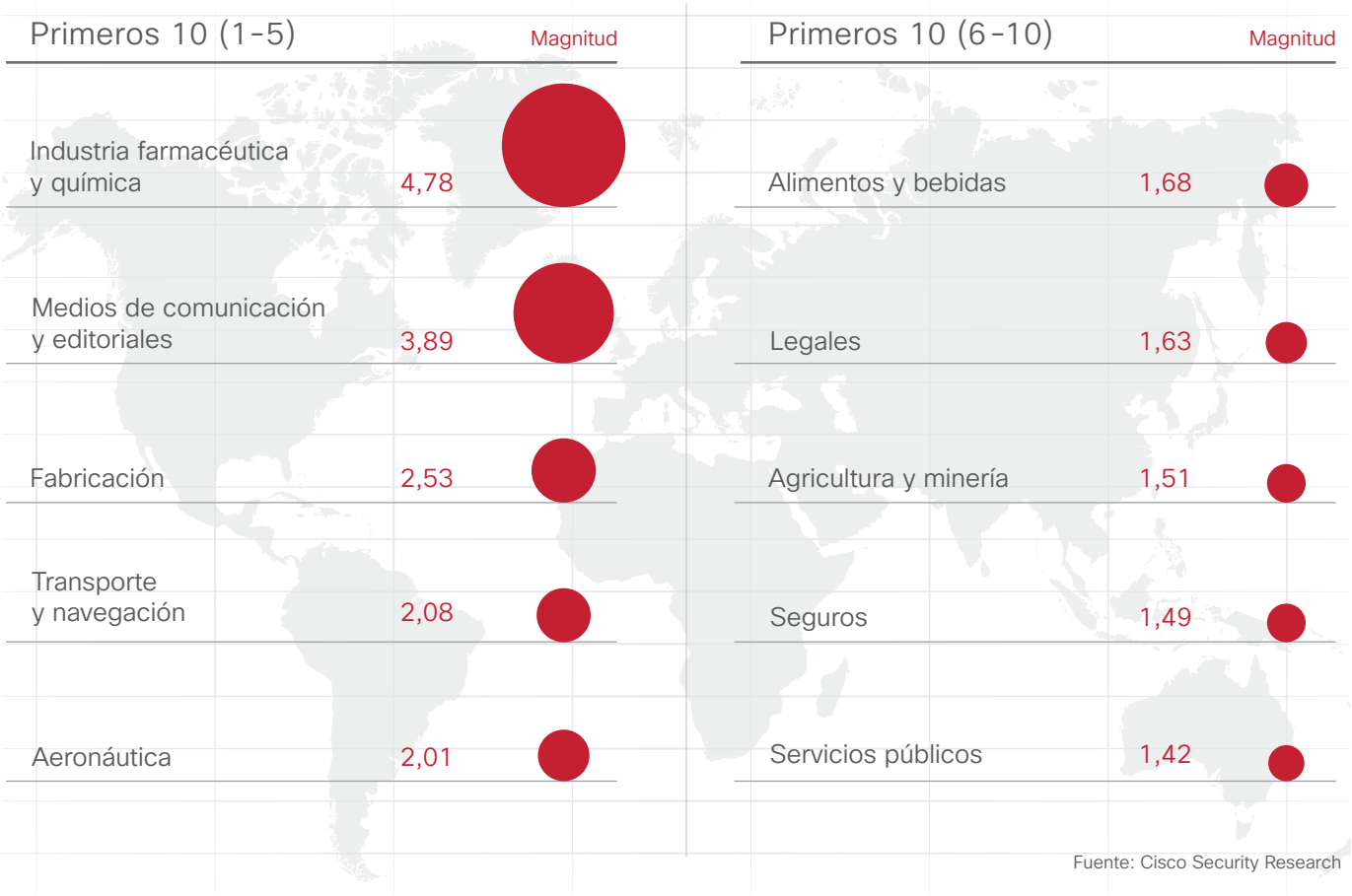
Aunque cabe esperar que el sector minorista tenga una clasificación más alta en esta lista debido a recientes ataques de alto perfil que han plagado a la industria, son los hallazgos maliciosos, y no las brechas reales, los que generan las clasificaciones.

Para determinar los índices de hallazgo de malware específicos de un sector, Cisco Security Research compara el índice mediano de hallazgo correspondiente a todas las organizaciones que utilizan Cisco Cloud Web Security con el índice mediano de hallazgo correspondiente a todas las compañías de un sector específico que utiliza el servicio (Figura 9). Un índice de hallazgo de la industria superior al 1% refleja un riesgo más alto que lo normal de hallazgos de malware basado en la web, mientras que un índice inferior al 1% refleja un riesgo menor. Por ejemplo, una compañía con un índice de hallazgo del 1,7% tiene un riesgo del 70% por encima de la mediana. En cambio, una compañía con un índice de hallazgo del 0,7% tiene un riesgo del 30% por debajo de la mediana.

Hallazgo frente a Riesgo

Un “hallazgo” es una instancia donde se bloquea malware. A diferencia de un “riesgo”, el usuario no se infecta durante el hallazgo porque no se descarga ningún código binario.

Figura 9. Riesgo vertical de hallazgos de malware basado en la web, todas las regiones, del 1.º de enero al 15 de noviembre de 2014



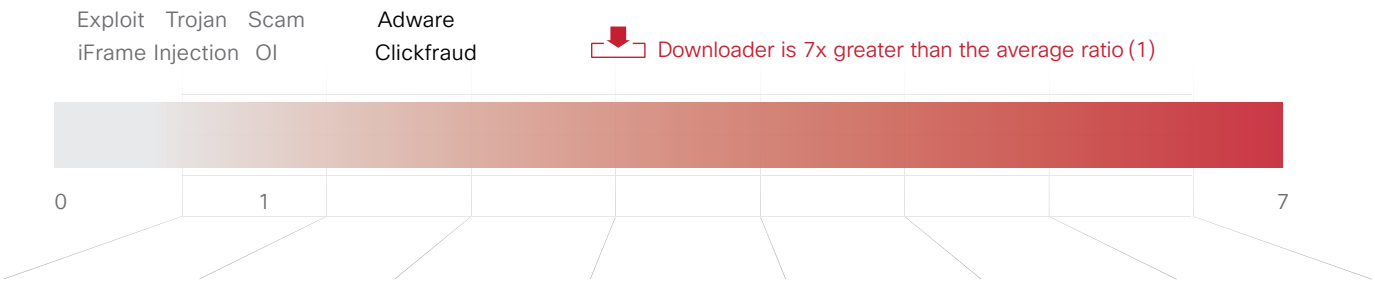
Fuente: Cisco Security Research

Cisco Security Research examinó ocho tipos de métodos de ataque (Figura 10) para determinar si los objetivos de los adversarios o el uso que se hace de la Web fueron el factor clave del aumento de riesgo del sector de la industria respecto de los hallazgos de malware. Se encontraron con una situación catastrófica, dado que la combinación de métodos de ataque dirigidos y comportamientos de usuarios negligentes en línea afecta el nivel de riesgo.

Para determinar si realmente había una diferencia entre los comportamientos de usuarios verticales de alto y bajo riesgo, Cisco Security Research analizó cuatro tipos de métodos de ataque no dirigidos que los usuarios normalmente confrontan al navegar por Internet: adware, clics fraudulentos, estafas e inserciones de IFrame. El equipo también analizó cuatro tipos de métodos de ataque más avanzados que los adversarios frecuentemente emplean en las campañas dirigidas: kits de aprovechamiento de vulnerabilidades, troyanos, OI (detección de malware) y descargadores.

Nota: los ocho métodos de ataque han sido categorizados por Cisco Security Research en depósitos heurísticos.

Figura 10. Métodos de ataque de malware basado en la web: comparación de los primeros cuatro y los últimos cuatro sectores de alto riesgo



Fuente: Cisco Security Research

Teniendo en cuenta los primeros cuatro y los últimos cuatro sectores más expuestos al malware, conforme a los datos de Cisco Cloud Web Security, Cisco Security Research tomó los porcentajes de incidentes de cada tipo de método de ataque y generó índices promedio de los primeros cuatro y los últimos cuatro sectores. La comparación que se muestra en la Figura 10 se obtuvo dividiendo los promedios más altos por los promedios más bajos. Una relación de uno indica que se observaron los mismos patrones de actividad entre los grupos más y menos focalizados.

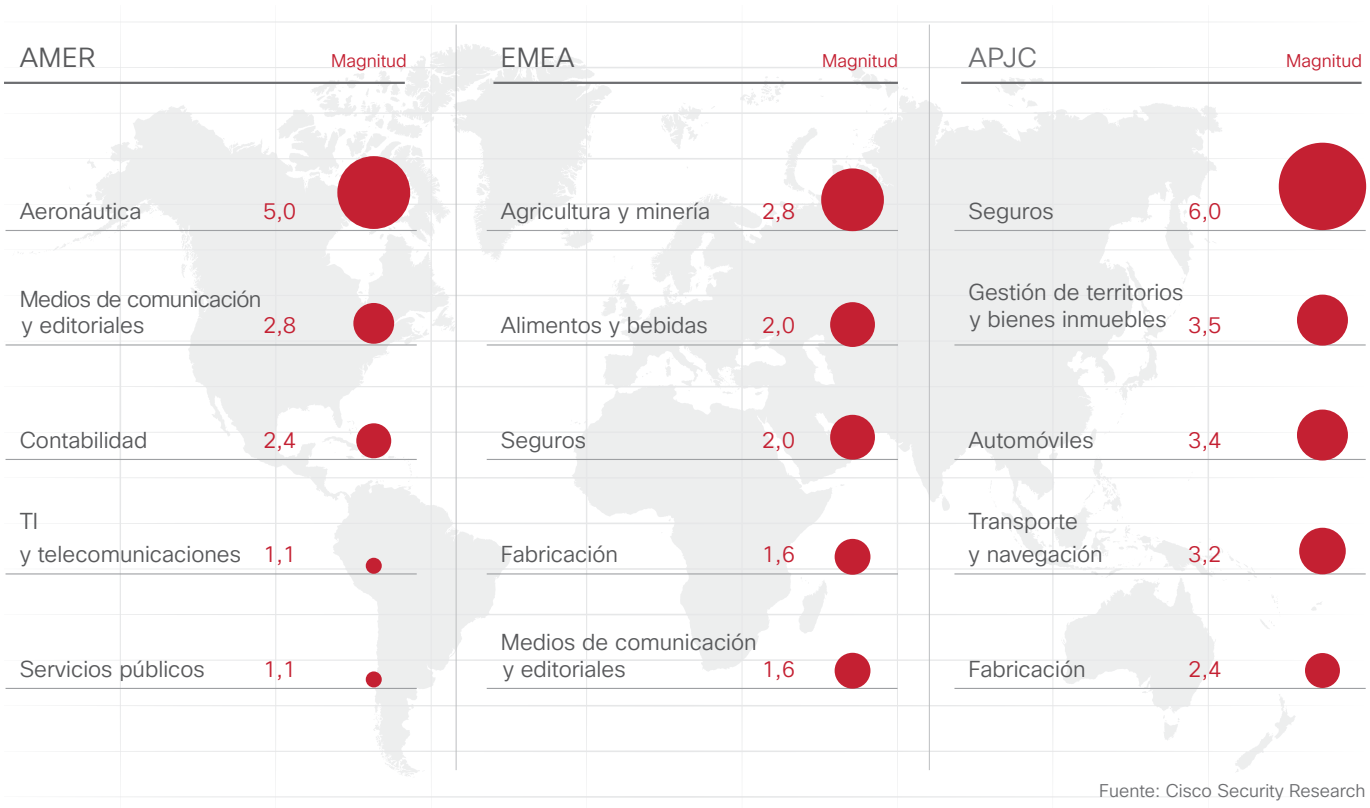
Los datos muestran que los sectores de alto riesgo de la industria se encuentran frente a métodos de ataque de descargadores sofisticados con una frecuencia siete veces mayor que los últimos cuatro sectores de alto riesgo de la industria. Esto es consecuente con lo previsto si se adoptan métodos de ataque dirigidos contra los sectores de mayor riesgo.

El índice de hallazgo de clics fraudulentos y adware también es superior en los sectores de alto riesgo de la industria más focalizados en comparación con los sectores de menor riesgo menos focalizados. Esto sugiere que la diferencia puede ser más compleja que ser simplemente el objetivo de los protagonistas malintencionados. El comportamiento de los usuarios también puede verse implicado en la creciente exposición al malware, posiblemente a través de las diferencias entre cómo los usuarios utilizan Internet y sus hábitos de navegación, y en consecuencia contribuye a la mayor frecuencia de hallazgos de métodos de ataque de malware basado en la web en los sectores de alto riesgo de la industria. Además, los usuarios de las industrias donde se fomenta y necesita la rápida adopción de nuevos medios de competencia e innovación posiblemente se encuentran frente a métodos de ataque de malware basado en la web con mayor frecuencia que los usuarios de otras industrias, como el gobierno, donde el uso de Internet está más limitado o estrictamente controlado.

Por ejemplo, Cisco Security Research sugiere que, debido a que los usuarios de la industria de las editoriales y los medios de comunicación generalmente utilizan Internet con más frecuencia, corren el riesgo de enfrentarse a vulnerabilidades de seguridad web más seguido que los usuarios de otros sectores de la industria.

Nota: en 2014, la industria de las editoriales y los medios de comunicación experimentó índices de hallazgo de malware basado en la web significativamente superiores a los normales en comparación con los observados anteriormente por Cisco Security Research, recopilados en estos datos desde 2008. La exposición de los usuarios a publicidad malintencionada más generalizada en sitios web legítimos puede contribuir a este aumento.

Figura 11. Sectores de mayor riesgo de exposición a malware en AMER, APJC y EMEA



Fuente: Cisco Security Research

Hallazgos de malware por región

A continuación se presentan los datos de riesgo de los hallazgos de malware basado en la web para los sectores de alto riesgo de la industria por región. Las tres regiones se definen de la siguiente manera:

- Norteamérica, Centroamérica y Latinoamérica (AMER)
- Asia Pacífico, China, Japón y la India (APJC)
- África, Europa y Oriente Medio (EMEA)

Cisco Security Research identificó los sectores de mayor riesgo de la industria ubicados en todo el mundo (consulte las industrias enumeradas en la Figura 11) y determinó que:

- Los usuarios de la industria de los seguros en APJC son seis veces más propensos a quedar expuestos al malware en comparación con los 12 sectores examinados en las tres regiones. (Base de referencia: 1,5).
- Los usuarios de la industria de la aviación en AMER son cinco veces más propensos a quedar expuestos al malware.
- Los usuarios de la industria de gestión de territorios y bienes inmuebles en APJC, y los usuarios de la industria automotriz de dicha región, son 3,5 veces más propensos a quedar expuestos al malware.
- Los usuarios de la industria del transporte y la navegación en APJC son 3,25 veces más propensos a quedar expuestos al malware.

Cisco Security Research cita los altos precios de los terrenos y las viviendas, los últimos desastres naturales y la gran actividad de fabricación y exportación en APJC como los factores que utilizan los adversarios para apuntar a los usuarios de dicha región que trabajan o realizan negocios en las industrias automotriz, de seguros, gestión de territorios y bienes inmuebles, transporte y de navegación. El robo de datos de los clientes, propiedad intelectual (incluidos objetivos de estados nacionales) y cargas aéreas se encuentra entre las motivos principales para apuntar a los usuarios de la industria de la aviación en AMER.

Más métodos de ataque para la distribución de malware por región

Las Figuras 12a a 12c revelan las técnicas que utilizan con más frecuencia los adversarios para distribuir malware por región. Los resultados de estos gráficos se basan primordialmente en los sitios en los que se registraron bloqueos de malware basado en la web (es decir, hallazgos), según los datos de Cisco Cloud Web Security frente a los tipos de amenazas en la red.

Durante el 2014, los usuarios en AMER fueron los principales destinatarios de scripts malintencionados; las inserciones de IFrame ocuparon un distante segundo lugar. En APJC, los adversarios han dependido mucho de las estafas, los scripts malintencionados y el aprovechamiento de vulnerabilidades basado en la web durante el último año para poner en riesgo a los usuarios de todos los sectores. Y en EMEA, el aprovechamiento de vulnerabilidades basado en la web prevalece especialmente.

Lea la entrada de blog de Cisco Security: "Amenaza destacada: Grupo 72" para obtener información sobre el papel que desempeña Cisco Security Research en la identificación y la interrupción de las actividades de un grupo de protagonistas que amenaza a organizaciones individualizadas de alto perfil que cuentan con propiedad intelectual de gran valor en los sectores de producción, industriales, aeroespaciales, de defensa y medios de comunicación.

Para obtener detalles sobre la herramienta de administración remota (RAT) que utiliza Grupo 72 para llevar a cabo el espionaje cibernético, lea la entrada: "Amenaza destacada: Grupo 72, apertura de ZxShell".

Figura 12a. Distribución de métodos de ataque, AMER

Método de ataque	% total
Script	24,93%
Inserciones de iFrame	17,43%
Aprovechamiento de vulnerabilidades	13,63%
OI (detección de malware)	10,35%
Troyano	10,06%

Fuente: Cisco Security Research

Figura 12b. Distribución de métodos de ataque, APJC

Método de ataque	% total
Estafa	25,26%
Script	25,04%
Inserciones de iFrame	18,68%
OI (detección de malware)	9,93%
Aprovechamiento de vulnerabilidades	6,72%

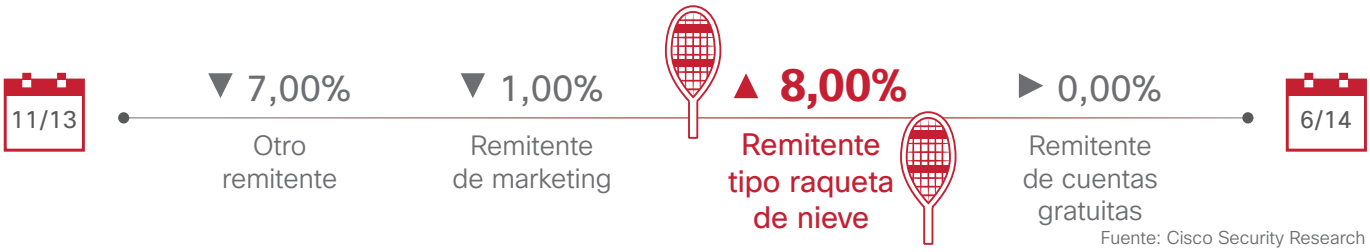
Fuente: Cisco Security Research

Figura 12c. Distribución de métodos de ataque, EMEA

Método de ataque	% total
Inserciones de iFrame	51,48%
Script	15,17%
Aprovechamiento de vulnerabilidades	8,64%
Estafas	7,31%
OI (detección de malware)	4,16%

Fuente: Cisco Security Research

Figura 13. Spam de remitentes tipo raqueta de nieve en aumento



Fuente: Cisco Security Research

Actualización de spam: los piratas informáticos adoptan la estrategia "Snowshoe"

El robo de identidad es aún útil como herramienta para los delincuentes para distribuir malware y robar credenciales porque los usuarios siguen siendo presa de tácticas de spam conocidas. Los atacantes son conscientes de que es más fácil aprovecharse de los usuarios a nivel del navegador y el correo electrónico en lugar de poner en riesgo a los servidores, lo que significa que los piratas informáticos se siguen innovando.

No es inusual ver que un sistema anti-spam captura más del 99% del spam que filtra. La mayoría de los mejores sistemas anti-spam captura más del 99,9% del spam. En este entorno, los piratas informáticos intentan casi cualquier cosa con tal de evadir los filtros de spam. Para asegurarse de que el spam llega a la audiencia objetivo, los piratas informáticos utilizan cada vez más estas tácticas a fin de evitar la detección de tecnologías de reputación anti-spam basada en IP.

Ingreso de spam tipo raqueta de nieve (snowshoe): la comparación es oportuna porque las raquetas de nieve permiten que las personas caminen sobre la nieve profunda y distribuir el peso sobre una superficie de mayor tamaño; de esta manera, se impide que el pie de la persona se hunda. El spam tipo raqueta de nieve consta del envío de correo electrónico masivo no solicitado mediante una gran cantidad de direcciones IP y mensajes de poco volumen por dirección IP, lo que impide que algunos sistemas de spam hundan el spam. La Figura 13 resalta el aumento del spam tipo raqueta de nieve de 2013 a 2014.

En una campaña reciente de spam tipo raqueta de nieve observada por Cisco Security Research, se utilizó el enfoque de campaña intensiva. Esto quiere decir que la campaña completa de spam se llevó a cabo en tres horas, pero en un punto significó el 10% del tráfico de spam global (Figura 14).

Para obtener más información sobre el spam tipo raqueta de nieve, consulte la entrada de blog de Cisco Security: "El ataque de spam tipo raqueta de nieve va y viene como una ráfaga".

Los mensajes tipo raqueta de nieve examinados por los investigadores de Cisco muestran características estándar de spam. Por ejemplo, tienen líneas de asunto mal escritas, como "fatcura 2921411.pdf", e incluyen números generados al azar. Los adjuntos son generalmente archivos PDF que contienen un troyano que se aprovecha de una vulnerabilidad de Adobe Reader.

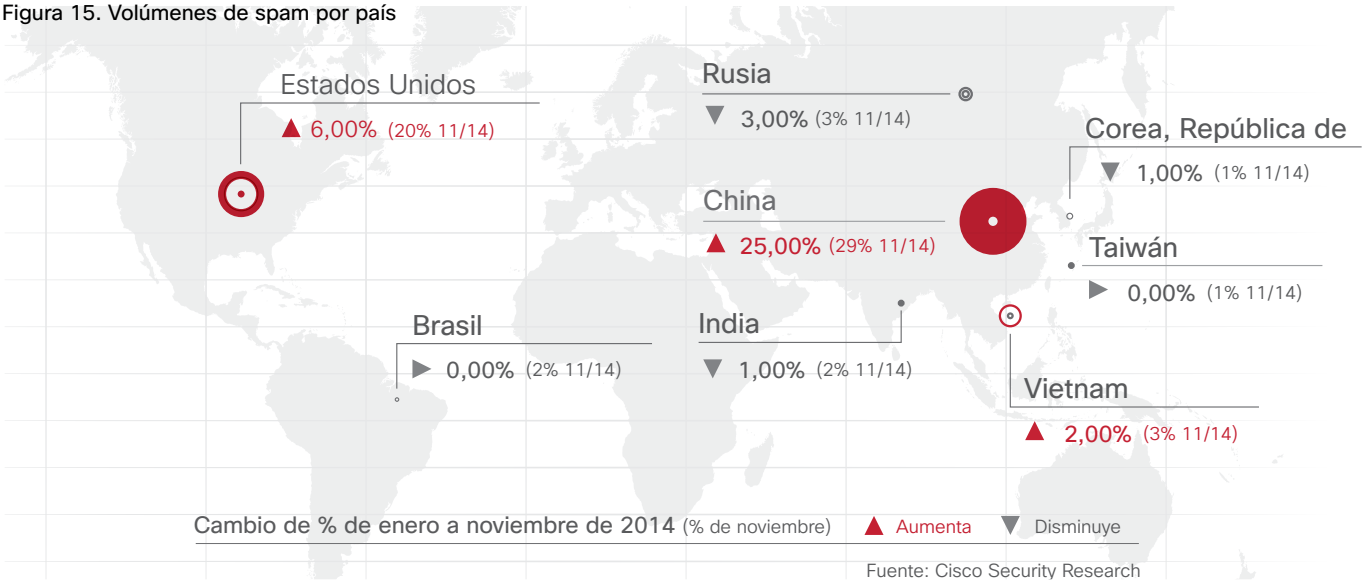
Figura 14. Incidente de campaña de spam tipo raqueta de nieve

Fuente: Cisco Security Research

Para mitigar el spam tipo raqueta de nieve, los profesionales de seguridad no pueden solo confiar en las soluciones basadas en la reputación, dado que los mismos mensajes de una campaña pueden originarse en cientos o incluso miles de sitios en el caso de las campañas derivadas de botnets. Examinar otras características del spam, como la higiene del servidor de correo electrónico, puede brindar una detección más precisa. Por ejemplo, en las campañas observadas por Cisco Security Research, muchas de las direcciones IP carecen de sistemas de nombres de dominios (DNS) directos e inversos equivalentes, lo que normalmente se considera un indicador obvio de ilegitimidad del servidor de correo electrónico.

Muchas de estas direcciones IP además carecen de registros de envío de correos electrónicos anteriores al inicio de la campaña tipo raqueta de nieve, lo que además indica que los delincuentes en línea utilizan máquinas en riesgo para crear una infraestructura para el spam tipo raqueta de nieve.

Figura 15. Volúmenes de spam por país



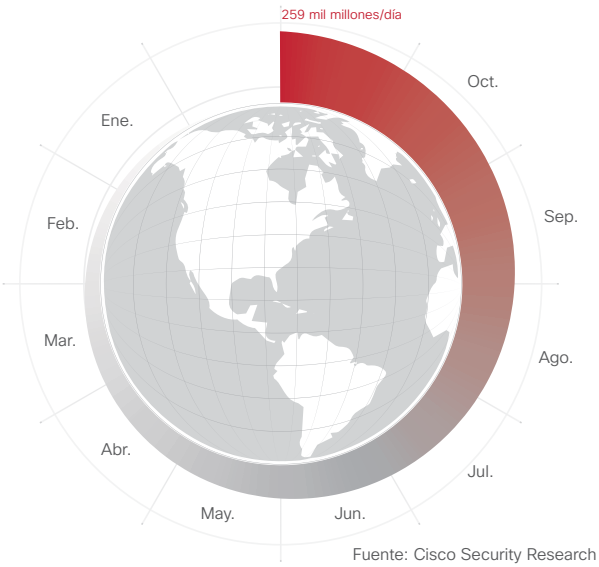
Fuente: Cisco Security Research

Los piratas informáticos expanden sus tácticas para aventajar a los consumidores

Los volúmenes de spam en todo el mundo están en aumento, esto indica que el spam sigue siendo un vector lucrativo para los delincuentes en línea (Figura 16). Los adversarios continúan perfeccionando los mensajes a fin de que el spam tenga más probabilidad de engañar a los destinatarios para que hagan clic en los enlaces peligrosos, con frecuencia mediante tácticas de ingeniería social.

Aunque los volúmenes de spam han disminuido en líneas generales en los Estados Unidos en 2014, los niveles aumentaron en otros países durante el mismo período (Figura 15). Cisco Security Research sugiere que esto indica que los protagonistas malintencionados están cambiando su base de operaciones. El aumento de los volúmenes de spam en ciertos países puede además ser un signo de que otras regiones están alcanzando a los Estados Unidos en términos de producción de spam, dado que dicho país ha sido durante mucho tiempo una fuente principal de spam en todo el mundo. Al fin y al cabo, Estados Unidos terminó el año en primer lugar.

Figura 16. Aumento internacional del volumen de spam en 2014



Fuente: Cisco Security Research

Los mensajes de robo de identidad individualizados, un elemento básico de los delincuentes en línea durante años, han evolucionado hasta el punto de que incluso los usuarios finales experimentados han tenido dificultad para detectar mensajes falsos entre los correos electrónicos auténticos. Estos mensajes, que apuntan a individuos específicos con un mensaje bien elaborado, parecen derivar de proveedores de servicios o proveedores reconocidos de quienes los usuarios comúnmente reciben mensajes; por ejemplo, servicios de entrega, sitios de compras en línea y proveedores de música y entretenimiento. Los correos electrónicos con un nombre y un logotipo de confianza, aunque sean falsos, tienen más peso que los mensajes de spam tradicionales que importunan a la industria farmacéutica o de relojes. Y si los mensajes poseen un llamado a la acción conocido para los destinatarios, como un aviso sobre un pedido reciente o un número de seguimiento de entrega, incitan a los usuarios a hacer clic en los enlaces contenidos en el correo electrónico.

Cisco Security Research recientemente observó una pequeña cantidad de mensajes de robo de identidad individualizados que pretendía originarse desde Apple Inc. con el pretexto de que los destinatarios habían descargado un popular juego para dispositivos iOS móviles. La línea de asunto del correo electrónico incluía un número de recibo generado al azar, otro aparente detalle auténtico, dado que los correos electrónicos legítimos usualmente contienen dicho número. Un enlace en el mensaje sugería a los destinatarios iniciar sesión y modificar las contraseñas si aún no habían iniciado la descarga del juego, dicho enlace redirigía a los usuarios a un conocido sitio web de robo de identidad.

Los piratas informáticos transforman los mensajes para evadir la detección

Cuando los piratas informáticos descubren una fórmula exitosa (es decir, son capaces de convencer a los usuarios para que hagan clic en los enlaces del spam o compren productos falsos), retocan los mensajes para que su estructura básica siga siendo la misma. Pero dichos mensajes son lo suficientemente diferentes como para evadir los filtros de spam, al menos por un tiempo. En la Tabla 2, los investigadores de Cisco llevaron la cuenta de la cantidad de veces que los piratas informáticos intentaron modificar el contenido de un mensaje para evadir la mitigación constante durante un período deprueba. La tabla enumera las amenazas que requirieron la modificación de las reglas del dispositivo de seguridad de correo electrónico (ESA) de Cisco.

Tabla 2. Alertas de epidemias de amenazas: amenazas de robo de identidad y spam más persistentes

ID de IntelliShield	Título	Versión	Urgencia	Credibilidad	Gravedad
24986	Alerta de epidemias de amenazas: notificación de envío falso de FedEx	95			
31819	Alerta de epidemias de amenazas: correo electrónico de envío de mensaje de fax falso	88			
30527	Alerta de epidemias de amenazas: imágenes de personal maliciosas adjuntas	81			
36121	Alerta de epidemias de amenazas: cancelación de pago electrónico falsa	80			
23517	Alerta de epidemias de amenazas: mensaje de correo electrónico de pedido de producto falso	79			
23517	Alerta de epidemias de amenazas: extracto de factura falso adjunto	78			
27077	Alerta de epidemias de amenazas: notificación de transferencia de dinero falsa	78			
26690	Alerta de epidemias de amenazas: notificación de transferencia de pago bancario falsa	78			

Fuente: Cisco Security Research

Publicidad malintencionada de complementos del navegador: causa daños menores a cada usuario para obtener grandes recompensas

Cisco Security Research recientemente realizó un análisis profundo de una amenaza basada en la web que utiliza publicidad malintencionada (malvertising) de complementos del navegador web como medio de distribución de malware y aplicaciones no deseadas. El grupo descubrió que la amenaza tenía características básicas semejantes al comportamiento de un botnet. En la investigación del equipo, que incluyó la evaluación de la actividad de más de 800 000 usuarios de 70 compañías del 1 de enero al 30 de noviembre de 2014, Cisco Security Research midió el tamaño general de la amenaza y corroboró su intención y estructura.

El análisis reveló que esta familia de complementos del navegador es mucho más amplia de lo esperado y que los creadores de malware utilizan una combinación de un código escrito de manera profesional altamente sofisticado y un modelo empresarial perfeccionado para que la operación del malware siga siendo rentable a largo plazo. En otras palabras, no es necesario controlar por completo el host focalizado para tener una rentabilidad exitosa. Esto genera una mayor incidencia de malware deliberadamente diseñado para tener un bajo impacto en el host afectado y optimizado para una rentabilidad a largo plazo sobre una gran población afectada.

Los usuarios en riesgo se infectan con estos complementos maliciosos del navegador mediante la instalación del paquete de software (software distribuido con otro producto o paquete de software), generalmente sin su consentimiento expreso. Los usuarios instalan voluntariamente aplicaciones tales como herramientas PDF o reproductores de video descargados de fuentes poco confiables bajo la creencia de que son legítimas.

Estas aplicaciones pueden estar "incluidas" dentro de software malicioso no deseado. Este enfoque de distribución de malware sigue un esquema de rentabilidad de pago por instalación (PPI), en que la persona que publica recibe un pago por la instalación de cada paquete de software incluido en la aplicación original.

Muchos usuarios confían intrínsecamente en los complementos o simplemente los consideran benignos, lo que hace que este enfoque de distribución de malware sea exitoso para los protagonistas malintencionados. Este método de distribución de malware permite a los adversarios disminuir su dependencia de otras técnicas, como los kits de aprovechamiento de vulnerabilidades, que son más fáciles de detectar. (Consulte "Vulnerabilidades de seguridad web: para los creadores de kits de aprovechamiento de vulnerabilidades, ocupar el primer lugar no implica ser los mejores" en la página 7).

Cisco Security Research observó que el tráfico web generado por esta familia de complementos del navegador tiene características específicas y puede identificarse mediante dos patrones bien definidos. La cadena de consulta normalmente contiene datos cifrados en los que se exfiltra información tal como el nombre del complemento y la URL anteriormente visitada por el usuario (incluidos enlaces de la intranet).

Durante este análisis, Cisco Security Research encontró más de 4000 nombres de complementos diferentes, entre ellos, PassShow, Bettersurf, Bettermarkit y algoritmos de hash seguros (SHA) asociados (bee4b83970ffa8346f0e791be92555702154348c14bd8 a1048abaf5b3ca049e35167317272539fa0dece3ac1a60 10c7a936be8cbf70c09e547e0973ef21718e5). Debido a que puede utilizarse más de un nombre de complemento por instalación, es muy difícil seguir el malware (Figura 17).

Figura 17. Actividad de amenazas y flujo de infección

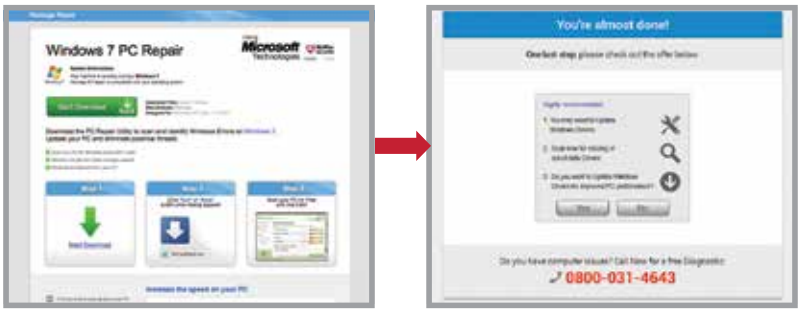
Fuente: Cisco Security Research

El malware detecta los tipos de SO y distribuye los kits de aprovechamiento de vulnerabilidades correspondientes

Los investigadores de seguridad de Cisco observaron que los complementos maliciosos analizados mostraban cierto tipo de publicidad en función de la "huella digital" de navegador del usuario. Las publicidades insertadas para los usuarios de Linux generalmente son sobre sitios de juegos en línea. Los usuarios que tienen instalado Microsoft IE son redirigidos a anuncios que generan la descarga de software aparentemente legítimo, que en realidad es malicioso.

Linux

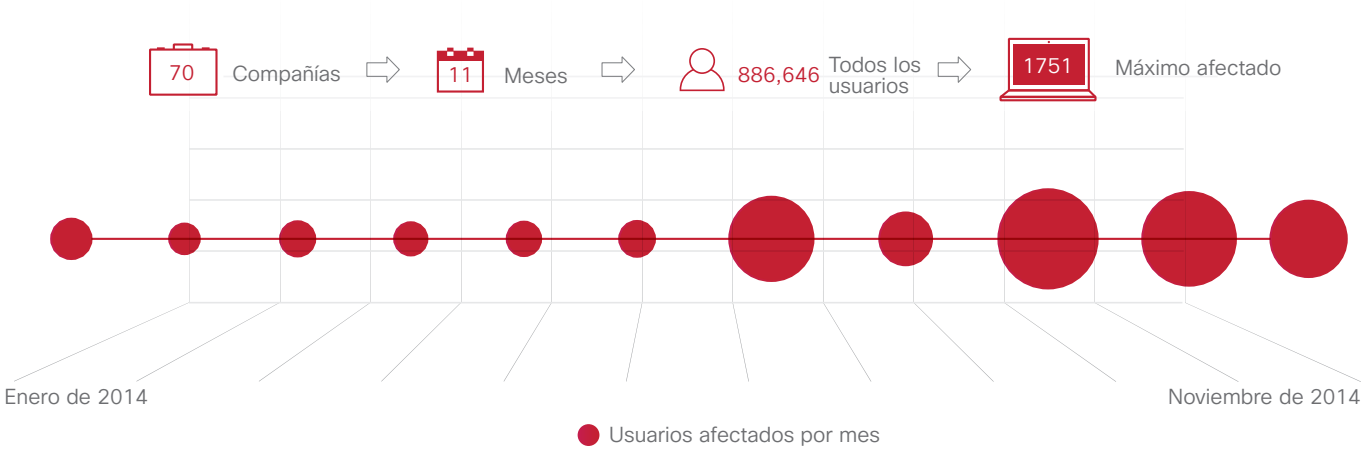
Microsoft IE



En función del análisis de 11 meses de actividad de los usuarios de 70 compañías, la cantidad de usuarios afectados por esta amenaza ha aumentado. En enero, 711 usuarios fueron afectados pero, en la segunda mitad del año, la cantidad de usuarios afectados superó los 1000, con un pico de 1751 en septiembre (Figura 18). Uno de los motivos de este importante aumento en septiembre y octubre puede haber sido el incremento de la actividad en línea de las personas que regresaban de las vacaciones de verano.

Mediante la investigación, los expertos en seguridad de Cisco descubrieron que los adversarios emplean varios servidores diferentes para respaldar sus campañas de malware. Esto significa que una organización de delincuentes cibernéticos especializada en el mantenimiento de actividades segmentadas es responsable de la amenaza o un "proveedor de tecnología" vende su producto a varios grupos. No obstante, el responsable de la distribución de malware parece estar intentando crear un botnet de tamaño considerable.

Figura 18. Cantidad de usuarios afectados por mes, de enero a noviembre de 2014



Fuente: Cisco Security Research

Cisco Security Research además encontró más de 500 dominios únicos asociados a esta amenaza, 24 de los cuales están por debajo del millón de dominios principales de la clasificación de Alexa. Muchos son también dominios con una clasificación relativamente elevada (Figura 19). Esto significa que son dominios populares pero muy peligrosos para que los usuarios los visiten debido al riesgo de compromiso.

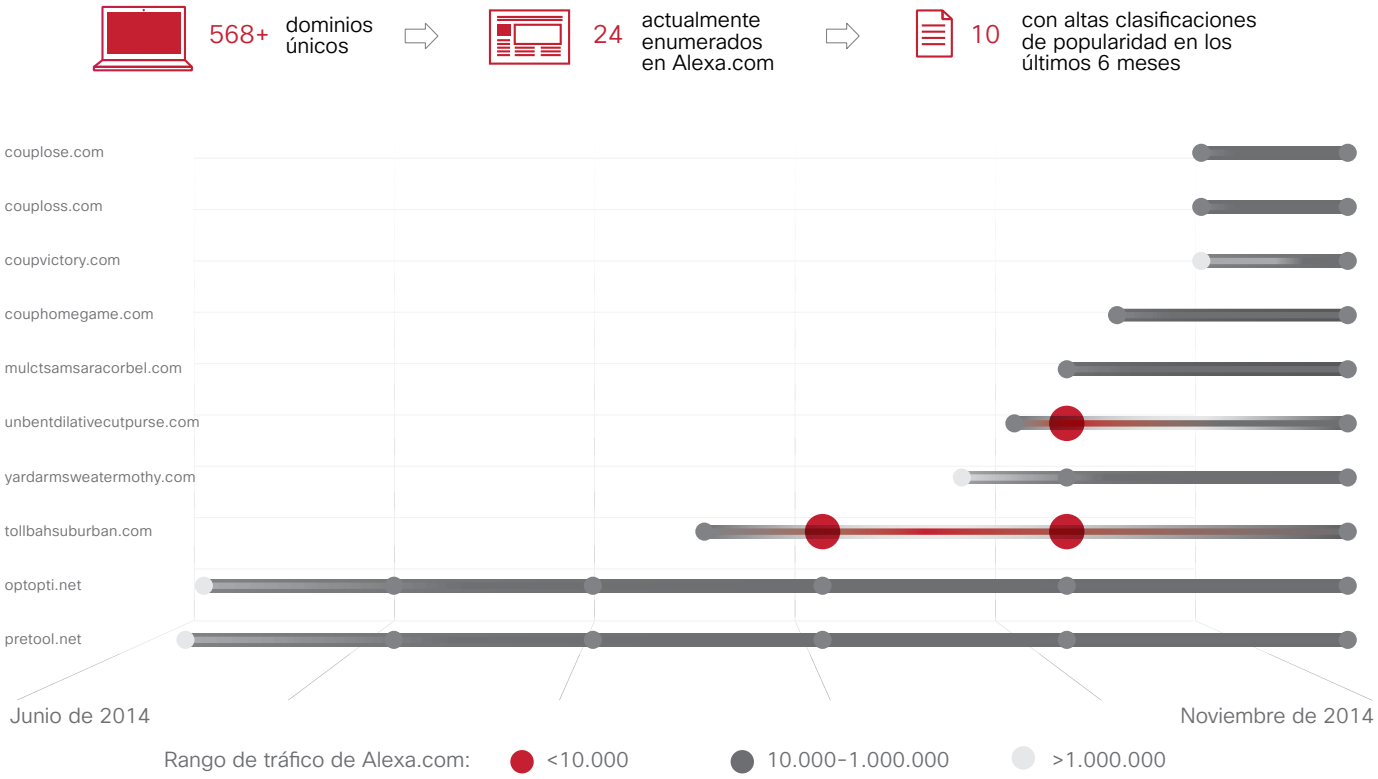
Algunos de estos dominios han estado activos por más de un año, pero la mayoría tiene un ciclo de vida más corto de solo unas semanas en la mayoría de los casos (Figura 19). Todos los dominios comparten una característica: se vuelven populares demasiado pronto.

Sugerencias de prevención y corrección

Para evitar verse comprometidos por el esquema de complementos del navegador o abordar una infección existente, los usuarios deben seguir estas sugerencias:

- Se deben descargar las aplicaciones de fuentes confiables.
- Se debe anular la selección de software no deseado en los paquetes de instalación.
- Se deben utilizar análisis de amenazas, tecnologías en modo seguro y tecnologías de seguridad web para prevenir y detectar este tipo de amenaza.
- Si es posible, se deben eliminar manualmente los complementos y utilizar herramientas antispyware para limpiar los programas no deseados.

Figura 19. Dominios populares utilizados por la publicidad malintencionada en el esquema de complementos del navegador clasificados por Alexa



Fuente: Cisco Security Research

2. Estudio comparativo de capacidades de seguridad de Cisco

Para evaluar las percepciones de los profesionales de seguridad respecto del estado de la seguridad en las organizaciones, Cisco consultó a jefes de seguridad de la información (CISO) y gerentes de operaciones de seguridad (SecOps) de varios países y organizaciones de diferente tamaño sobre sus procedimientos y recursos de seguridad. El *Estudio comparativo de capacidades de seguridad de Cisco,* completado en octubre de 2014, presenta las perspectivas del nivel de sofisticación de las actuales operaciones de seguridad y prácticas de seguridad en uso.

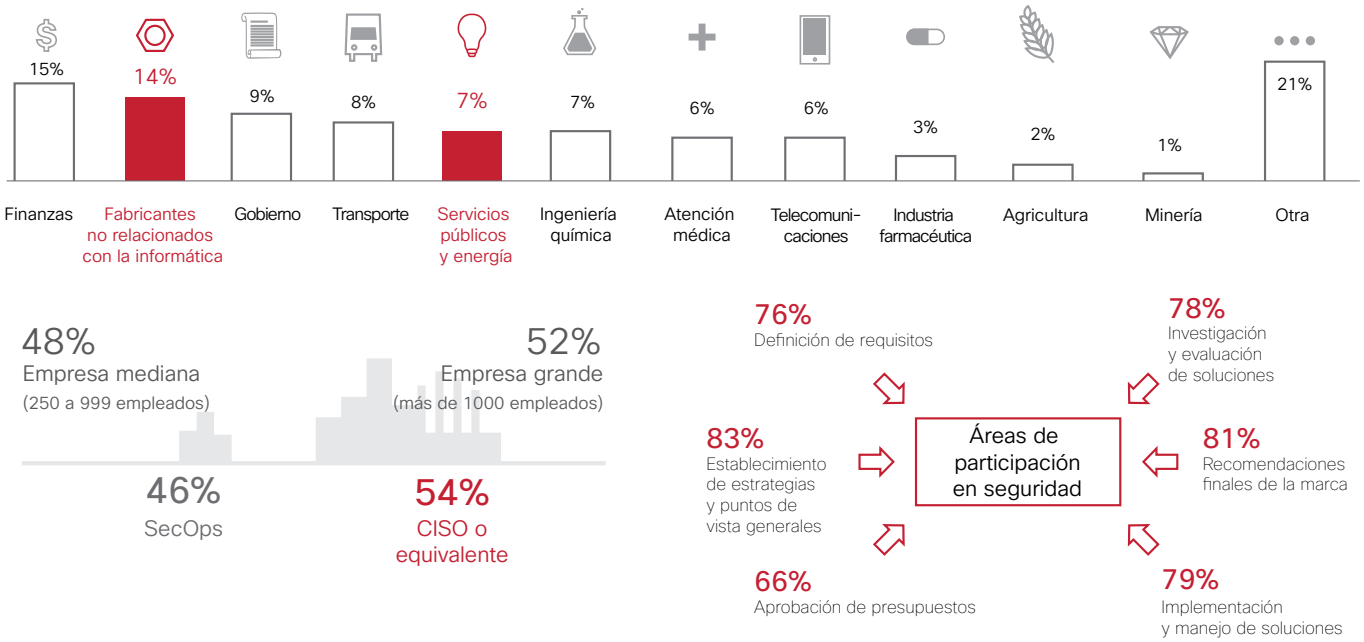
Capacidades de seguridad de Cisco: ¿Están a la altura las organizaciones?

¿Cómo ven los profesionales de seguridad empresarial la preparación de las organizaciones para manejar las brechas de seguridad? La respuesta depende del papel que desempeñan en las organizaciones y las industrias en las que trabajan, conforme al nuevo Estudio comparativo de capacidades de seguridad de Cisco.

La Figura 20 muestra las respuestas de los profesionales por industria y tamaño de la compañía. Los fabricantes no relacionados con la informática y los encuestados de servicios públicos/energía informaron los mayores niveles de conocimiento y participación en seguridad.

C (cantidad de encuestados) = 1738

Figura 20. Perfiles de los encuestados y respuestas ante la brecha de seguridad



Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

El estudio encuestó a los CISO y gerentes de SecOps para conocer los recursos que las compañías utilizan para la seguridad cibernética; los procedimientos, las políticas y las operaciones de seguridad; y el nivel de sofisticación de las operaciones de seguridad cibernética. La buena noticia de la encuesta es que la mayoría de los profesionales de seguridad cree que cuenta con herramientas y procesos vigentes para mantener una seguridad eficaz. Sin embargo, los CISO son notablemente más optimistas que sus colegas de SecOps respecto del estado de la seguridad. Por ejemplo, el 62% de los CISO está totalmente de acuerdo con que los procesos de seguridad de sus organizaciones son claros e inequívocos en comparación con el 48% de los gerentes de SecOps. Los CISO además consideran que los procesos de seguridad son favorables. El 59% de los encuestados está totalmente de acuerdo con que los procesos están optimizados y en que se centrarán en la mejora de dichos procesos en comparación con el 46% de los gerentes de SecOps.

¿Por qué existe esta diferencia entre los niveles de confianza? Probablemente debido al hecho de que los CISO están más alejados de las actividades de seguridad diarias, mientras que el personal de SecOps trabaja en estrecha relación para resolver los incidentes de seguridad mayores y menores. Es posible que el CISO de una gran organización no se dé cuenta de que mil máquinas están infectadas con malware en un día típico, mientras que el gerente de SecOps dedica mucho más tiempo a mitigar la infección; por consiguiente, tiene una visión menos optimista de la seguridad de la organización.

Además, los CISO establecen las políticas, como el bloqueo del acceso a los medios sociales, lo que les concede la ilusión de defensas de seguridad más impenetrables y herméticas. Pero al cerrar dichos canales por completo, quitan a los equipos de seguridad la posibilidad de conocer o experimentar las amenazas que aún existen fuera de sus redes.

Otra diferencia en la confianza surgió cuando se preguntó a los encuestados sobre la fiabilidad de las políticas de seguridad de las organizaciones. Tanto los CISO como los gerentes de SecOps mostraron altos niveles de confianza en las políticas (consulte la Figura 21), aunque demostraron menos confianza en sus capacidades para abarcar y contener los riesgos (consulte la Figura 28).

Una brecha similar surgió cuando se preguntó a los encuestados sobre los controles de seguridad: casi todos los encuestados dijeron que cuentan con buenos controles de seguridad, pero aproximadamente un cuarto considera que las herramientas de seguridad son solo “medianamente” eficaces en lugar de “muy” o “extremadamente” eficaces (consulte la Figura 29).

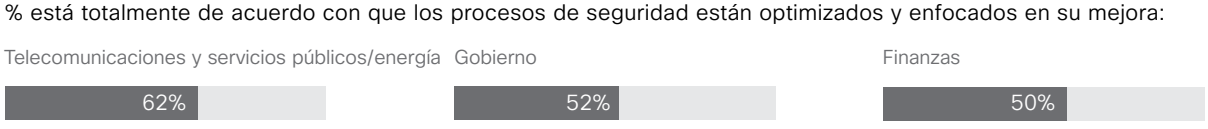
La confianza en las prácticas y los procesos de seguridad también parece variar por industria. Los CISO y gerentes de SecOps de las compañías de servicios públicos/energía y las empresas de telecomunicaciones parecen ser los más confiados, mientras que las organizaciones gubernamentales, farmacéuticas, sanitarias y de servicios financieros parecen ser menos confiados. De hecho, el 62% de los ejecutivos de seguridad de telecomunicaciones y servicios públicos/energía está totalmente de acuerdo con que los procesos de seguridad están optimizados en comparación con el 50% de quienes trabajan en servicios financieros y el 52% que trabaja en el gobierno.

Los profesionales de seguridad de telecomunicaciones y servicios públicos/energía parecen ser los más sofisticados en las prácticas de seguridad, mientras que las organizaciones gubernamentales y de servicios financieros son las menos sofisticadas. Las organizaciones de servicios públicos y energía tienden a contar con procedimientos y procesos bien documentados para el seguimiento de incidentes. Sin embargo, esto no necesariamente significa que están más protegidas que las organizaciones de otras industrias.

Figura 21. Descubrimientos clave por puesto e industria

El 90% de las compañías confía en sus procedimientos, procesos y políticas de seguridad.

No obstante, el 54% ha debido manejar el escrutinio público tras una falla de seguridad.

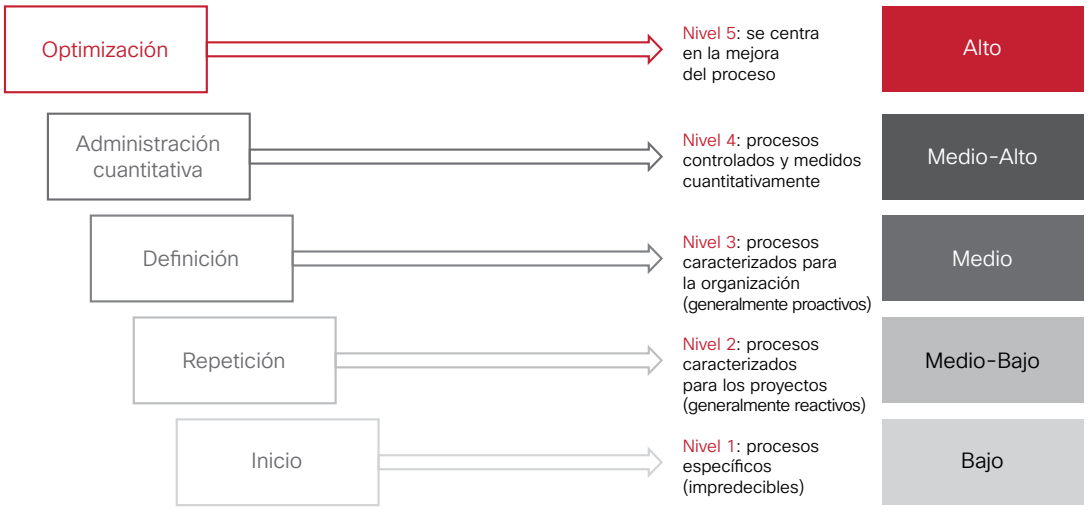


Existen pocas diferencias entre las empresas y las organizaciones medianas que indican que la cantidad de empleados de por sí tiene poco que ver con la sofisticación de la seguridad.

Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Figura 22. Representación de los niveles de sofisticación de la muestra actual

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



Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Signos de sofisticación de la seguridad

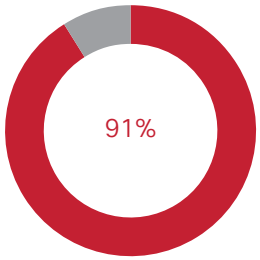
El *Estudio comparativo de capacidades de seguridad de Cisco* además resalta las características de las organizaciones más sofisticadas respecto de sus estados de seguridad. Las características incluyen:

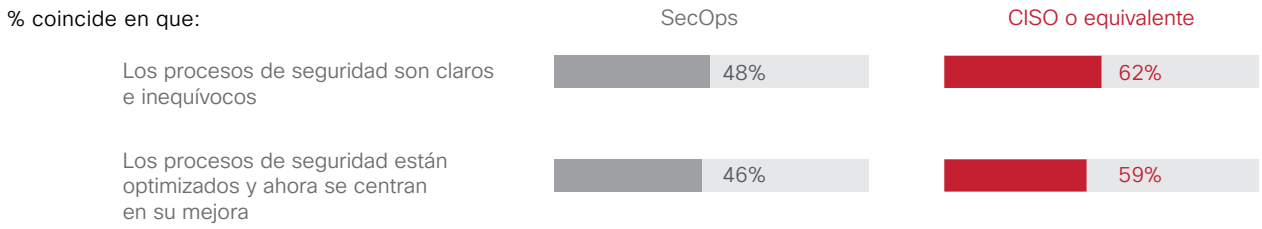
- Liderazgo ejecutivo que prioriza la seguridad.
- Procedimientos y políticas inequívocos bien documentados.
- Herramientas integradas que funcionan en conjunto.

El 91% de los encuestados de compañías sofisticadas está totalmente de acuerdo en que los ejecutivos de las compañías consideran la seguridad como alta prioridad, mientras que solo el 22% de los encuestados de compañías menos sofisticadas concuerda con esta afirmación. Además, el 88% de los encuestados de compañías sofisticadas está totalmente de acuerdo en que los procesos de seguridad son claros e inequívocos en comparación con el 0% de los encuestados de compañías menos sofisticadas.

Figura 23. Descubrimientos clave sobre el liderazgo en seguridad dentro de las organizaciones

El 91% informó que cuenta con un ejecutivo con responsabilidad directa sobre la seguridad.
Es el caso más frecuente de CISO (29%) o CSO (24%).





Los CISO (y equivalentes) son más optimistas que los gerentes de SecOps respecto del estado de la seguridad en las compañías, tal vez porque están más alejados de las realidades diarias.

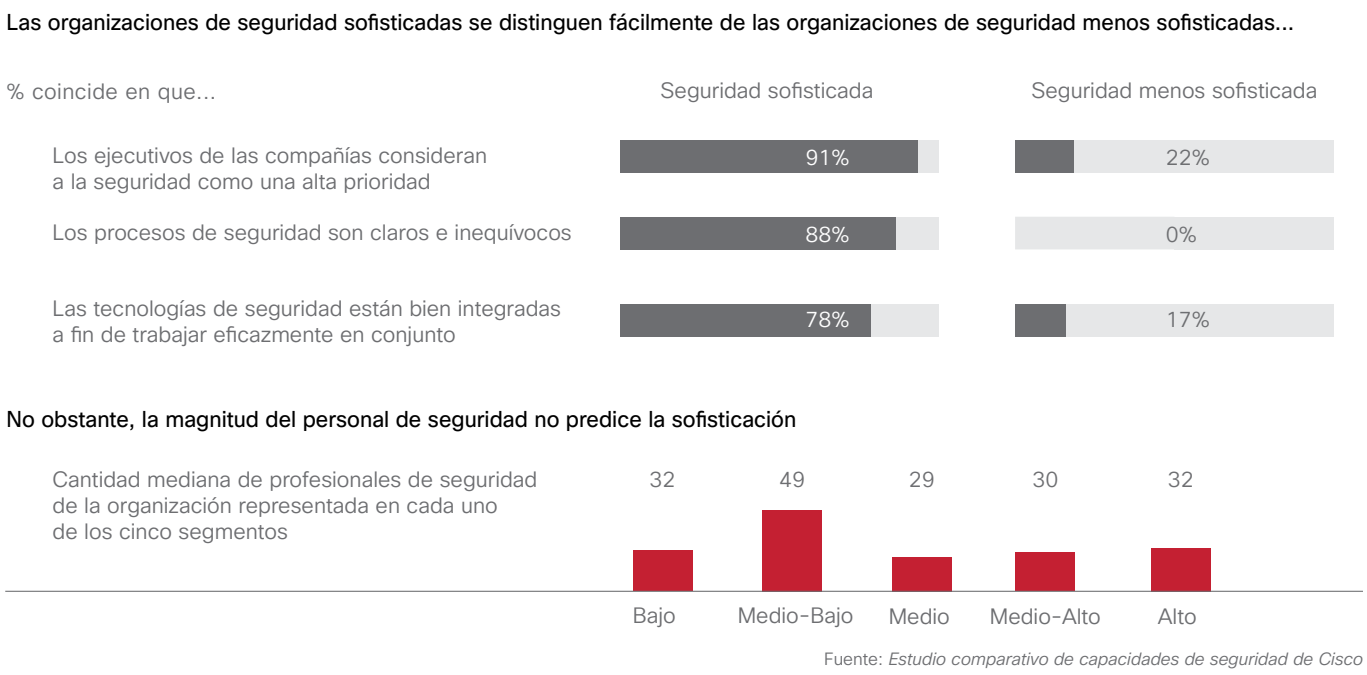
Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

La Figura 23 muestra que el 91% de los encuestados informó que cuenta con un ejecutivo con responsabilidad directa sobre la seguridad, generalmente un CISO o CSO (jefe de seguridad). El alto nivel de organizaciones que cuentan con una persona en el punto de seguridad es alentador: sin el liderazgo en seguridad, los procesos están menos definidos, difundidos y aplicados. Es probable que las últimas brechas de seguridad de alto perfil en las organizaciones hayan dado lugar a la gestión de seguridad en rangos ejecutivos.

El 78% de los encuestados de las compañías más sofisticadas coincide plenamente en que las tecnologías de seguridad están bien integradas a fin de trabajar eficazmente en conjunto en comparación con el 17% de los encuestados de las compañías menos sofisticadas.

La noticia positiva para las organizaciones que esperan incrementar la sofisticación de los procesos de seguridad es que reunir un gran equipo de talentos de seguridad difíciles de encontrar no es un requisito necesario. En las organizaciones menos sofisticadas, la cantidad mediana de profesionales de seguridad es de 32; en aquellas con mayores niveles de sofisticación, la cantidad mediana de personal de seguridad también es de 32. Por lo tanto, emplear a más personas no parece tener una correlación directa con una mejor gestión de los procesos de seguridad. Un enfoque superior para dotar el departamento de personal de seguridad puede ser encontrar una relación óptima entre el personal de seguridad y la cantidad general de empleados de la compañía.

Figura 24. Descubrimientos clave sobre la priorización de la seguridad



Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

La Figura 24 revela que las organizaciones de seguridad menos sofisticadas generalmente no creen que los ejecutivos consideran la seguridad como una alta prioridad ni que los procesos de seguridad son claros e inequívocos.

En la comparación de los niveles de sofisticación de seguridad de las organizaciones por país hay más buenas noticias: las organizaciones altamente sofisticadas son mayoría en cada segmento. Sin embargo, los encuestados de algunos países parecen tener una visión más positiva de su propio estado de seguridad que el mundo exterior. Las percepciones demasiado confiadas de los encuestados de algunos países pueden deberse en parte a valores sociales fundamentales de la cultura, como la necesidad de mostrar una actitud positiva tanto propia como de la organización.

Tenga cuidado con el exceso de confianza

A pesar de que los CISO y gerentes de SecOps confían en sus operaciones de seguridad, también indican que no utilizan herramientas estándar para evitar las brechas de seguridad. Menos del 50% de los encuestados utiliza las siguientes herramientas:

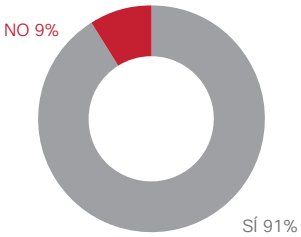
- Administración de identidad o provisión de usuarios
- Revisión y configuración
- Prueba de penetración
- Análisis forense de terminales
- Análisis de vulnerabilidades

Recursos de seguridad de la organización

Figura 25. Cantidad de profesionales dedicados a la seguridad dentro de las organizaciones
Las organizaciones tienen un promedio de 123 profesionales dedicados a la seguridad. Las organizaciones gubernamentales son más propensas a externalizar sus servicios de seguridad.

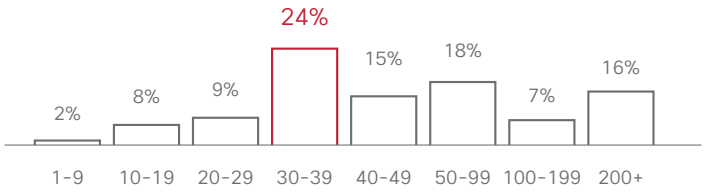
Instantánea de los recursos de seguridad

¿Cuenta su organización con un equipo de respuesta a incidentes de seguridad?



Cantidad promedio de profesionales dedicados a la seguridad

Porcentaje promedio del tiempo dedicado a las tareas relacionadas con la seguridad



Cantidad de profesionales dedicados a la seguridad

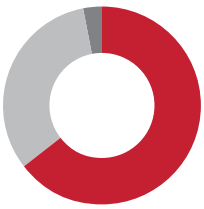
El gobierno parece externalizar más servicios de seguridad que otros grupos de la industria.

Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Figura 26. Tecnologías de seguridad utilizadas por las organizaciones

Aproximadamente dos tercios de los encuestados consideran que las tecnologías de seguridad están al día y se actualizan con frecuencia.

¿Cómo describiría su infraestructura de seguridad? Base: C = 1738



64% Nuestra infraestructura de seguridad está al día y se cambian las versiones constantemente por las mejores tecnologías disponibles.

33% Reemplazamos o cambiamos las versiones de nuestras tecnologías de seguridad periódicamente, pero no estamos equipados con las mejores y más recientes herramientas.

3% Reemplazamos o cambiamos las versiones de nuestras tecnologías de seguridad solo cuando las anteriores ya no funcionan o son obsoletas, o cuando identificamos necesidades totalmente nuevas.

Una proporción significativamente elevada de CISO (70%) considera que la infraestructura de su organización está al día en comparación con los gerentes de SecOps (57%).

Las compañías de telecomunicaciones son más propensas a mantener su infraestructura de seguridad al día.

Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Figura 27. Defensas contra amenazas de seguridad utilizadas por las organizaciones

Diferentes defensas contra amenazas de seguridad utilizadas por las organizaciones en 2014.

	Defensas contra amenazas de seguridad utilizadas por la organización		Defensas administradas a través de servicios basados en la nube	
	SecOps C = 797	CISO C = 941	SecOps C = 759	CISO C = 887
Seguridad de la red, prevención de intrusiones/firewalls	57%	64%	30%	39%
Seguridad web	56%	62%	33%	41%
Seguridad de mensajería/correo electrónico	53%	58%	33%	41%
Prevención de pérdida de datos	55%	55%	-	-
Cifrado/Privacidad/Protección de datos	52%	55%	-	-
Autorización/Control de acceso	55%	52%	24%	24%
AutenticaciónSeguridad móvil	54%	51%	24%	22%
Mobility security	48%	54%	24%	32%
Tecnología inalámbrica protegida	47%	52%	22%	30%
Protección terminal/anti-malware	45%	52%	24%	27%
Análisis de vulnerabilidades	44%	51%	24%	26%
VPN	49%	46%	25%	27%
Administración de identidad/Provisión de usuarios	43%	47%	16%	23%
Gestión de eventos e información de seguridad (SIEM)	39%	46%	-	-
Análisis de redes forenses	41%	43%	-	-
Revisión y configuración	38%	40%	-	-
Prueba de penetración	39%	37%	20%	19%
Defensa de DDoS	35%	37%	-	-
Análisis de terminales forenses	29%	33%	-	-

Encuestados sobre seguridad que utilizan defensas contra amenazas de seguridad; C = 1646

El 13% de los encuestados dijo que ninguna de las defensas contra amenazas de seguridad utilizadas se administra mediante servicios basados en la nube. Esto es especialmente cierto en el caso de las industrias sanitaria, farmacéutica y de servicios financieros.

Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Operaciones, procedimientos y políticas de seguridad de las organizaciones

Figura 28. Niveles de confiabilidad en las políticas de seguridad de las organizaciones y capacidad de las organizaciones para contener los riesgo

Aunque las organizaciones parecen confiar en sus políticas de seguridad organizativa, muestran menos confianza en la capacidad para abarcar y contener los compromisos.

Niveles de confiabilidad en las políticas de seguridad de las organizaciones

Políticas de seguridad C = 1738	SecOps C = 797			CISO C = 941		
	En desacuerdo/De acuerdo/ Totalmente de acuerdo			En desacuerdo/De acuerdo/ Totalmente de acuerdo		
Se llevan a cabo clasificaciones e inventarios claros de los activos de información.	11%	40%	49%	4%	38%	58%
Realizamos un excelente trabajo en el manejo de la seguridad de RR. HH.	9%	45%	46%	4%	36%	60%
Las instalaciones informáticas de la organización están bien protegidas.	10%	39%	51%	4%	34%	62%
Los controles de seguridad técnica de los sistemas y las redes están bien administrados.	6%	41%	53%	3%	31%	66%
Los derechos de acceso a las redes, los sistemas, las aplicaciones, las funciones y los datos se controlan adecuadamente.	8%	35%	57%	4%	32%	64%
Realizamos un buen trabajo en la incorporación de la seguridad en los sistemas y las aplicaciones.	10%	38%	52%	4%	32%	64%
Realizamos un buen trabajo en la incorporación de la seguridad en los procedimientos de adquisición, desarrollo y mantenimiento de los sistemas.	9%	41%	50%	4%	35%	61%

Niveles de confiabilidad en la capacidad de las organizaciones para contener los compromisos

Operatividad de la seguridad C = 1738	SecOps C = 797			CISO C = 941		
	En desacuerdo/De acuerdo/ Totalmente de acuerdo			En desacuerdo/De acuerdo/ Totalmente de acuerdo		
Revisamos y mejoramos nuestras prácticas de seguridad periódica, formal y estratégicamente todo el tiempo.	7%	42%	51%	3%	36%	61%
Contamos con herramientas vigentes que nos permiten revisar y brindar comentarios relacionados con las capacidades de la práctica de seguridad.	10%	41%	49%	4%	39%	57%
Investigamos rutinaria y sistemáticamente los incidentes de seguridad.	11%	40%	49%	3%	37%	60%
Podemos incrementar los controles de seguridad de los activos de gran valor si las circunstancias lo requieren.	10%	43%	47%	3%	38%	59%
Revisamos periódicamente la actividad de conexión de la red para garantizar el funcionamiento previsto de las medidas de seguridad.	8%	39%	53%	4%	33%	63%
Nuestras capacidades de bloqueo y detección de amenazas están al día.	9%	38%	53%	3%	36%	61%
Nuestras tecnologías de seguridad están bien integradas a fin de trabajar eficazmente en conjunto.	9%	40%	51%	3%	37%	60%
La seguridad está bien integrada en las capacidades comerciales y los objetivos de la organización.	10%	39%	51%	2%	34%	64%
Es fácil determinar el alcance del compromiso, contenerlo y corregirlo del aprovechamiento de vulnerabilidades.	15%	44%	41%	8%	42%	50%

Muchos encuestados de empresas medianas están totalmente de acuerdo con que "revisan y mejoran las prácticas de seguridad periódica, formal y estratégicamente todo el tiempo" en comparación con los encuestados de grandes empresas.

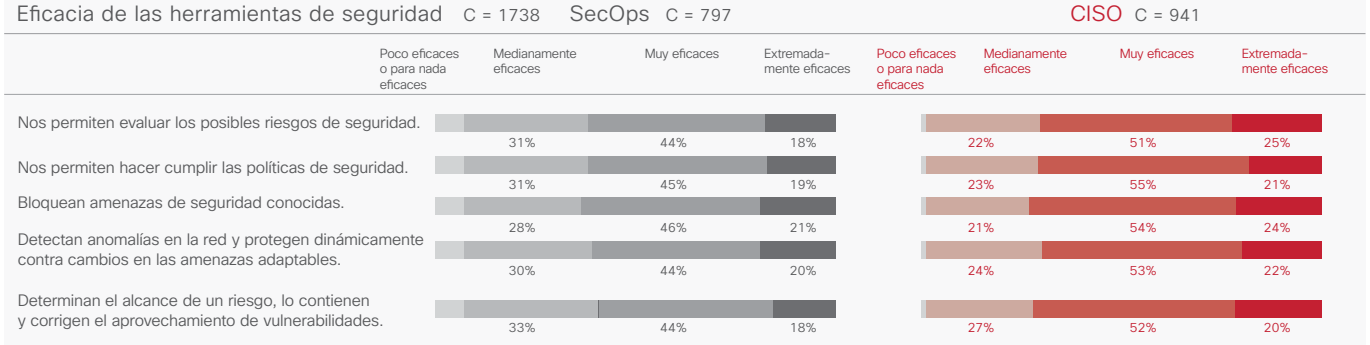
Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Figura 29. Consideraciones de los encuestados sobre los controles de seguridad de las compañías y las herramientas de seguridad de las organizaciones

Si bien los profesionales de seguridad consideran que las organizaciones tienen buenos controles de seguridad, aproximadamente un cuarto de los encuestados cree que las herramientas de seguridad son solo medianamente eficaces.

C de controles de seguridad C = 1738	SecOps C = 797			CISO C = 941		
	En desacuerdo/	De acuerdo/	Totalmente de acuerdo	En desacuerdo/	De acuerdo/	Totalmente de acuerdo
Seguimos prácticas de respuesta a incidentes estandarizadas, como RFC2350, ISO/IEC 27035:2011 o certificaciones estadounidenses.	15%	42%	43%	6%	40%	54%
Contamos con procesos eficaces para interpretar y priorizar los informes entrantes de incidentes y comprenderlos.	11%	46%	43%	4%	39%	57%
Tenemos buenos sistemas de verificación de ocurrencia real de incidentes de seguridad.	11%	41%	48%	4%	36%	60%
Tenemos un buen sistema de categorización de información relacionada con incidentes.	10%	43%	47%	4%	37%	59%
Realizamos un buen trabajo en la notificación y colaboración con las partes interesadas respecto de los incidentes de seguridad.	10%	46%	44%	3%	40%	57%
Contamos con procedimientos y procesos bien documentados de respuesta y seguimiento de incidentes.	9%	40%	51%	4%	35%	61%
Incorporamos periódicamente evaluaciones de riesgos cibernéticos en nuestro proceso de evaluación general de riesgos.	10%	37%	53%	4%	36%	60%

Una cantidad significativa de encuestados de servicios públicos/energía concuerda con la afirmación "Contamos con procedimientos y procesos bien documentados de respuesta y seguimiento de incidentes" en comparación con los profesionales de la mayoría de las demás industrias.



Los profesionales de seguridad de la industria del transporte expresan menos confianza en la capacidad de su organización para detectar y proteger contra amenazas de seguridad conocidas.

Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Figura 30. Procesos utilizados para analizar los sistemas comprometidos y eliminar las causas de incidencias de seguridad

Los profesionales de seguridad son más propensos a utilizar registros de firewall para analizar los riesgos, aunque estos registros generalmente carecen de datos de alta calidad o contexto para la información. Para analizar mejor los riesgos, los profesionales de seguridad deben revisar los registros de IDS e IPS, el proxy, los sistemas de prevención de intrusiones basados en host (HIPS), los registros de aplicaciones y NetFlow periódicamente.

Sorprende ver que "Análisis de registros/eventos correlacionados" aparece por debajo en la lista de herramientas utilizadas para analizar los riesgos. Esto puede significar que los encuestados no correlacionan los datos con las fuentes de vinculación de datos, lo que proporcionaría análisis más profundos del evento de seguridad.

Procesos de análisis de los sistemas en riesgo	SecOps	CISO
	C = 797	C = 941
Registros de firewall	59%	62%
Análisis de registros de sistemas	58%	60%
Análisis de regresión de archivos o malware	51%	58%
Análisis del flujo de red	51%	54%
Análisis de registros	48%	51%
Análisis de captura de paquete completo	44%	48%
Análisis de registros/eventos correlacionados	40%	44%
Análisis forense de la memoria	39%	43%
Análisis forense del disco	38%	41%
Detección de indicadores de riesgo (IOC)	38%	38%
Equipos de análisis/respuesta a incidentes externos (o de terceros)	36%	38%

Los encuestados del gobierno tienden a informar el uso de más procesos de análisis de sistemas en riesgo que los encuestados de la mayoría de las demás industrias.

Procesos para eliminar las causas de incidentes de seguridad	SecOps	CISO
	C = 797	C = 941
Cuarentena o eliminación de aplicaciones malintencionadas	55%	60%
Análisis de causa principal	55%	56%
Detención de la comunicación de software malicioso	51%	55%
Control adicional	51%	53%
Actualización de las políticas	50%	51%
Detención de la comunicación de aplicaciones comprometidas	47%	49%
Desarrollo de correcciones a largo plazo	46%	48%
Replicación de la imagen del sistema al estado anterior	43%	47%

Las respuestas de los CISO y los SecOps son coherentes, excepto en el caso de la detención de la comunicación de software malicioso.

Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Figura 31. Respuestas de los CISO y SecOps sobre los controles posteriores a los incidentes

Más CISO que profesionales de operaciones de seguridad informan la implementación de controles adicionales posteriores a los incidentes.

Procesos de restauración de sistemas afectados	SecOps	CISO
	C = 797	C = 941
Implementación de detecciones y controles nuevos o adicionales en función de las debilidades posteriores a los incidentes	55%	65%
Revisión y actualización de aplicaciones consideradas vulnerables	59%	60%
Restauración de copias de seguridad previas a los incidentes	53%	60%
Restauración diferencial	53%	58%
Restauración de imagen de la memoria central	33%	36%

Los encuestados de telecomunicaciones y servicios públicos/energía indicaron que utilizan la restauración de imagen de la memoria central con más frecuencia que otras industrias.

Figura 32. Quiénes reciben las notificaciones de incidentes de seguridad

El personal de operaciones y los partners tecnológicos son más propensos a recibir notificaciones de incidentes de seguridad a través de procesos más formales.

Grupos notificados en caso de un incidente	SecOps	CISO
	C = 797	C = 941
Operaciones	44%	48%
Partners tecnológicos	42%	47%
Ingeniería	38%	37%
Recursos Humanos	37%	35%
Legales	37%	35%
Todos los empleados	38%	33%
Fabricación	31%	36%
Partners comerciales	31%	33%
Marketing	30%	31%
Relaciones públicas	30%	27%
Autoridades externas	25%	20%

Las agencias gubernamentales son mucho más propensas a tener procesos de notificación claramente definidos con más grupos constituyentes que otras industrias.

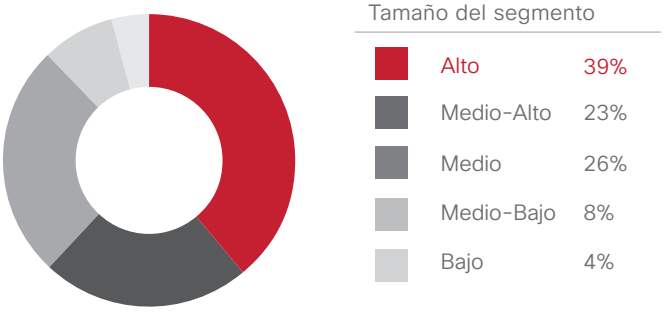
Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Sofisticación de seguridad de la organización

Figura 33. Sofisticación de los procesos de seguridad

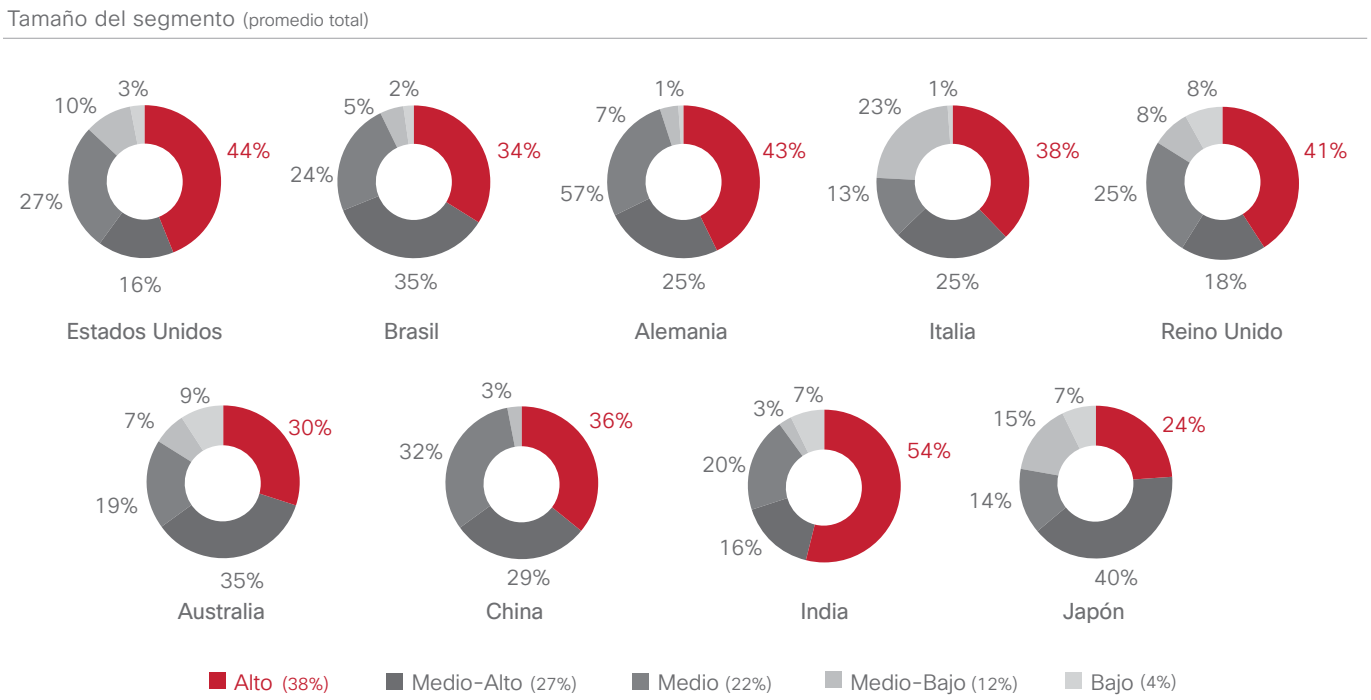
La mayoría de las compañías se ajusta a perfiles de seguridad más sofisticados. Esto es cierto en todos los países (Figura 34) y todas las industrias (Figura 35).

Los segmentos reflejan los crecientes niveles de sofisticación alrededor de la prioridad de la seguridad y cómo se traducen en procesos y procedimientos.



Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

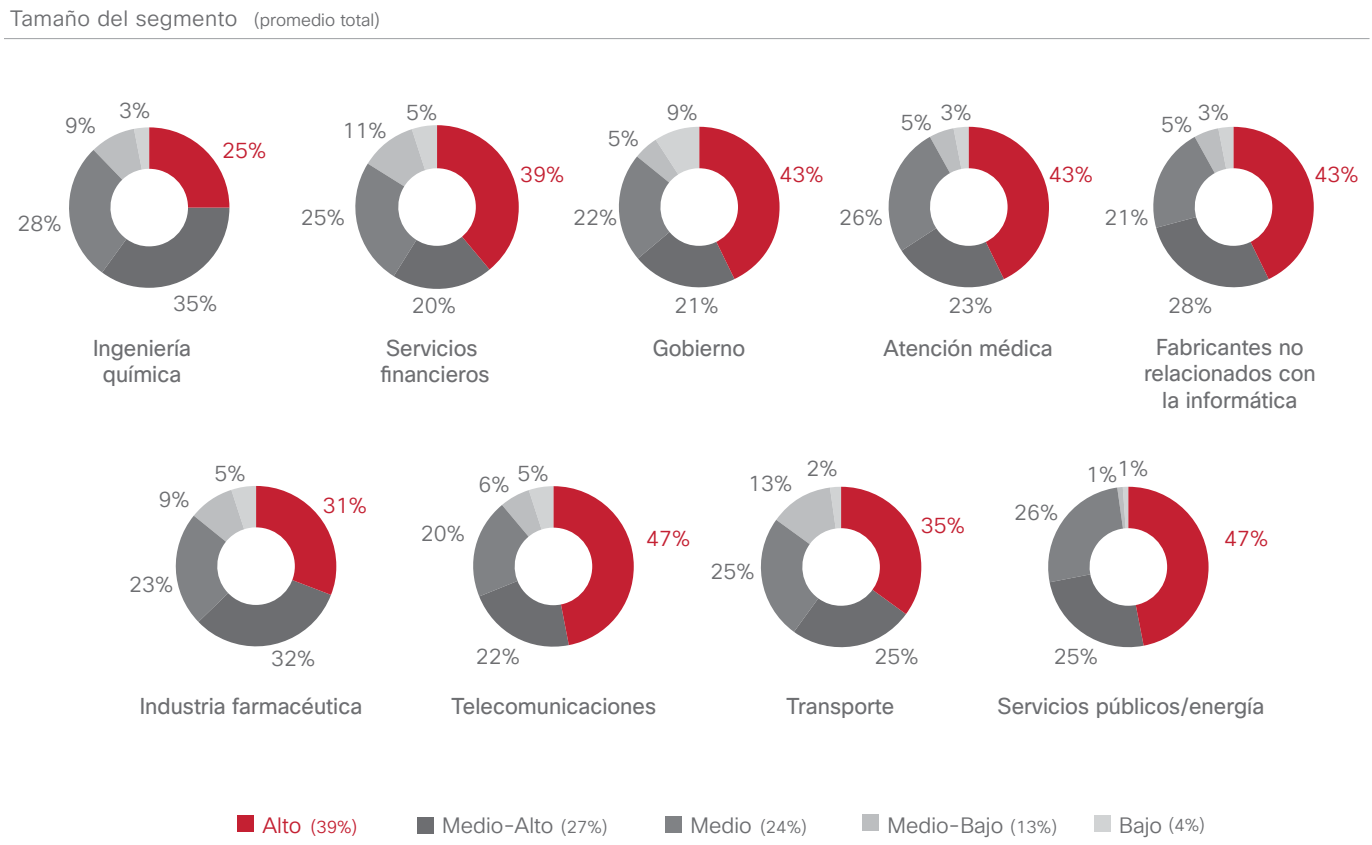
Figura 34. Sofisticación de los procesos de seguridad por país



Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Figura 35. Sofisticación de los procesos de seguridad por industria

Casi la mitad de las organizaciones de telecomunicaciones y servicios públicos/energía está categorizada en el segmento de seguridad altamente sofisticada.



Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

Las organizaciones medianas están bien posicionadas respecto de la preparación para la seguridad

Se espera que las organizaciones muy grandes manejen con éxito la seguridad, dado que tienen acceso a los mejores recursos: presupuestos para adquirir las últimas tecnologías y personal cualificado para manejarlas. Cabe suponer que las empresas de tamaño mediano (definidas a los propósitos de este estudio como empresas de 500 a 999 empleados) quedan detrás de sus contrapartes de mayor tamaño (1000 empleados o más) en términos de preparación para responder a incidentes de seguridad. Sin embargo, según el *Estudio comparativo de capacidades de seguridad de Cisco,* las empresas medianas más grandes no solo son un reflejo de la preparación para la seguridad de las empresas grandes en muchas áreas, sino que con frecuencia tienen una clasificación mayor que las organizaciones grandes; tal vez debido a la mayor flexibilidad de las organizaciones y a su mayor agilidad.

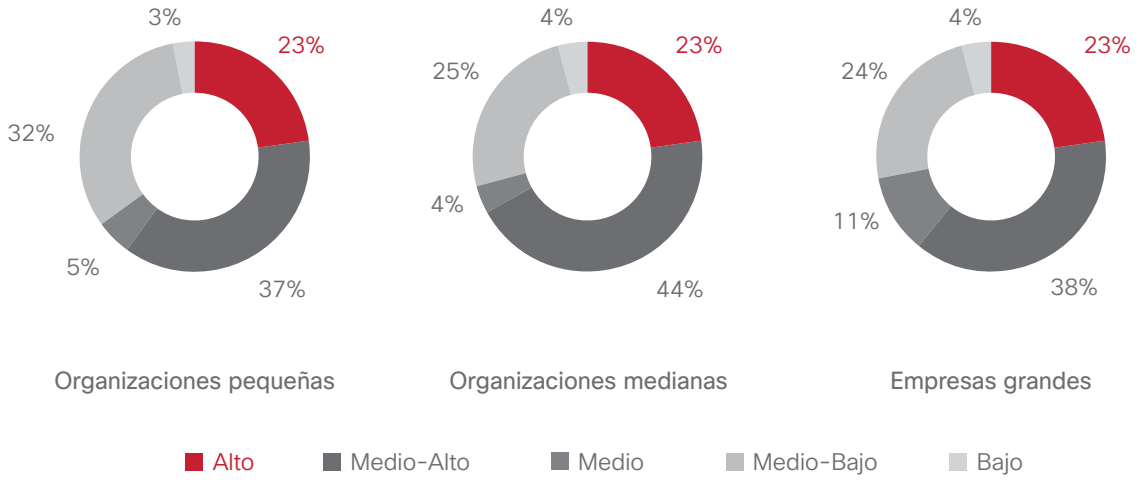
De hecho, conforme al estudio, las organizaciones medianas más grandes son más propensas a tener estados de seguridad altamente sofisticados. Como se ilustra en la Figura 36, las organizaciones medianas significativamente más grandes clasifican en el nivel medio-alto y alto de sofisticación en comparación con las organizaciones medianas más pequeñas (250-499 empleados) y las organizaciones empresariales (1000 o más empleados).

Esta gran nivelación de las condiciones para las empresas medianas es una noticia alentadora, dado que las compañías medianas son el motor de la recuperación económica.

Descubrimientos clave de la encuesta de referencia a empresas medianas sobre su preparación para la seguridad:

- El 92% de las organizaciones medianas cuenta con equipos de respuesta a incidentes internos, al contrario del 93% de las empresas grandes.
- El 94% de las organizaciones medianas cuenta con un ejecutivo con responsabilidad directa sobre la seguridad, al contrario del 92% de las empresas grandes.

Figura 36. Nivel de sofisticación del estado de seguridad de las organizaciones medianas más grandes



Los segmentos reflejan los crecientes niveles de sofisticación alrededor de la prioridad de la seguridad dentro de la organización y cómo se traducen en procesos y procedimientos.

Más organizaciones medianas clasifican en el nivel medio-alto y alto en comparación con organizaciones más pequeñas y empresas.

Al menos el 60% se ajusta a perfiles de seguridad más sofisticados.

Fuente: *Estudio comparativo de capacidades de seguridad de Cisco*

3. Geopolítica y tendencias de la industria

Los expertos en política, geopolítica y seguridad de Cisco identifican tendencias geopolíticas actuales y emergentes que las organizaciones, especialmente las compañías multinacionales, deben monitorear. Estos mismos expertos además examinan recientes y posibles desarrollos internacionales relacionados con los temas de soberanía de datos, localización de datos, cifrado y compatibilidad de datos.

Los delitos cibernéticos prosperan en áreas de débil gestión

A pesar de que los CISO y otros líderes de seguridad no siempre prestan demasiada atención a la dinámica geopolítica, deberían hacerlo, especialmente si trabajan para organizaciones multinacionales. Lo que sucede en el panorama geopolítico puede tener un impacto directo en las cadenas de abastecimiento mundial y en la manera en que las empresas manejan los datos de empleados y clientes en distintos países; también puede generar mayores costos legales y regulatorios, riesgos de robo de secretos comerciales, además de riesgos físicos y de reputación.

Los delitos cibernéticos prosperan en todo el mundo, especialmente en áreas de débil gestión. Europa oriental, un hervidero de crimen organizado durante mucho tiempo, es un ejemplo. En áreas de débil gestión, no es raro encontrar evidencia de fuertes vínculos entre los servicios de inteligencia gubernamental y los grupos organizados involucrados en los delitos cibernéticos.

Según las autoridades estadounidenses, ciertos ataques recientes de alto perfil dirigidos a los activos de los Estados Unidos probablemente se originaron en dichas áreas. Algunos de los ataques parecieron no tener fines de lucro, sino ser campañas políticamente motivadas o intentos de recopilar información o infiltrarse en la infraestructura.[7] Esto puede indicar que las campañas fueron patrocinadas por el estado u orquestadas por organizaciones de delito cibernético sofisticadas.

Cada vez más gobiernos hacen el esfuerzo concertado de implementar una mayor gestión cibernética a través de la legislación y la regulación. China, por ejemplo, hizo del tema del cuarto pleno del 18.° Congreso del Partido Comunista de China (CCP) un "estado de derecho".[8] Pekín se ha comprometido a erradicar la corrupción y hacer cumplir las leyes en las empresas y el gobierno. Estos esfuerzos pueden reforzar el cumplimiento de la ley y los esfuerzos internacionales de perseguir a los delincuentes cibernéticos y dificultarles el ocultamiento.

Grupos terroristas transnacionales aprovechan Internet

La aparición de grupos terroristas transnacionales, como el denominado Estado islámico (ISIS o ISIL), es otra tendencia geopolítica que debe vigilarse. Aunque los grupos tales como el ISIS no parecen estar involucrados en ninguna actividad de delito cibernético importante, dependen mucho de Internet (concretamente de los medios sociales) para contratar miembros. Al parecer, por ahora, los principales grupos terroristas transnacionales hacen suficiente dinero mediante actividades de recaudación de fondos tradicionales, como la extorsión, el tráfico humano y el petróleo. Pero a medida que estas organizaciones crecen, pueden volcarse al delito cibernético como medio de financiación de sus esfuerzos en todo el mundo. También existe la posibilidad de que las organizaciones terroristas incipientes que no tienen acceso a los mismos recursos que los grupos más establecidos exploren el delito cibernético como vía rápida de crecimiento.

Consulte la entrada de blog de Cisco: "Cupcakes y espionaje cibernético" para obtener información sobre un nuevo enfoque sugerido de defensa contra el espionaje cibernético.

El enigma de la soberanía de datos, la localización de datos y el cifrado

El alegato de Edward Snowden sobre las extralimitaciones de la vigilancia, la soberanía de datos (el concepto de que los datos están sujetos a la jurisdicción del país donde se ubican y no de los gobiernos extranjeros o los tribunales que buscan su acceso unilateral) y la localización de datos (mandato gubernamental que determina el lugar de almacenamiento de los datos) del gobierno estadounidense se ha convertido en un tema candente.

Algunos países procuran la capacidad de localizar sus datos como forma de impedir que los gobiernos extranjeros accedan a los datos de los ciudadanos. Elaboran requisitos para que los datos permanezcan dentro del país o se envíen de determinada manera y para que las compañías utilicen equipos de fabricación nacional.

Brasil, por ejemplo, recientemente implementó una nueva ley que "contiene requisitos de privacidad que restringen ampliamente (cubren) a las compañías del intercambio de información personal de los usuarios, comunicaciones y ciertos datos de inicio de sesión en línea".[9] Rusia, mientras tanto, enmendó hace poco su legislación sobre protección de datos e información y exige que todos los operadores de datos procesen los datos personales de los ciudadanos rusos, incluidos los datos de Internet, a fin de conservar copias de dicha información en servidores y bases de datos dentro de Rusia; esta ley entrará en vigencia en 2015.[10]

Una consecuencia potencialmente negativa de los países que promulgan la localización de datos (legislación no interoperable) es que las compañías multinacionales pueden quedar sujetas a requisitos legales conflictivos. La obligación de cumplir con las demandas de producción, retención o destrucción de datos de una nación puede infringir las leyes de otro país.

Aparte de causar posibles obligaciones legales conflictivas, la localización de datos además tiene el potencial de restringir el flujo de datos entre las fronteras. Esto puede generar confusión, así como también desafíos importantes en la administración de redes. También aparece un aspecto de la cadena de abastecimiento: más operadores de la cadena de abastecimiento mundial adoptan tecnologías basadas en la nube para conectarse con todos sus partners en todo el mundo. La localización de datos puede obstaculizar o impedir el intercambio de datos en dichas redes comerciales y posiblemente dificultar las actividades policiales contra el delito cibernético entre las fronteras.

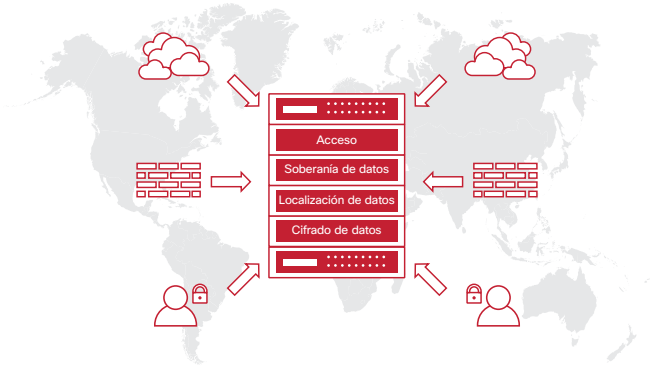
Adicionalmente, dado que algunos países optan por utilizar solo tecnologías nacionales o imponen importantes restricciones respecto de quién puede manejar los datos de los ciudadanos, existe el posible riesgo de quedar excluidos de los equipos de expertos en el mundo y perder las innovaciones que surgen del intercambio de nuevas ideas.

Algunas compañías estadounidenses líderes en tecnología esperan que el uso del cifrado integral satisfaga las inquietudes de sus clientes respecto de la protección de los datos que atraviesan el espacio sin fronteras de Internet. No obstante, el gobierno estadounidense ha expresado su preocupación sobre el hecho de que dicho cifrado interfiera en su capacidad para proteger a los ciudadanos. El nuevo director del Cuartel General de Comunicaciones del Gobierno (GCHQ), la principal organización de inteligencia de señales británica, similar a la Agencia Nacional de Seguridad de los Estados Unidos, incluso sugiere que los gigantes tecnológicos de las redes sociales estadounidenses contribuyen a los esfuerzos de los terroristas al permitirles enviar comunicaciones cifradas a todo el mundo.[11]

A pesar de estas críticas, las compañías tecnológicas son propensas a procurar el desarrollo y la adopción de medidas tecnológicas que apuntan a restaurar la confianza de los clientes hasta que el gobierno adopte políticas que reflejen eficazmente la importancia de permitir la libre expresión y garantizar el comercio mientras brindan protección contra amenazas a la seguridad pública y nacional.

La confianza en los productos tecnológicos y las compañías que los desarrollan significarán un gran avance para que los países, sus gobiernos y ciudadanos confíen en su propia protección y la protección de sus datos. Como Mark Chandler, secretario, asesor jurídico y vicepresidente ejecutivo de Cisco, mencionó en una entrada de blog de Cisco a principio de este año: "Un esfuerzo serio para abordar estos problemas puede generar confianza y, lo que es más importante, derivar en la promesa de cumplimiento de la siguiente generación de Internet, un mundo en el que la conexión entre personas y dispositivos impulse una mayor libertad, prosperidad y oportunidad para todos los ciudadanos del mundo".[12]

Figura 37. El enigma de la soberanía de datos, la localización de datos y el cifrado

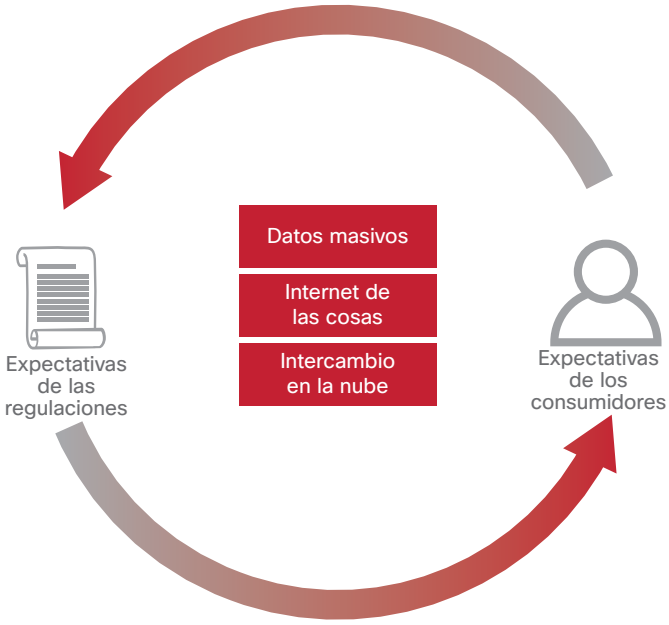


Compatibilidad de la privacidad de datos

Las actitudes de las personas o las organizaciones sobre la privacidad de los datos pueden variar considerablemente según el lugar del mundo en que residen y trabajan. Estos diversos puntos de vista afectan a la manera en que los gobiernos regulan la privacidad de los datos y la manera en que las empresas realizan negocios cuando estas regulaciones son contradictorias. El ***Informe de la encuesta sobre índices críticos de protección de datos***, patrocinado por Cisco y preparado por Cloud Security Alliance, detalla algunos de los desafíos que enfrentan las empresas que trabajan con datos fuera de sus propios países o datos que pertenecen a individuos fuera del país en que opera la empresa.

El diálogo en torno a la compatibilidad de la privacidad de datos (es decir, la generación de enfoques globales coherentes sobre la privacidad de datos) es cada día más urgente debido al crecimiento de los servicios en la nube. Por ejemplo, si una compañía con sede en los Estados Unidos adquiere el almacenamiento en la nube de una compañía en la India y utiliza dicha nube para almacenar datos de clientes que residen en Alemania, ¿las leyes de privacidad de qué país o región se aplican?

Figura 38. Cumplimiento de las diversas expectativas de los consumidores y las regulaciones



Otros factores de compatibilidad de la privacidad de datos son Internet de las cosas (IdC) y datos masivos. A medida que las empresas consideran nuevas formas de conectar dispositivos entre sí y utilizar conjuntos de datos masivos para tomar decisiones empresariales, necesitan estructuras y reglas para la manipulación a escala global de estos datos.

Ya está en marcha una serie de esfuerzos destinados a armonizar los requisitos de privacidad de los datos en una región o un grupo de países . Por ejemplo, la legislación de la Unión Europea, la *Regulación general de protección de datos,* que busca armonizar las regulaciones de protección de datos, se enmendará a fin de actualizar el marco de protección de datos existente. También se están intensificando los esfuerzos para alcanzar el consenso en torno a las leyes de soberanía de datos y privacidad de datos. Una mayor armonización será bien recibida, sin embargo también es importante que el texto final esté orientado a los resultados, interopere con otras regiones y se adecue a las nuevas realidades tecnológicas. La región de Asia Pacífico ha desarrollado un Acuerdo de cumplimiento de la privacidad entre fronteras con la Cooperación Económica de Asia Pacífico (APEC) que facilita el intercambio de datos en economías locales. Los gobiernes deben seguir trabajando para lograr el objetivo final de generar regímenes compatibles para la privacidad de los datos y la seguridad conforme a estándares mundialmente reconocidos que promuevan una Internet abierta con flujos libres de datos entre las fronteras nacionales y regionales.

Cuando los países y las regiones esclarezcan sus enfoques de privacidad de los datos, las empresas serán más capaces de aplicar prácticas de privacidad uniformes internacionalmente e implementar marcos de “privacidad desde el diseño” más eficaces, donde las capacidades de privacidad se incorporen a los productos y servicios desde el principio. Los marcos regulatorios de privacidad precisos y uniformes permitirán que las compañías cumplan y superen los requisitos de privacidad independientemente de dónde se aplican las ofertas, lo que fomentará el desarrollo de productos innovadores y el uso de datos.

Privacidad de los datos: un entendimiento común

En la encuesta sobre protección de datos se preguntó a los expertos en privacidad global de Norteamérica, la Unión Europea y la región de Asia Pacífico sobre la regulación de los datos, las prácticas gubernamentales, el contenido de usuario y los estándares de seguridad en su región. Las respuestas mostraron un alto nivel de coherencia de entendimiento de los encuestados sobre el significado de la privacidad de los datos y el valor de los estándares de privacidad globales.

- **Soberanía y residencia de los datos:** los encuestados identificaron datos personales e información de identificación personal (PII) como datos obligatorios para ser residente en la mayoría de los países.
- **Interceptación legal:** los encuestados mostraron una interpretación universal de cuándo y cómo deben interceptarse los datos; por ejemplo, cuando es necesario para una investigación penal.
- **Consentimiento del usuario:** el 73% de los encuestados coincidió en que debería haber una declaración de derechos de privacidad del consumidor global en lugar de regional. El 65% dijo que las Naciones Unidas deberían desempeñar un papel activo en la creación de dicha declaración.
- **Principios de privacidad:** se preguntó a los encuestados si los principios de seguridad de la Organización para la Cooperación y el Desarrollo Económico facilitan la armonización de datos o generan una mayor tensión. Los expertos en privacidad de los datos encuestados estuvieron a favor de la adopción de estos principios.

En resumen, la encuesta sobre privacidad de los datos demuestra que muchos expertos aceptan los principios básicos de privacidad que, si se adoptan y estandarizan globalmente, pueden activar los negocios en lugar de obstaculizarlos. Los resultados también indican que los expertos en privacidad de datos comparten un interés por "elaborar" principios de privacidad para nuevas soluciones tecnológicas en lugar de intentar acondicionar estas soluciones para que se adapten a los requisitos de privacidad. No obstante, los marcos regulatorios de la privacidad actuales son relativamente incipientes y evolucionan rápido.

Si se avanza a un nivel más alto de armonización, las compañías y los individuos se beneficiarán. Pero en la medida en que la industria siga elaborando marcos de privacidad mundialmente discordantes, las compañías deberán analizar detenidamente los problemas de privacidad y protección de datos y adaptar proactivamente sus ofertas y procesos a fin de satisfacer las diversas expectativas de los consumidores y las regulaciones.

Para obtener más información sobre problemas de protección de datos, consulte la entrada de blog de Cisco Security: **"Balance de la protección de datos: innovación y protección de los ciudadanos estadounidenses".**

4. Cambio de actitud frente a la seguridad cibernética: de los usuarios a la sala de reuniones del directorio

Los expertos en seguridad de Cisco sugieren que ha llegado el momento de que las empresas comiencen a considerar su enfoque sobre la seguridad cibernética de manera diferente para proteger verdaderamente a sus organizaciones. Entre las estrategias se incluyen: considerar nuevos enfoques para coordinar personas, procesos y tecnologías; instituir la seguridad como tema a tratar en la sala de reuniones del directorio; y adoptar controles de seguridad más sofisticados para reducir la superficie terminal del ataque, y fortalecer la red después de un ataque.

Acceso seguro: sepa quién, cuándo y cómo está en su red.

Los CISO y otros profesionales de seguridad se enfrentan a desafíos complejos relacionados con el acceso a servicios e información en la red. Gracias a las tendencias de las políticas de movilidad y Traiga su propio dispositivo (BYOD), es necesario asegurarse de que los empleados accedan a los recursos de la empresa, independientemente de dónde se encuentran y de cómo acceden a la red.

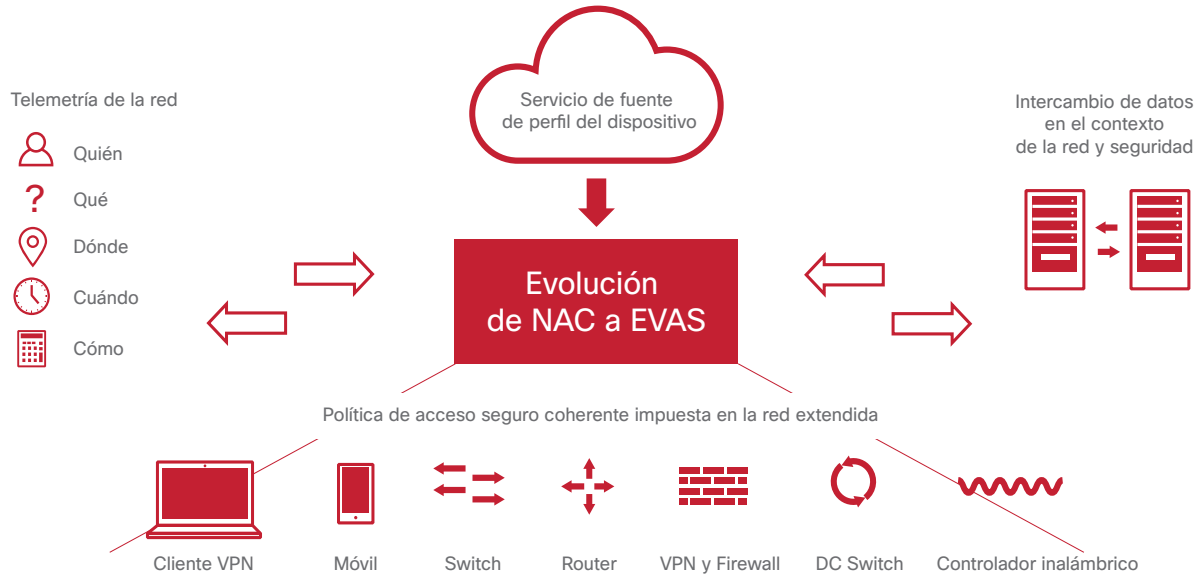
Los profesionales de seguridad además deben proteger la red de usuarios no aprobados o ataques delictivos de manera tal que no se interrumpa el acceso a los usuarios legítimos. Un ejemplo son las redes privadas virtuales (VPN) que se utilizan como solución estándar para controlar el acceso a la red. Sin embargo, algunas de estas VPN exigen procedimientos de inicio de sesión complicados por usuario, así como también un software especial, que limitan el momento y la manera en que las personas acceden a la red. Además, muchas VPN no ayudan a los departamentos de TI a identificar quién accede y desde dónde, ni pueden identificar el dispositivo en uso. Pero las VPN evolucionan para brindar más visibilidad y ofrecer una experiencia más transparente a los usuarios a fin de proporcionar mayor seguridad terminal.

Los controles de acceso a la red (NAC) han evolucionado a partir de la protección básica de seguridad hasta convertirse en controles de seguridad, acceso y visibilidad terminal (EVAS) más sofisticados. A diferencia de las anteriores tecnologías de NAC, los controles de EVAS utilizan información más granular para hacer cumplir las políticas de acceso, como datos de rol de usuario, ubicación, consideraciones del proceso comercial y gestión de riesgos. Los controles de EVAS además permiten conceder acceso más allá de las computadoras, lo que permite a los administradores de redes proporcionar acceso a través de dispositivos móviles o de IdC.

Los controles de EVAS permiten el enfoque de red como sensor para reforzar la seguridad y permitir o interrumpir el acceso a través de la red extendida, ya sea desde un dispositivo remoto (VPN) antes de conectarse a los servicios en red o dentro de la red mediante fuentes de recursos sensibles. Los controles de EVAS también permiten a las organizaciones reducir la superficie terminal de ataque de la red, limitar el ámbito y el alcance de un ataque, corregir los procesos de resolución de problemas e incluso fortalecer la red después de un ataque.

Para más información sobre las soluciones de EVAS y cómo ayudan a las organizaciones a mejorar la seguridad, consulte la entrada de blog de Cisco Security: "Nuevo documento informativo del Grupo de Estrategias Empresariales sobre la evolución y la necesidad de acceso seguro a la red".

Figura 39. Evolución de controles de acceso a la red (NAC) para controles de seguridad, acceso y visibilidad terminal (EVAS)



Antes de un ataque, los controles de EVAS pueden:

- **Identificar los activos en riesgo.** Monitorear todos los activos conectados a la red en cualquier momento; identificar aplicaciones, dispositivos y usuarios incumplidores; y correlacionar esta información con herramientas de evaluación de vulnerabilidades de terceros.
- **Mejorar la mitigación de riesgos.** Recopilar información práctica que puede compartirse con otras aplicaciones de seguridad y de red para mejorar los flujos de trabajo, optimizar las operaciones y priorizar la actividad de corrección.
- **Hacer cumplir las políticas de acceso a la red granular.** Proporcionar información contextual al cumplimiento de la política granular y limitar el acceso a segmentos de la red, activos o contenido sensible.

Durante un ataque, los controles de EVAS pueden:

- **Integrarse a sistemas de defensa avanzada de amenazas basados en la red.** Compartir información cuando se detecta una actividad maliciosa con el fin de correlacionar los patrones de comportamiento, las configuraciones y las conexiones terminales de datos del ataque con el tiempo.
- **Bloquear las tácticas de "cadena de eliminación" de los sistemas en riesgo.** Limitar el movimiento de ataque lateral al evitar que los sistemas en riesgo lleguen a los activos de la red no autorizados controlados por la política para robar credenciales, escalar privilegios y exfiltrar datos valiosos.
- **Limitar el alcance de un ataque.** Restringir y poner en cuarentena los sistemas que exhiben un comportamiento anómalo.

Después de la detección de un ataque, los controles de EVAS pueden:

- **Evaluar los perfiles terminales en busca de vulnerabilidades.** Compartir información de la base de datos de los controles de EVAS con herramientas de análisis de vulnerabilidad, que permiten a las operaciones de TI priorizar la corrección.
- **Corregir sistemas en riesgo.** Cuando se integran con los sistemas de gestión de eventos e información de seguridad (SIEM) y con los sistemas de seguridad terminal, los controles de EVAS pueden automatizar las correcciones y monitorear el progreso.
- **Ajustar los controles de seguridad y las políticas de acceso.** Trabajar junto con los equipos de redes y seguridad para segmentar el tráfico de la aplicación o agregar nuevas reglas de firewall o firmas de IPS.

A diferencia de los antiguos controles de acceso a la red excesivamente complejos, las soluciones de EVAS son facilitadores de negocios. A medida que las organizaciones adoptan las políticas de BYOD, la computación en la nube y las iniciativas móviles, se vuelve imperativo obtener visibilidad, mejorar el contexto de los dispositivos y usuarios conectados, y hacer cumplir eficientemente las políticas de seguridad. Los expertos en seguridad de Cisco predicen que los CISO optarán por las soluciones de EVAS para gestionar la compleja red de conexiones entre los usuarios, los dispositivos, las redes y los servicios en la nube.

El futuro de la seguridad cibernética depende de la actual participación de la sala de reuniones

Conforme al *Estudio comparativo de capacidades de seguridad de Cisco*, el 91% de las organizaciones cuenta con un ejecutivo con responsabilidad directa sobre la seguridad. Pero en el caso de las empresas modernas, el liderazgo en seguridad debe ascender más en la organización hasta llegar la sala de reuniones.

Las recientes brechas de datos masivos que implicaron a reconocidas compañías, la legislación y regulación relacionadas con la seguridad de los datos, la dinámica geopolítica y las expectativas de las partes interesadas son todos factores que hacen que la seguridad cibernética forme parte de la agenda de la sala de reuniones. Un informe de la Asociación de Auditoría y Control de Sistemas de Información (ISACA) reveló que el 55% de los directores corporativos debe comprender y manejar personalmente la seguridad cibernética como área de riesgo.[13]

Este es un desarrollo positivo que los líderes de seguridad de Cisco consideran muy postergado. En la economía moderna, cada compañía opera bajo TI. Esto hace que la seguridad sea responsabilidad de cada persona dentro de la organización, desde el director ejecutivo hasta el nuevo contratado y no solo del personal con el puesto o la descripción laboral de "seguridad". Todos son responsables y deben aprender a no convertirse en víctimas.

Los líderes de seguridad de Cisco sostienen que un componente fundamental del futuro de la seguridad cibernética será la mayor participación de la junta directiva. Los consejos de administración de las industrias deben conocer los riesgos de seguridad cibernética de las empresas y su posible impacto. Para entender por completo el alcance de los problemas de seguridad cibernética que afectan las organizaciones, es posible que las juntas directivas deban incorporar personal con experiencia en tecnología y seguridad cibernética.

Las juntas directivas además deben comenzar a formularse preguntas rigurosas sobre los controles de seguridad tales como: *¿Qué controles tenemos vigentes? ¿Están bien comprobados? ¿Contamos con procesos de generación de informes? ¿Con qué velocidad podemos detectar y corregir riesgos inevitables?* Y tal vez la pregunta más importante: *¿Qué más debemos saber?* Los CIO deben estar preparados para responder dichas preguntas ante la junta directiva de manera clara para sus miembros y que a la vez explique las implicaciones empresariales.

En una entrevista reciente en la revista FORTUNE[14], el jefe de seguridad y administrador fiduciario de Cisco, John Stewart, dijo que la junta directiva que formula este tipo de preguntas suscita "un interesante conjunto de efectos subsiguientes" que genera en definitiva la madurez de la industria de la seguridad. A partir de esto, declaró que el siguiente paso vital, la esperanza, es que los fabricantes finalmente reconozcan que deben integrar la seguridad a sus productos.

Stewart predice que, a medida que evolucione Internet de las cosas (IdC) y haya más "personas que dependan menos de los dispositivos que más personas con dispositivos en Internet", habrá más "accidentes" inevitables de posible gran magnitud. El diseño de la seguridad dentro de los productos permitirá evitar muchos de estos problemas o, al menos, reducir su impacto.

Por lo tanto, las juntas directivas de los fabricantes de tecnología deben preguntar a sus líderes de seguridad: *¿Incorporamos la seguridad en nuestros productos? Caso contrario, ¿Qué tan pronto podemos comenzar?*

Vea el video en el blog del jefe de seguridad y administrador fiduciario de Cisco, John Stewart, sobre la importancia de la transparencia de la seguridad cibernética y la responsabilidad ante la junta directiva: http://blogs.cisco.com/security/ensuring-security-and-trust-stewardship-and-accountability.

Manifiesto de seguridad de Cisco: principios básicos para alcanzar la seguridad del mundo real

Hoy en día, los CISO deben responder preguntas difíciles: *¿Cómo hago de mi equipo de seguridad el principal punto de contacto empresarial cuando surgen posibles problemas de seguridad? ¿Cómo garantizo que mi equipo cuente con las herramientas y la visibilidad para determinar cuáles son los problemas de seguridad más relevantes que requieren acción? ¿Y cómo protejo a los usuarios -la clave del éxito empresarial- cuando trabajan fuera del lugar?*

Los expertos en seguridad de Cisco sugieren que los CISO pueden abordar estas preguntas mediante la implementación y el seguimiento de un conjunto de principios de seguridad conocido como Manifiesto de seguridad de Cisco.

Este manifiesto de seguridad inaugural permite a los equipos de seguridad y los usuarios en las organizaciones comprender mejor y responder ante los desafíos de seguridad cibernética del mundo actual. Estos principios sirven como base de referencia a las organizaciones que aspiran a ser más dinámicas en su enfoque respecto de la seguridad y más adaptables e innovadoras que los adversarios:

1. **La seguridad debe considerarse un motor de crecimiento de la empresa.** La seguridad nunca debe ser un obstáculo ni un inconveniente que socave la productividad del usuario y se interponga en la innovación empresarial. Sin embargo, los equipos de seguridad imponen soluciones tecnológicas que hacen exactamente eso. Una razón primordial es que no se los invita a tiempo o directamente no se los invita a los debates sobre proyectos empresariales que requieren la implementación de tecnología nueva. Aun así, los profesionales de seguridad son culpables de esperar la invitación que nunca recibirán. En cambio, deben adoptar medidas proactivas para garantizar su participación en las conversaciones sobre tecnología y comprender cómo pueden los procesos de seguridad ofrecer a las organizaciones agilidad y éxito mientras protegen sus datos, activos e imágenes.
2. **La seguridad debe trabajar con la arquitectura existente y ser útil.** Los equipos de seguridad no deben desarrollar una arquitectura para albergar las nuevas soluciones tecnológicas destinadas a mejorar la seguridad. Las arquitecturas, por naturaleza, son restrictivas. Las organizaciones no deberían tener que modificar la manera en la que llevan a cabo sus negocios para albergar nuevas tecnologías de seguridad ni verse impedidas de modificar la manera en la que operan debido a las tecnologías vigentes. El resultado final de la "sobrecarga de arquitectura" será que los usuarios eludirán la arquitectura de seguridad y dejarán la organización desprotegida. Además, si una tecnología de seguridad es muy difícil de comprender para los usuarios y debe mantenerse mediante equipos de talentos de seguridad especializados difíciles de encontrar, no es útil para la organización.
3. **La seguridad debe ser transparente e informativa.** Los usuarios deben recibir la información de tal modo que les permita comprender por qué la seguridad les impide llevar a cabo una acción en particular. También deben saber cómo hacer lo que tienen que hacer de manera segura, en lugar de eludir la seguridad para realizar el trabajo. Por ejemplo, si un usuario intenta acceder a una página web y se encuentra con el mensaje: "El administrador ha denegado el acceso a este sitio", este carece de contexto acerca de por qué no puede acceder a la página. Pero si el mensaje dice: "Se ha denegado el acceso a este sitio porque ha distribuido malware en las últimas 48 horas", el usuario estará mejor informado y comprenderá el posible riesgo no solo para la organización, sino también para sí mismo como usuario individual. Las tecnologías de seguridad además deben permitir a los usuarios lograr sus objetivos de manera segura a través de recomendaciones claras o del redireccionamiento a los recursos adecuados para una asistencia oportuna.
4. **La seguridad debe habilitar la visibilidad y las acciones correctas.** Las soluciones de seguridad con arquitecturas de seguridad abiertas permiten a los equipos de seguridad determinar si dichas soluciones son realmente eficaces. Los profesionales de seguridad además necesitan herramientas para automatizar la visibilidad de la red a fin de ver no solo el tráfico, sino también los activos que conforman la red. Al entender el funcionamiento de las tecnologías de seguridad y qué es normal (y anormal) en el entorno de TI, los equipos de seguridad pueden reducir la carga de trabajo administrativa, y ser más dinámicos y precisos en la identificación y respuesta ante amenazas y la adaptación de las defensas. Mediante este enfoque, los equipos de seguridad pueden aprovechar al máximo los controles más individualizados y relevantes para contribuir a la resolución.
5. **La seguridad debe considerarse un "problema de la gente".** Un enfoque centrado en la tecnología para la seguridad no mejora la seguridad, sino que la agudiza. Las tecnologías son meras herramientas que pueden mejorar la capacidad de las personas para proteger el entorno. Los equipos de seguridad deben educar a los usuarios sobre los hábitos seguros que deben aplicar independientemente de dónde utilizan la tecnología (la oficina, la casa, de viaje) para tomar buenas decisiones y sentirse capaces de buscar ayuda oportuna si consideran que algo está mal. El diálogo mejorado entre los profesionales de seguridad y los usuarios permitirá que los usuarios vean que la tecnología no garantiza la seguridad. Las personas, los procesos y la tecnología en conjunto deben formar la defensa contra las amenazas actuales. El compromiso y la vigilancia de todos los usuarios de la organización, desde el primero hasta el último, facultan el éxito de la seguridad.

El Manifiesto de seguridad de Cisco es un llamado al cambio. En el mundo real, la tecnología de la seguridad, las políticas y las mejores prácticas deben elevar el nivel promedio de seguridad de todos los miembros de la organización y permitir que las empresas tomen más decisiones de riesgo informadas, hasta cada usuario individual. Cuando se cuenta con principios sólidos que sirven de guía, los usuarios son capaces de entender con claridad por qué no pueden realizar ciertas acciones y cuál será el impacto si deciden eludir la seguridad.

El Manifiesto de seguridad de Cisco o cualquier texto que refleje sus principios básicos permitirá tanto a los usuarios como a los profesionales de seguridad tener un "panorama completo" de la seguridad; si bien muchas amenazas pueden evitarse, el riesgo es inevitable, aunque la corrección sea rápida. El objetivo es minimizar el tiempo de resolución cuando existe un alto riesgo y no centrarse solo en el intento de evitar estos eventos.

Acerca de Cisco

Cisco presta seguridad cibernética al mundo real a través de una de los portafolios de soluciones de protección avanzada contra amenazas más integrales de la industria contra la gama más amplia 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 Collective Security Intelligence (CSI) reúnen, bajo una misma estructura, la inteligencia contra amenazas líder de la industria con la telemetría obtenida de la enorme impronta de dispositivos y sensores, fuentes públicas y privadas, y la comunidad de fuente abierta de Cisco. Esto equivale a un ingreso diario de miles de millones de solicitudes web y millones de correos electrónicos, muestras de malware e intrusiones en las redes.

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

El ecosistema CSI consta de varios grupos con distintas personerías: TALOS, Organización de Fideicomiso y Seguridad, Defensa Controlada contra Amenazas (MTD) y Operaciones e Investigación de Seguridad (SR&O).

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

Apéndice

Descubrimientos adicionales del Estudio comparativo de capacidades de seguridad

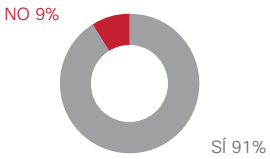
Recursos

¿Forma parte del presupuesto de TI el presupuesto de seguridad? Miembros del departamento de TI; C = 1720

Operaciones, procedimientos y políticas de seguridad

Los ejecutivos de mayor jerarquía responsables de la seguridad generalmente son los CISO o CSO.

¿Cuenta su organización con un ejecutivo con responsabilidad directa sobre la seguridad?
Encuestados que informaron responsabilidades y funciones claras; C =1603



Puesto del ejecutivo
Encuestados que informaron un ejecutivo con responsabilidad sobre la seguridad; C = 1465

La industria sanitaria es menos propensa que otras industrias a identificar un ejecutivo con responsabilidad sobre la seguridad.

Casi dos tercios dijeron que los líderes ejecutivos consideran la seguridad como una alta prioridad.

Participación de los ejecutivos C = 1738	SecOps C = 797			CISO C = 941		
	En desacuerdo/	De acuerdo/	Totalmente de acuerdo	En desacuerdo/	De acuerdo/	Totalmente de acuerdo
Los líderes ejecutivos de mi organización consideran a la seguridad como una alta prioridad.	8%	34%	58%	3%	30%	67%
El equipo ejecutivo de mi organización tiene responsabilidades y funciones de seguridad claras.	9%	39%	52%	2%	32%	64%
El equipo ejecutivo de mi organización ha establecido métricas claras para evaluar la eficacia de nuestro programa de seguridad.	11%	44%	45%	4%	37%	59%

Muchos encuestados que informaron no haber tenido que manejar el escrutinio público tras una falla de seguridad en la organización coinciden plenamente en que “los líderes ejecutivos de la organización consideran la seguridad como una alta prioridad”.

Altas proporciones informan procesos de seguridad que fomentan la participación de los empleados.

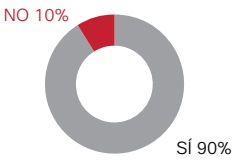
Procesos de seguridad C = 1738	SecOps C = 797			CISO C = 941		
	En desacuerdo/	De acuerdo/	Totalmente de acuerdo	En desacuerdo/	De acuerdo/	Totalmente de acuerdo
Se estimula a los gerentes de la línea de negocios a contribuir a los procedimientos y las políticas de seguridad.	12%	39%	49%	6%	40%	54%
Mi organización es capaz de detectar las debilidades de seguridad antes de que se conviertan en incidentes completos.	13%	43%	44%	4%	39%	57%
Se estimula a los empleados de mi organización a informar las fallas y los problemas de seguridad.	11%	34%	55%	4%	36%	60%
Los procedimientos y procesos de seguridad de mi organización son claros e inequívocos.	13%	39%	48%	4%	37%	59%
Los procesos de seguridad de mi organización nos permiten anticipar y mitigar los posibles problemas de seguridad de forma proactiva.	14%	40%	46%	3%	40%	47%
Los procesos de seguridad de mi organización se miden y controlan mediante datos cuantitativos.	13%	40%	47%	4%	35%	61%
Mi organización ha optimizado sus procesos de seguridad y ahora se centra en la mejora de dichos procesos.	12%	42%	46%	4%	36%	60%

Los profesionales de seguridad de las organizaciones medianas tienden a expresar mayores niveles de acuerdo respecto de los elementos de los procesos de seguridad que los profesionales de las grandes empresas.

Nueve de diez encuestados dijeron que se proporciona capacitación en seguridad periódica a los empleados de seguridad, generalmente a cargo del equipo de seguridad.

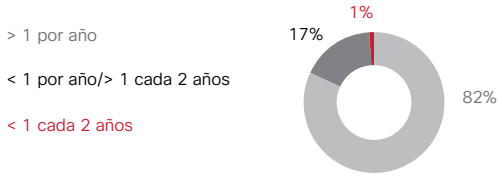
¿Se proporcionan programas de capacitación o concientización sobre seguridad al personal de seguridad periódicamente?

Encuestados dedicados a la seguridad; C = 1726



¿Con qué frecuencia se proporciona capacitación en seguridad?

Encuestados dedicados a la seguridad; C = 1556

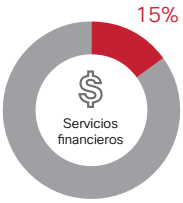


¿Quién presta la capacitación en seguridad?

Encuestados cuyos equipos de seguridad reciben capacitación; C = 1556

Equipo de seguridad interno 79% | Contratistas de terceros 38% | Recursos Humanos 25% | Otros empleados 10% | Otros 1%

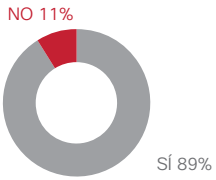
El 15% de los profesionales de servicios financieros dijo que la capacitación en seguridad no se ofrece periódicamente.



El personal comúnmente asiste a conferencias o capacitaciones, aproximadamente dos tercios respondieron que participan en asociaciones de seguridad de la industria.

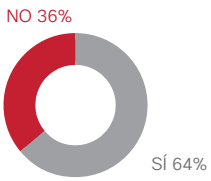
¿Asisten los miembros del personal de seguridad a conferencias o capacitaciones externas para mejorar y mantener sus habilidades?

Encuestados dedicados a la seguridad; C = 1715



¿Desempeñan funciones los empleados en comités o juntas de seguridad?

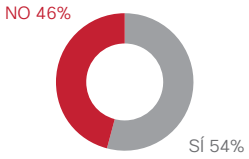
Encuestados dedicados a la seguridad; C = 1690



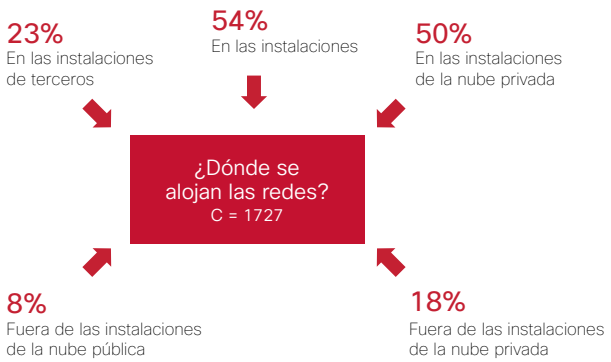
Más de la mitad de los encuestados dijo que su organización ha debido manejar el escrutinio público tras una falla de seguridad.

¿Ha debido su organización manejar alguna vez el escrutinio público tras una falla de seguridad?

Encuestados dedicados a la seguridad; C = 1701



El alojamiento de las redes en las instalaciones de la organización es más común; menos de una organización cada diez informa el alojamiento en la nube pública.



Una cantidad significativa de encuestados de SecOps dijo que en su organización se utiliza el alojamiento fuera de las instalaciones (tanto en la nube pública como privada) en comparación con los CISO.

Sofisticación

Los segmentos varían previsiblemente en muchas medidas de sofisticación de la seguridad...

	Bajo	Medio-Bajo	Medio	Medio-Alto	Alto
Los ejecutivos de las compañías consideran la seguridad como una alta prioridad...	22%	38%	45%	71%	81%
y tienen métricas claras para evaluar la eficacia de los programa de seguridad.	17%	19%	32%	52%	79%
La compañía tiene procedimientos y procesos de seguridad claros e inequívocos...	0%	22%	15%	72%	88%
que se miden y controlan a través de datos cuantitativos.	0%	17%	33%	65%	76%
y revisa regularmente las herramientas y las prácticas de seguridad para garantizar que estén actualizadas y sean eficaces.	0%	17%	33%	65%	76%
La compañía lleva a cabo un trabajo excelente en el manejo de la seguridad de RR. HH. mediante procesos buenos e integrados para las transferencias y las salidas...	16%	27%	36%	52%	76%
y lleva a cabo clasificaciones e inventarios claros de los activos de información.	17%	26%	40%	58%	73%
y protege bien a las instalaciones informáticas de la organización.	17%	21%	41%	63%	80%
Las tecnologías de seguridad están bien integradas a fin de trabajar eficazmente en conjunto...	17%	21%	38%	59%	78%
y la compañía es capaz de detectar las debilidades de seguridad antes de que se conviertan en incidentes completos.	0%	23%	25%	63%	70%

Pero no en todas...

	Bajo	Medio-Bajo	Medio	Medio-Alto	Alto
Hay un ejecutivo con responsabilidad directa sobre la seguridad.	85%	91%	88%	93%	93%
La compañía cuenta con una estrategia de seguridad formal escrita para toda la organización que se revisa periódicamente.	59%	47%	58%	65%	60%
La compañía sigue una práctica de política de seguridad de la información estandarizada, como ISO 27001.	47%	44%	50%	59%	54%

Notas finales

1. *Informe de seguridad de mitad de año de 2014 de Cisco:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
2. Para obtener más información sobre las vulnerabilidades de los CMS, consulte "Vulnerabilidades de Wordpress: ¿Quién cuida la tienda?" en el *Informe de seguridad de mitad de año de 2014 de Cisco:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
3. "Actividad de los kits de aprovechamiento de vulnerabilidades Goon/Infinity/RIG", Cisco IntelliShield: boletín informativo de actividades de seguridad, julio de 2014: http://tools.cisco.com/security/center/mviewAlert.x?alertId=34999.
4. *Informe de seguridad de mitad de año de 2014 de Cisco:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
5. "Respuesta a eventos de Cisco: vulnerabilidad de POODLE", 15 de octubre de 2014: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Poodle_10152014.html.
6. "Vulnerabilidad Heartbleed de OpenSSL CVE-2014-0160 – Productos y soluciones de mitigación de Cisco", blog de seguridad de Cisco, 9 de abril de 2014: http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations.
7. "JP Morgan y otros bancos atacados por piratas informáticos", por Nicole Perlroth, *The New York Times,* 27 de agosto de 2014: http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=0; "Error de 'caballo de Troya' oculto en computadoras estadounidenses vitales desde 2011", por Jack Cloherty y Pierre Thomas, ABC News, 6 de noviembre de 2014: http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.
8. "Cuatro aspectos aprendidos del 4.º pleno de China", por Shannon Tiezzi, *The Diplomat,* 23 de octubre de 2014: http://thediplomat.com/2014/10/4-things-we-learned-from-chinas-4th-plenum/.
9. "La nueva ley de Internet de Brasil puede afectar ampliamente la privacidad en línea y las prácticas de manipulación de datos", *Chronicle of Data Protection,* 16 de mayo de 2014: http://www.hldataprotection.com/2014/05/articles/international-eu-privacy/marco-civil-da-internet-brazils-new-internet-law-could-broadly-impact-online-companies-privacy-and-data-handling-practices/.
10. "La ley de localización de datos rusa entrará en vigencia un año antes de lo previsto en septiembre de 2015", por Hogan Lovells, Natalia Gulyaeva, Maria Sedykh y Bret S. Cohen, Lexology.com, 18 de diciembre de 2014: http://www.lexology.com/library/detail.aspx?g=849ca1a9-2aa2-42a7-902f-32e140af9d1e.
11. "El director del GCHQ acusa a los gigantes tecnológicos estadounidenses de convertirse en 'redes opcionales' de los terroristas", por Ben Quinn, James Ball y Dominic Rushe, *The Guardian,* 3 de noviembre de 2014: http://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan.
12. "La seguridad de Internet es necesaria para la economía tecnológica mundial", por Mark Chandler, blog de Cisco, 13 de mayo de 2014: http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy.
13. "Seguridad cibernética: Qué preguntas deben formular las juntas de directores", ISACA y Fundación de Investigación del Instituto de Auditores Internos, agosto de 2014: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx.
14. "Es hora de que las juntas corporativas aborden la seguridad cibernética. Descubra por qué", por Andrew Nusca, revista FORTUNE, 25 de abril de 2014: http://fortune.com/2014/04/25/its-time-for-corporate-boards-to-tackle-cybersecurity-heres-why/.

Sede central en América
Cisco Systems Inc.
San José CA

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

Sede Central en Europa
Cisco Systems International BV
Ámsterdam, Países Bajos

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