# INFORME DE SEGURIDAD 2013 DE CHECK POINT

ENERO DE 2013

Check Point®
SOFTWARE TECHNOLOGIES LTD.

# INFORME DE SEGURIDAD CHECK POINT 2013

# 01 INTRODUCCIÓN Y METODOLOGÍA

**"AL IGUAL QUE EL AGUA NO MANTIENE UNA FORMA CONSTANTE, TAMPOCO EN LA GUERRA SE DAN CONDICIONES CONSTANTES"** [1]

AUNQUE ESTA FRASE SE PRONUNCIÓ HACE 2600 AÑOS, SORPRENDETEMENTE SIGUE SIENDO MÁS QUE RELEVANTE, REFLEJANDO LA GUERRA ACTUAL – LA CIBER GUERRA.

Las técnicas de los hackers cambian constantemente, empleando métodos más avanzados y sofisticados de ataque, elevando las necesidades de seguridad a nuevos niveles. Los centros de datos, ordenadores y teléfonos móviles de empleados, son los primeros objetivos de los hackers, sembrando una amplísima variedad de malware como bots, troyanos y descargas ocultas. Los hackers recurren a las tretas y la ingeniería social, manipulando a usuarios inocentes, para acceder a información corporativa como documentación interna, registros financieros, números de tarjetas de crédito y credenciales de usuario, o simplemente para hacer caer servicios mediante ataques de denegación de servicio. Esta guerra moderna de engaños y ataques sofisticados es una realidad y va a perdurar. La cantidad de información corporativa almacenada en centros de datos, servidores, PCs y teléfonos móviles crece a velocidad de vértigo, y el mayor volumen de datos y plataformas implica mayor riesgo. Por último, la lista de amenazas de seguridad no es precisamente corta, revelando cada nuevo ataque mayor nivel de sofisticación. ¿Cuáles fueron los riesgos principales que afrontó su entorno de red el año pasado? ¿A qué riesgos estará expuesto el año que viene? Estas fueron las cuestiones principales que mantuvieron ocupado al equipo de investigación en seguridad de Check Point los últimos meses. Buscando respuestas a estas preguntas, Check Point ha efectuado un análisis de seguridad intensivo.

## Metodología

El Informe de Seguridad 2013 de Check Point está basado en la investigación cooperativa y análisis de incidentes de seguridad obtenidos de cuatro fuentes principales de informe: Check Point Security Gateways Analysis Reports [2], Check Point ThreatCloud© [3], Check Point SensorNet© y Check Point Endpoint Security.

Se efectuó un análisis global de los incidentes de seguridad de la red de 888 compañías a partir de los datos recopilados por los Check Point Security Gateways, que inspeccionan el tráfico de red entrante y saliente en tiempo real. Se inspeccionó el tráfico mediante la tecnología multinivel Software Blades de Check Point para identificar un abanico de amenazas de seguridad como aplicaciones de alto riesgo, intentos de intrusión, virus y bots, pérdida de datos sensibles, etc. Se monitorizó el tráfico de red en tiempo real implementando Check Point Security Gateway en línea o en el modo de monitorización (tap).

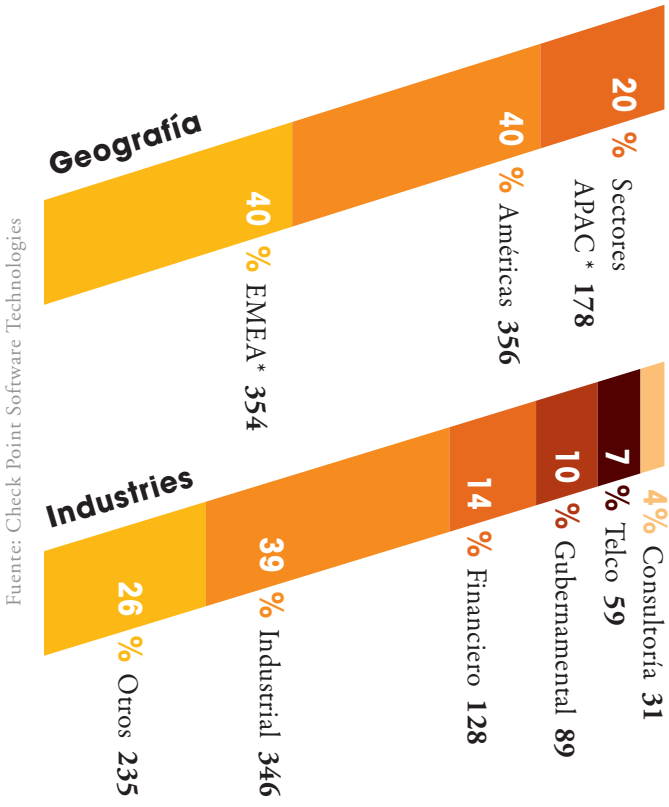
De media, se monitorizó el tráfico de red de cada organización durante 134 horas. Las empresas recogidas en nuestros informes pertenecen a un amplio repertorio de negocios localizados por todo el mundo como se ilustra en las gráficas 1-A y 1-B.

Además, se analizaron 111,7 millones de eventos procedentes de 1494 Security Gateways empleando los datos generados por ThreatCloud© de Check Point. ThreatCloud es una base de datos de seguridad actualizada en tiempo real y alimentada con los datos de una gran red de sensores globales, emplazados estratégicamente por todo el mundo que recogen información sobre amenazas y ataques de malware. ThreatCloud permite la identificación de tendencias y amenazas globales de seguridad, creando una red cooperativa para luchar contra el cibercrimen. En esta investigación se analizaron datos provenientes de ThreatCloud que se recopilaron durante un periodo de tres meses entre agosto y octubre de 2012.

En lo referente a datos de amenazas, estos se recopilaron de la red de sensores SensorNet© de Check Point entre el uno de julio y el 30 de septiembre de 2012. SensorNet de Check Point es una red de sensores distribuida por todo el mundo que proporciona información de seguridad y estadísticas de tráfico a un sistema de análisis centralizado. Se analizan estos datos para detectar tendencias y anomalías, así como para elaborar una vista en tiempo real de la seguridad por todo el mundo.

Por último, se consideró el análisis de 628 informes de seguridad de controles procedentes de una gran variedad de organizaciones. Los análisis de seguridad incluyeron la exploración de cada host para valorar los riesgos de pérdida de datos, riesgos de intrusión y por malware. Los análisis se efectuaron con la herramienta de informes Endpoint Security de Check Point verificando si se estaba ejecutando el antivirus en el host, si el antivirus estaba actualizado, si se ejecutaba la última versión del software y otros parámetros. La herramienta es gratuita y de libre acceso, pudiendo descargarse del sitio Web público de Check Point [4].

Este informe está basado en los datos recopilados de estas fuentes.




**Gráfica 1-A**

**APAC - Asia, Pacífico y Japón. EMEA – Europa, Oriente medio y África.**

## Especificaciones de sectores

Industrial – Química / Refinerías, Salud, Farmacéutica, Informática, Fabricación, Transporte, Utilidades, Infraestructuras.
Financiero – Finanzas, Contabilidad, Banca, Inversiones. Gobierno – Gobierno, Defensa.
Telco – Telco, Proveedores de servicios, ISP, MSP.
Consultoría – Servicios de consultoría
Otros – Publicidad / Medios, Distribución, Educación, Abogacía, Tiempo libre / Hoteles, Venta minorista y mayorista, Seguridad, Otros.

# 02 AMENAZAS PARA SU EMPRESA

### Últimas noticias: Se ha descubierto un nuevo ciberataque

En 2012 continuaron proliferando los ciberataques y los titulares. Amenazas de software malicioso, ataques y redes de bots son noticias de portada casi a diario, poniendo en evidencia el infame éxito de los hackers robando información, paralizando operaciones, y espiando a empresas y gobiernos. Los siguientes ejemplos son sólo la punta del iceberg de los ciberataques producidos durante 2012: Los hackers atacaron la red [6] de la Casa Blanca, el grupo de activistas Anonymous hizo caer los sitios Web de grupos de empresas como U.S. Telecom Association y TechAmerica [7], los ciberataques afectaron también a Capital One Financial Corp., BB&T Corp., y HSBC Bank USA [8], entre otros.

### Amenazas persistentes avanzadas

Los cibercriminales no son ya amateurs aislados. En muchos casos pertenecen a organizaciones bien estructuradas, similares a células terroristas – sus fundamentos son sólidos y tienen motivación y objetivos. Los cibercriminales parecen dedicar una considerable cantidad de tiempo y recursos a recopilar información. Sus actividades criminales causan daños severos a las organizaciones como: pérdida de datos confidenciales, interrupciones del negocio, perjuicios de reputación y, desde luego, pérdidas económicas. Los ataques más sofisticados y de larga duración, están dirigidos a un objetivo predeterminado muy específico, refiriéndonos a ellos como Advanced Persistent Threats (APT). Estos ataques raramente los detectan los sistemas de seguridad tradicionales, poniendo a gobiernos, empresas, pequeños negocios e incluso redes personales en riesgo.

> "SÓLO EXISTEN DOS TIPOS DE COMPAÑÍAS, LAS QUE YA HAN SIDO ATACADAS Y **LAS QUE LO SERÁN"**
>
> Robert Mueller, Director, FBI, MARZO, 2012

## BLACKHOLE
## UN KIT EXPLOIT PARA LAS MASAS

Parte del gran incremento de la actividad maliciosa en el pasado año puede atribuirse a que los hackers se sirven fácilmente de herramientas y paquetes estándar. Con un clic cualquiera puede descargar una sofisticada suite de ataque repleta de opciones. Una de estas suites es el kit BlackHole – un paquete de software muy extendido basado en Web. BlackHole incluye una colección de herramientas que sacan partido de las vulnerabilidades de seguridad de los navegadores Web para descargar virus, bots, troyanos y otras variantes de software malicioso a los ordenadores de víctimas desprevenidas. Los precios de estos kits van de los 50 $ para usar un día, hasta los 1.500 $ para todo el año [9].

# INCIDENTES DE VIOLACIÓN DE DATOS EN 2012

Este año tuvieron lugar numerosos incidentes de violación de datos, exponiendo datos alojados en servidores corporativos relativos a tarjetas de crédito, clientes, estudiantes o datos de pacientes. Estas actividades maliciosas comparten como objetivo común hacerse con información confidencial. La siguiente lista nos ilustra algunos ejemplos:

**Global Payments Inc.**
Esta pasarela global de pagos resultó atacada en junio de 2012. Se sustrajeron sobre 1,5 millones de datos de tarjetas de crédito.

**Clarksville Tennessee U.S.**
En junio de 2012 los hackers entraron en el sistema de Clarksville- Montgomery County School para sustraer los nombres, números de Seguridad Social, y otros datos personales de unas 110.000 personas. Los hackers aprovecharon la información publicada por empleados y estudiantes en Internet para acceder al sistema [10].

**Serco Thrift Savings Plan**
En mayo de 2012 un ataque contra Serco en los Estados Unidos, dio como resultado la sustracción de los datos de 123.000 empleados federales.

**University of Nebraska**
Fue víctima de un robo de datos consistente en la sustracción de unos 650.000 archivos con datos de personal relativos a estudiantes, padres y empleados de la universidad de la base de datos de Nebraska Student Information Systems.

**U.S. Utah Dept. of Technology Services**
En marzo de 2012 se sustrajeron los datos médicos de 780.000 pacientes alojados en un servidor. Se piensa que el ataque provenía de más allá de Europa del este.

**National Health Service de Reino Unido**
Entre julio de 2011 y julio de 2012, el National Health Service del Reino Unido fue víctima de varios ataques que expusieron los registros de casi 1,8 millones de pacientes [11].

En los ataques APT, la primera acción que se ejecuta típicamente es efectuar un reconocimiento para recopilar información sobre el objetivo. Los atacantes efectúan una intrusión inicial en la red objetivo para abrir una puerta trasera y mantenerse de forma prolongada en la misma. Normalmente esto se lleva a cabo infectando el host con un bot, que permite al atacante comunicarse con el host infectado sin ser detectado. El atacante trata entonces de aumentar su penetración en la red, extendiéndose incluso a otros nodos. Tras este paso el atacante ha logrado su objetivo, puesto que puede acceder a los hosts infectados para sustraer datos o causarles daños remotamente, manteniendo la persistencia pensando en el largo plazo.

SE VENDEN HERRAMIENTAS ESPÍA POR INTERNET POR UNOS 500 $, MIENTRAS QUE LOS DAÑOS OCASIONADOS CUESTAN A LOS NEGOCIOS **MILLONES DE DÓLARES**

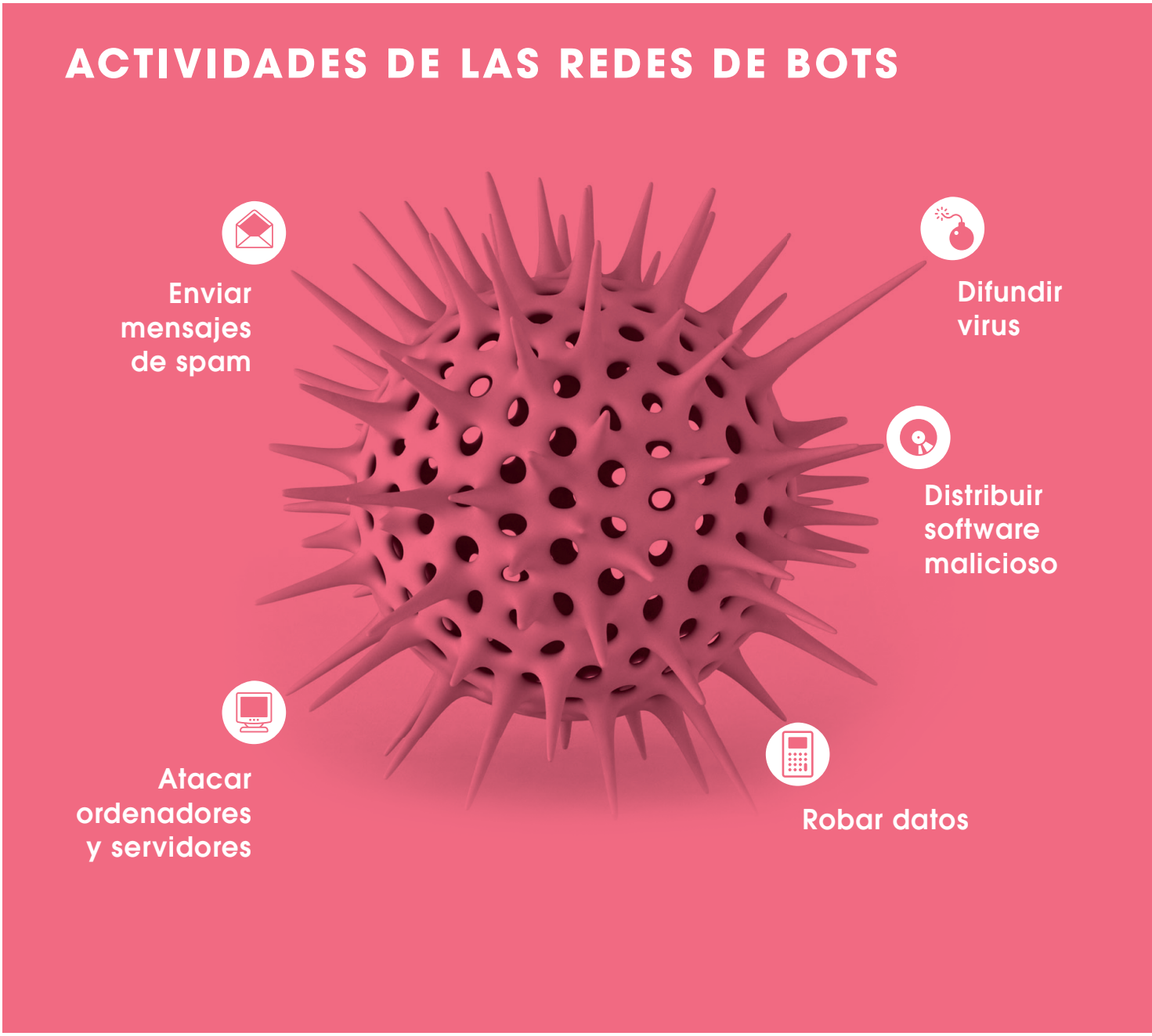
## Las redes de bots se instalan para mantenerse activas

Las redes de bots (botnets) se cuentan entre las amenazas más significativas de la seguridad a las que tienen que hacer frente las empresas. Un bot es un software malicioso que invade e infecta un ordenador (zombie) para permitir a los delincuentes controlarlo remotamente. El ordenador infectado puede desarrollar actividades ilegales, como: sustraer datos, distribuir spam, expandir malware y participar en ataques de Denegación de Servicio (DoS). El propietario del ordenador infectado puede ser

perfectamente ignorante de estas actividades. Los bots juegan también un papel protagonista en los ataques APT dirigidos.

Existen dos grandes tendencias en el perfil de las amenazas actuales dirigidas por ataques de bots. En el primer grupo se encuentra la creciente industria del cibercrimen orientado a los beneficios – en éste se encuadran cibercriminales, operadores de malware, proveedores de herramientas, codificadores y programas afiliados. Sus "productos" se pueden pedir fácilmente por Internet desde numerosos sitios Web (por ejemplo, kits malware hágalo Vd. mismo, envío de spam, robo de datos y ataques de Denegación de Servicio) encontrando dificultades las organizaciones para librarse de esta clase de ataques. El segundo grupo es ideológico y está dirigido a los estados, teniendo como objetivo a personas y organizaciones para promover causas políticas o desarrollar campañas de ciberguerra.

Las redes de bots están aquí para quedarse. En contraposición a los virus y otros malware tradicionales estáticos, (cuyo código y forma se mantienen estables), las redes de bots son dinámicas por naturaleza, pudiendo cambiar rápidamente de forma y patrones de tráfico. Los kits de bots se venden por



# EL 63% DE LAS ORGANIZACIONES DE NUESTRO ESTUDIO ESTABAN INFECTADAS CON BOTS

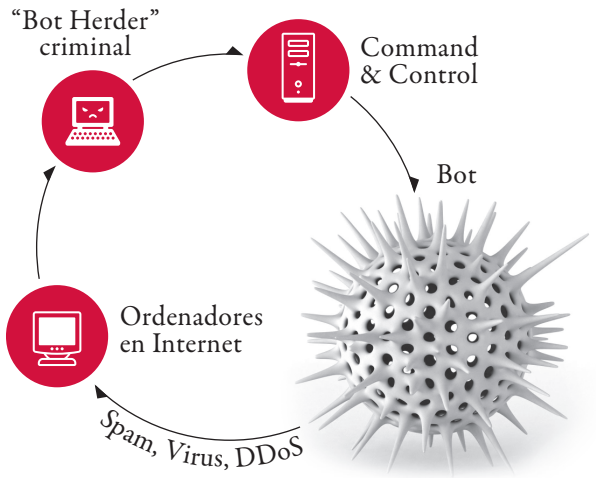
Internet desde 500 $, y sus ataques cuestan a los negocios millones de dólares. El problema de los bots se ha convertido en una cuestión relevante.

### Las redes de bots están por todas partes pero, ¿cómo es la situación de crítica?

Se estima que un 25% de los ordenadores personales conectados a Internet pueden ser parte de una red de bots [12]. Nuestra reciente investigación revela que en un 63% de las organizaciones se ha encontrado, al menos, un bot. La mayoría de las organizaciones estaban infectadas por varios bots.

### Cómo trabajan las redes de bots

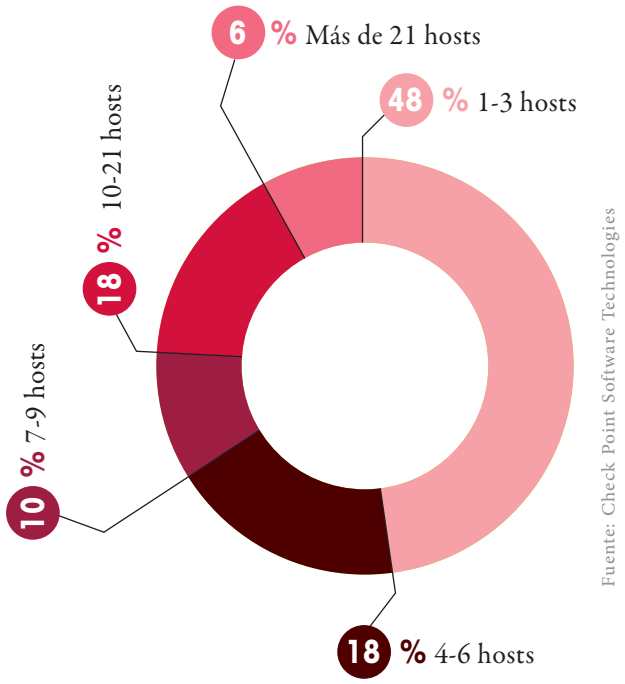
Típicamente una red de bots cuenta con un número de ordenadores infectados con software malicioso, que establece una conexión de red con un sistema o sistemas de control, conocidos como servidores Command & Control.




Cuando un ordenador resulta infectado por un bot, éste toma el control del ordenador y neutraliza las defensas del antivirus. Los bots resultan difíciles de identificar porque se esconden dentro del ordenador cambiando la forma en la cual se muestran de cara al software antivirus. El bot conecta entonces con el centro Command & Control (C&C) para recibir las instrucciones de los cibercriminales. Para este

### Número de hosts infectados con bots

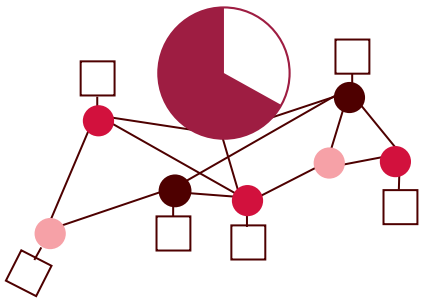
(% de organizaciones)




**Gráfica 2-A**

tipo de conexiones se emplean multitud de protocolos de comunicaciones diferentes, incluyendo Internet Relay Chat (IRC), HTTP, ICMP, DNS, SMTP y SSL, y en algunos casos protocolos personalizados creados por los desarrolladores del software del bot.

**CADA 21 MINUTOS**
UN BOT SE COMUNICA CON SU CENTRO COMMAND & CONTROL

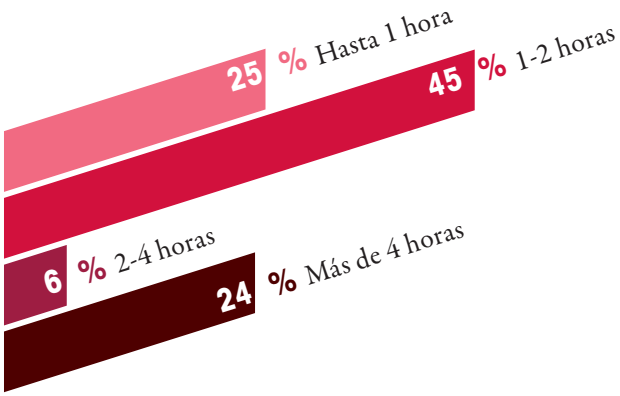


## Actividad Command & Control

Los bots se presentan con aspectos y formas muy diferentes, pudiendo ejecutar gran variedad de actividades. En muchos casos, un solo bot puede crear múltiples amenazas. Una vez que está gobernado por el servidor Command & Control, la red de bots puede ser dirigida en el ordenador infectado para desarrollar actividades ilegales sin conocimiento del usuario. Estas actividades incluyen: infectar más máquinas para añadirlas a la red de bots, efectuar envíos masivos de spam, ataques DDoS y sustracción de datos personales, financieros, y datos confidenciales de la empresa de la red de bots. A menudo los bots se utilizan también como herramientas en ataques APT en los que los cibercriminales seleccionan individuos u organizaciones a atacar. La gráfica 2-B ilustra la frecuencia de comunicación de los bots con sus centros Command & Control. El 70% de los bots detectados durante el estudio comunicaron con sus centros Command & Control, al menos, una vez cada dos horas. La mayoría de las actividades Command & Control están localizadas en los Estados Unidos, seguidos por Alemania, Holanda y Francia, como se ilustra en la gráfica 2-C.

Los distintos tipos de comunicación de los bots con sus centros Command & Control incluyen: informes de nuevos hosts que han resultado infectados, mensajes de correcto funcionamiento, y recopilación de datos del sistema host. Nuestra investigación revela que, de media, los bots se comunican con su centro Command & Control cada 21 minutos.

### Frecuencia de comunicación de los bots con su centro Command & Control




Fuente: Check Point Software Technologies

**Gráfica 2-B**

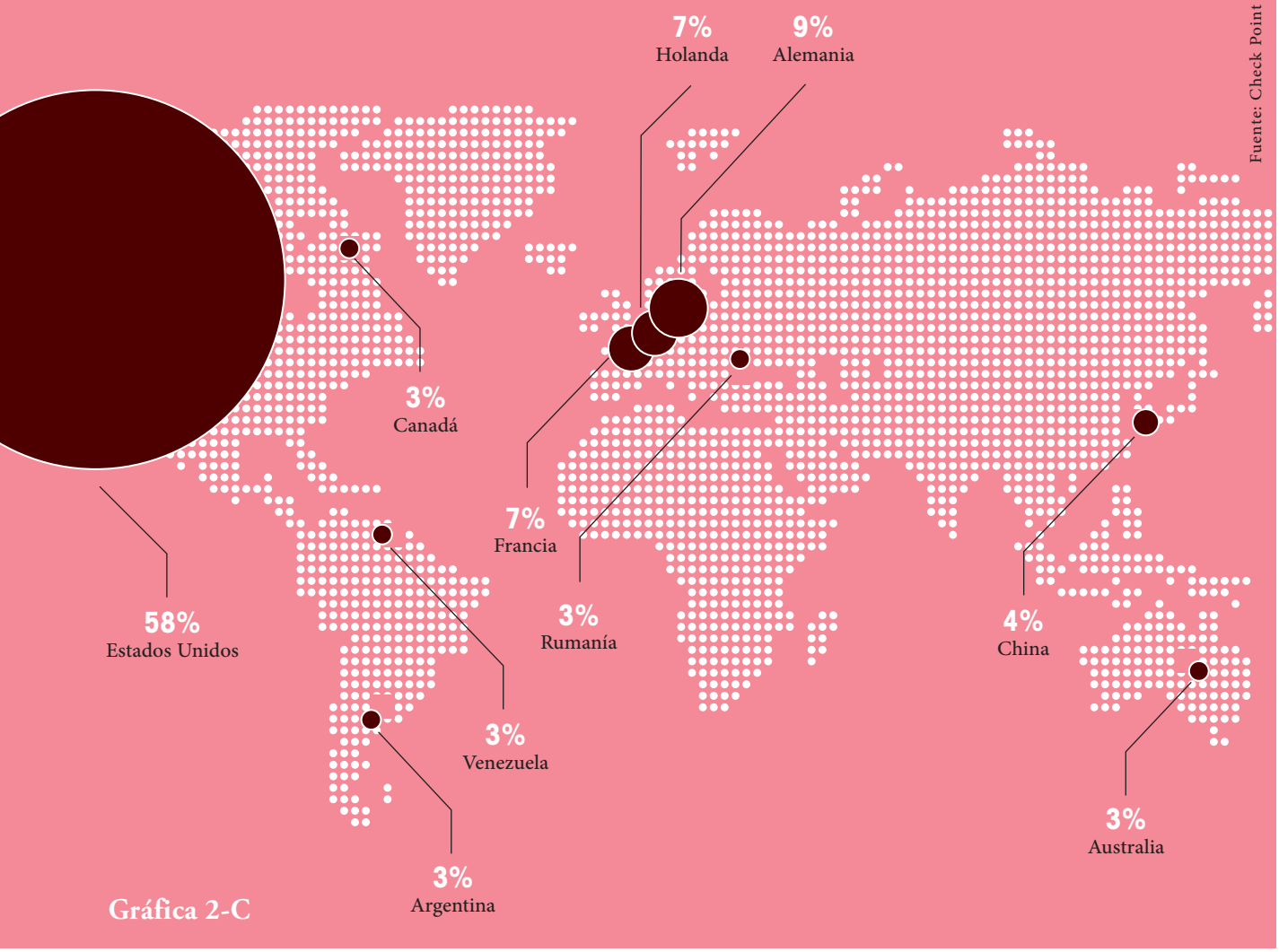
## ¿A qué redes de bots deberíamos estar atentos?

Actualmente están desplegadas miles de redes de bots. La siguiente tabla muestra las redes de bots o botnets más relevantes localizadas durante nuestro estudio. Para comprender mejor la transcendencia de estas amenazas, puede encontrarse información adicional sobre cada una de ellas en el Apéndice A.

| Familia de redes de bots | Actividad maliciosa |
|---|---|
| **Zeus** | Sustracción de credenciales bancarias en línea |
| **Zwangi** | Presentación al usuario de mensajes publicitarios no deseados |
| **Sality** | Autodifusión de virus |
| **Kuluoz** | Ejecución remota de archivos maliciosos |
| **Juasek** | Acciones maliciosas remotas: abrir la ventana de comandos, buscar, crear y eliminar archivos y más |
| **Papras** | Sustraer información financiera y obtener acceso remoto |

**Ver detalles adicionales en el Apéndice A**

## UBICACIÓN DE PAÍSES CON MÁS COMMAND & CONTROL




Fuente: Check Point Software Technologies

Gráfica 2-C

# EN EL 75% DE LAS ORGANIZACIONES UN HOST ACCEDE A UN SITIO WEB MALICIOSO

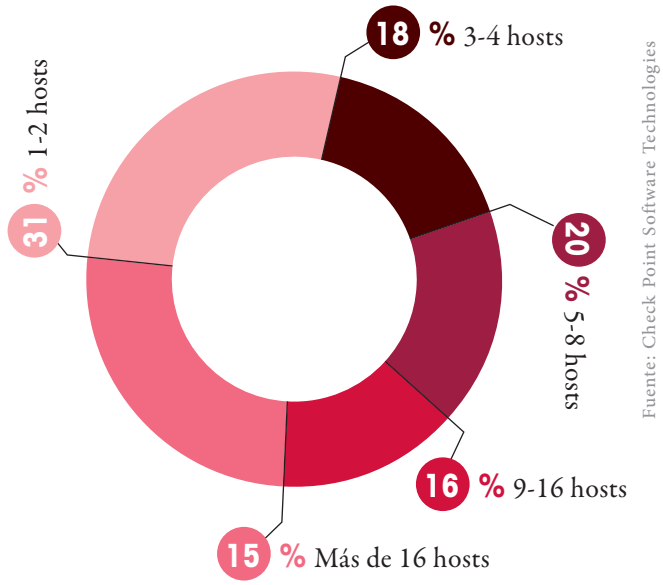
## **CADA 23 MINUTOS** UN HOST ACCEDE A UN SITIO WEB MALICIOSO

### Cómo puede su organización resultar infectada por malware

Existen múltiples puntos de entrada desde donde romper las defensas de la organización: vulnerabilidades basadas en navegador, teléfonos móviles, adjuntos maliciosos y soportes extraíbles, por nombrar algunos. Además, la explosión de aplicaciones Web 2.0 y redes sociales utilizadas como herramienta de negocio brindan a los hackers grandes oportunidades de encontrar víctimas que pulsen sobre enlaces maliciosos o en "malvertisement" – anuncios maliciosos que aparecen en sitios Web legítimos.
Aunque las redes de bots están llamadas a ser consideradas como una de las amenazas de red más relevantes de la actualidad, las organizaciones hacen frente a amenazas de seguridad adicionales procedentes del mundo del malware: virus, gusanos, spyware, adware, troyanos y demás. Nuestro estudio reveló que en el 75% de las organizaciones un host había accedido a un sitio Web malicioso.
El siguiente gráfico ilustra el número de hosts que accedieron a sitios Web maliciosos atendiendo al porcentaje de organizaciones. En aproximadamente el 50% de las organizaciones accedieron al menos 5 hosts a sitios Web maliciosos.

### Acceso a sitios Web maliciosos por número de hosts

(% de organizaciones)

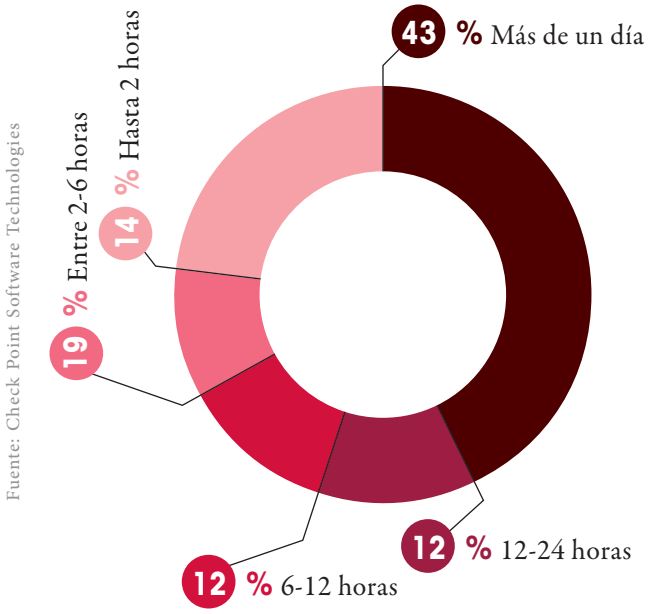



**Gráfica 2-D**

Un malware puede ser descargado por un usuario o por un bot que ya haya infectado al host. Apreciamos que en el 53% de las organizaciones se descargó malware de la propia red corporativa. En más del 50% de estas organizaciones, detectamos que habían descargado malware más de cuatro hosts. El siguiente gráfico circular ilustra la frecuencia promedio de descargas de malware en las organizaciones recogidas en nuestro estudio.

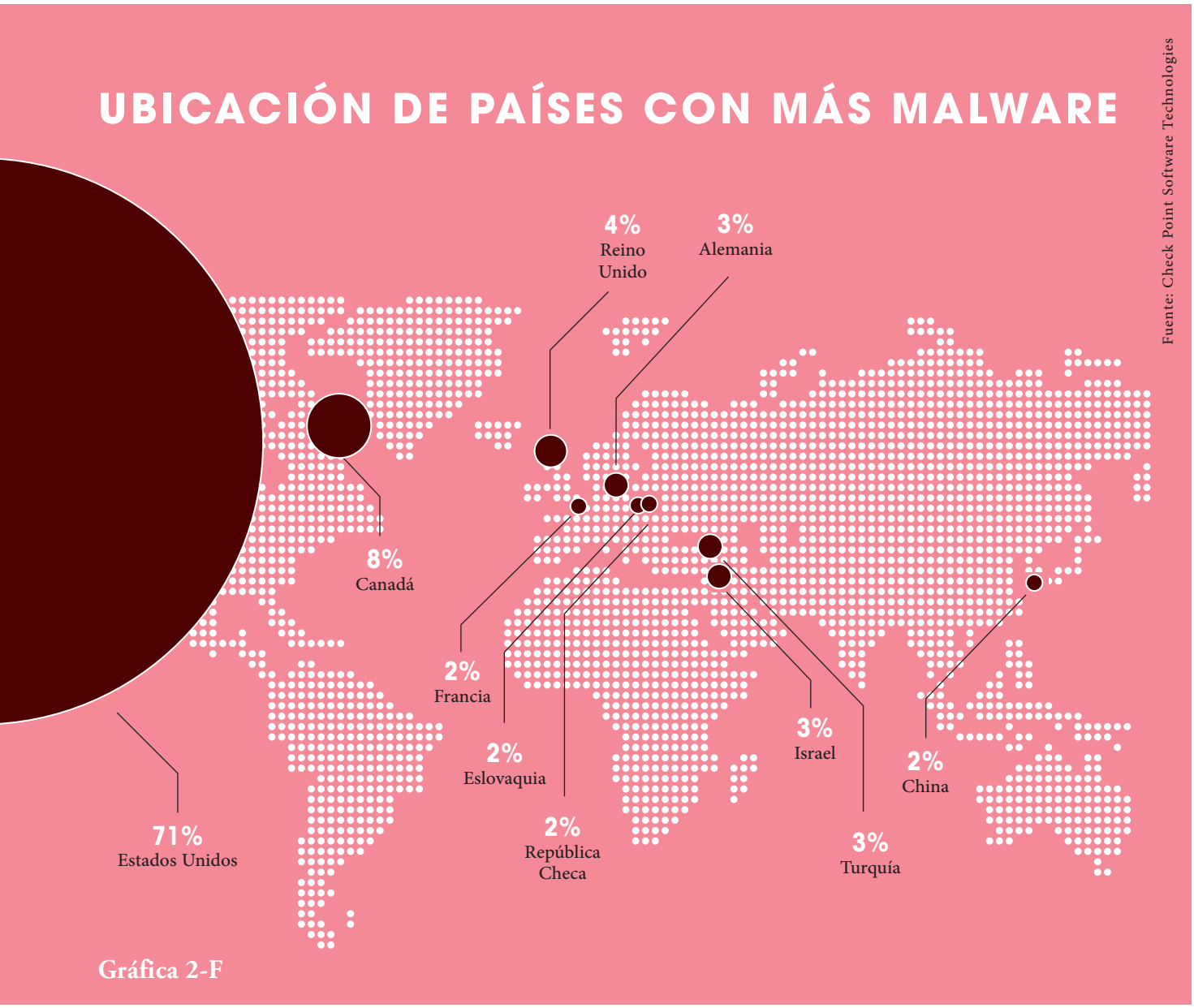
### Frecuencia de descarga de malware

(% de organizaciones)

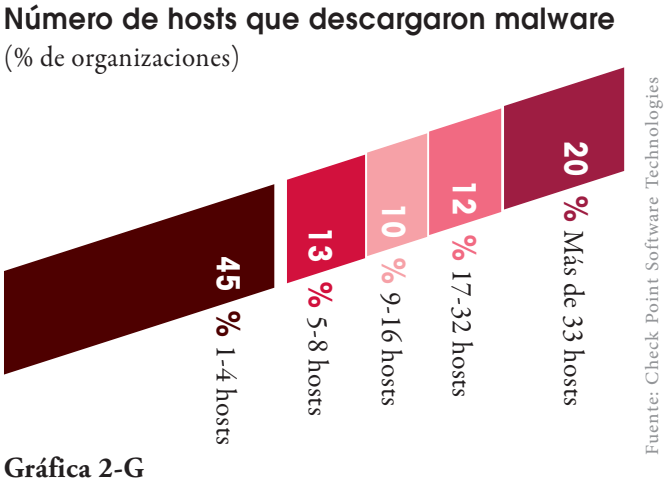



**Gráfica 2-E**

La gráfica 2-G representa el número de hosts que descargaron malware. En más del 50% de las organizaciones, al menos 5 hosts descargaron algún malware. En nuestro estudio, localizamos la mayoría del malware en los Estados Unidos, seguido de Canadá y Reino Unido, como se muestra en la gráfica 2-F.
La protección antivirus es uno de los métodos para luchar contra las infecciones de malware, aunque nuestro estudio revela que el 23% de los hosts de las organizaciones no actualizaban sus antivirus diariamente. Un host que no ejecute un antivirus actualizado está expuesto a los últimos virus. Desvelamos también que el 14% de los hosts de las organizaciones ni siquiera disponían de antivirus instalado en los ordenadores host. Los hosts que no ejecutan un antivirus se enfrentan a un gran riesgo potencial de infección por malware.




Gráfica 2-F




Gráfica 2-G

## Les presentamos a "miniFlame" el hermano pequeño, pero más peligroso, de Flame

Parece que Flame, que fue descubierto hace unos meses, era sólo el principio. Este año se descubrió un programa similar, denominado "miniFlame", que efectuó ataques más precisos sobre objetivos de Oriente medio. miniFlame incluye una "back door" que facilita el control remoto, sustracción de datos y la posibilidad de obtener capturas de pantalla.

# ATAQUE DE EUROGRABBER

## MÁS DE 36 MILLONES DE EUROS ROBADOS A MÁS DE 30.000 CLIENTES DE ENTIDADES BANCARIAS

Durante 2012 tuvo lugar un sofisticado ataque multidimensional robando según una estimación más de 36 millones de euros de entre más de 30.000 clientes bancarios entre múltiples bancos en Europa. De forma completamente transparente, los clientes de banca online no tenían ni idea de que estaban infectados con troyanos, y que sus sesiones de banca online estaban en compromiso o que se estaban robando fondos directamente desde sus cuentas. Esta campaña de ataques fue descubierta y denominada "Eurograbber" por Versafe y Check Point Software Technologies. El ataque Eurograbber emplea una variación nueva y exitosa de los troyanos ZITMO, o Zeus-In-The-Mobile. Hasta la fecha, esta vulnerabilidad solamente se ha detectado en países de la zona Euro, pero una variación de este ataque podría potencialmente afectar también a bancos en países fuera de la unión europea. El ataque en varias etapas infectó en principio ordenadores y dispositivos móviles de clientes de banca online, y una vez que los troyanos Eurograbber se instalaron en ambos dispositivos, las sesiones de banca online del cliente fueron monitorizadas y manipuladas completamente por los atacantes. Incluso el mecanismo de autenticación de dos factores usado en los bancos para garantizar la seguridad de las transacciones online fue burlado en el ataque y utilizado en realidad por los atacantes para autenticar sus transferencias ilícitas financieras.

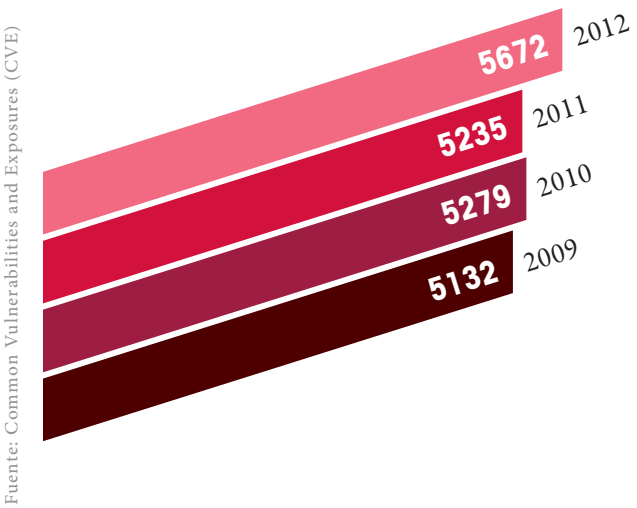
Es más, los troyanos usados para atacar los dispositivos móviles fueron desarrollados para plataformas BlackBerry y Android para facilitar un amplio "mercado objetivo", y como tal fueron capaces de infectar a usuarios de banca tanto corporativos como particulares y transferir de forma ilícita fondos fuera de las cuentas de los clientes en un rango de cantidades de entre 599 y 250.000 euros cada una. Puede encontrarse información adicional sobre el ataque Eurograbber, incluyendo un detallado paso a paso del ataque en el white paper[12] con el caso de estudio en el sitio web de Check Point.

### Más vulnerabilidades, más exploits

Las vulnerabilidades bien conocidas son los objetivos clave de los hackers, que confían en el simple hecho de que las organizaciones no actualizan su software de forma semanal. Cuanto más grande son las organizaciones, más difícil es para los administradores de seguridad mantener todos los sistemas completamente actualizados. Por ello, en muchos casos, una vulnerabilidad parcheada hace un año, puede utilizarse todavía para penetrar en los sistemas de grandes organizaciones que no han actualizado sus sistemas con las últimas actualizaciones y parches del software.

El enorme número de vulnerabilidades descubiertas cada año es abrumador, con más de 5.000[13] nuevas formas descubiertas para que los hackers causen daño y accedan a los sistemas en 2012, y todavía existen muchas vulnerabilidades más sin descubrir que están siendo utilizadas de forma activa por los ciberdelincuentes.

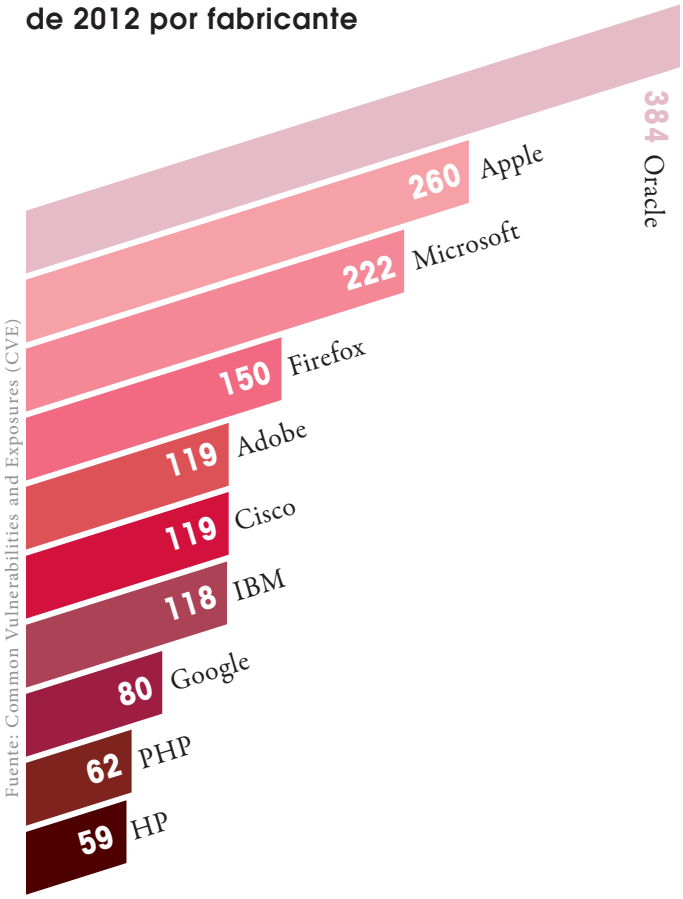
### Número total de vulnerabilidades y exposiciones comunes




**Gráfica 2-H**

La gráfica 2-I demuestra que los productos más populares utilizados por la mayoría de organizaciones en todo el mundo son también los más vulnerables – Oracle, Apple y Microsoft son los proveedores líderes en vulnerabilidad.

### Vulnerabilidades principales y riesgos de 2012 por fabricante



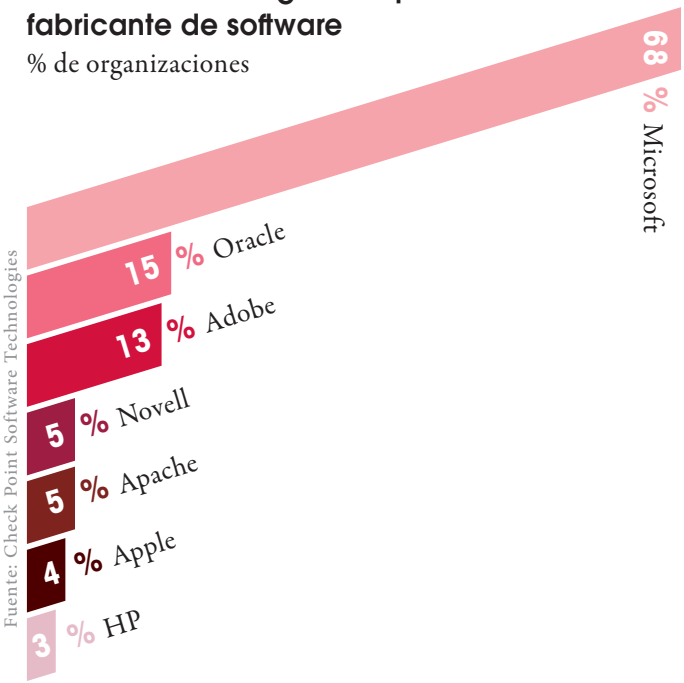

**Gráfica 2-I**

Nuestra investigación revela que el 75% de los hosts dentro de las organizaciones no utilizan las últimas versiones de software (por ejemplo: Acrobat Reader, Flash Player, Internet Explorer, Java Runtime Environment y otros muchos). La implicación de todo ello es que estos hosts están expuestos a un amplio espectro de vulnerabilidades que pueden ser aprovechadas por los hackers. Nuestra investigación también demuestra que el 44% de los hosts en las organizaciones no están ejecutando los últimos Service Packs de Microsoft Windows. Los Service Packs normalmente incluyen actualizaciones de seguridad para el sistema operativo. No estar ejecutando el último Service Pack implica estar en una situación de riesgo para la seguridad.

Además hemos descubierto que en el 68% de las organizaciones se encontraron incidentes de seguridad relacionados con productos Microsoft. Las incidencias para la seguridad relativas a otros fabricantes de software como Adobe y Apple, se encontraron en menos organizaciones. Es interesante observar que aunque Apple es la segunda en cantidad de vulnerabilidades, solamente un pequeño porcentaje de organizaciones han tenido incidencias relativas a productos Apple.

### Incidencias de seguridad por fabricante de software

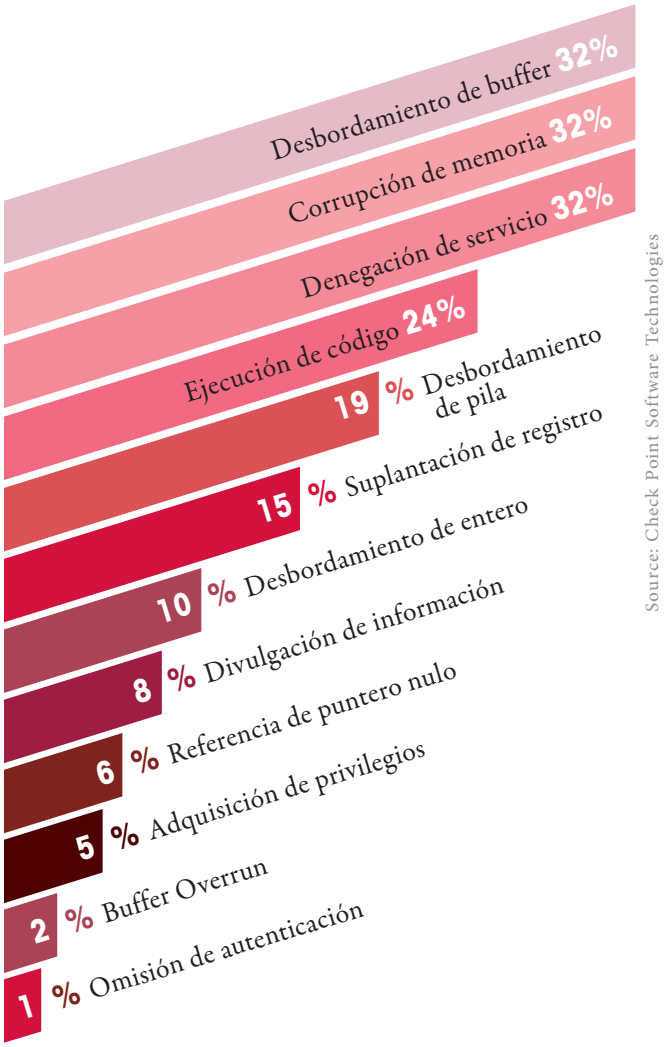
% de organizaciones




**Gráfica 2-J**

Los hackers utilizan diversas técnicas a las que se refieren como vectores de ataque. La gráfica 2-K enumera algunos de estos vectores de ataque, según el porcentaje de organizaciones que los han sufrido. Corrupción de la memoria, desbordamiento de buffer y denegación de servicio son los vectores de ataque más populares encontrados en nuestra investigación.

## Principales vectores de ataque




**Gráfica 2-K**

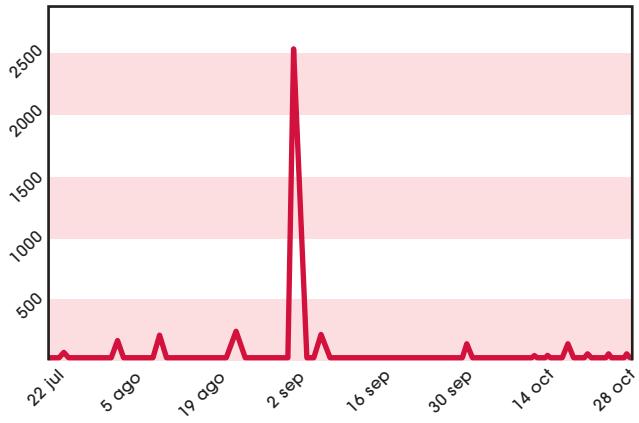
## ¿Qué aspecto tiene un ataque de inyección SQL? Incidencia de la Inyección SQL

Este caso muestra un ejemplo real de una serie de ataques de inyección SQL que tuvieron lugar entre julio y octubre de 2012 en el entorno de un cliente de Check Point. El ataque fue detectado y bloqueado por un Check Point Security Gateway. El caso fue informado por el equipo Check Point ThreatCloud Managed Security Service.

La inyección SQL es un exploit de seguridad (CVE-2005-0537) en el cuál el atacante añade código Structured Query Language (SQL) a una entrada de un formulario Web para obtener acceso a recursos o hacer cambios en los datos almacenados. La gráfica 2-M muestra el aspecto del ataque. El texto marcado es la información que el hacker intentó desvelar con la inyección SQL (en este caso nombres de usuario y contraseñas). Los comandos SQL son: select, concat y from. El ataque se produjo desde 99 IPs diferentes. Aunque la organización objetivo está localizada en Europa, los ataques se originaron desde muchas ubicaciones diferentes, como se presentan en la gráfica 2-M.

La inyección SQL puede realizarse manualmente (un hacker usando un teclado) o automáticamente (ataque mediante un script). En este caso, como se muestra en la gráfica 2-L, el pico del ataque fue una explosión de 4.184 intentos de ataque (la mayoría automatizados) que fueron lanzados durante dos días, usando el mismo patrón de inyección e iniciándose desde una única IP de origen.

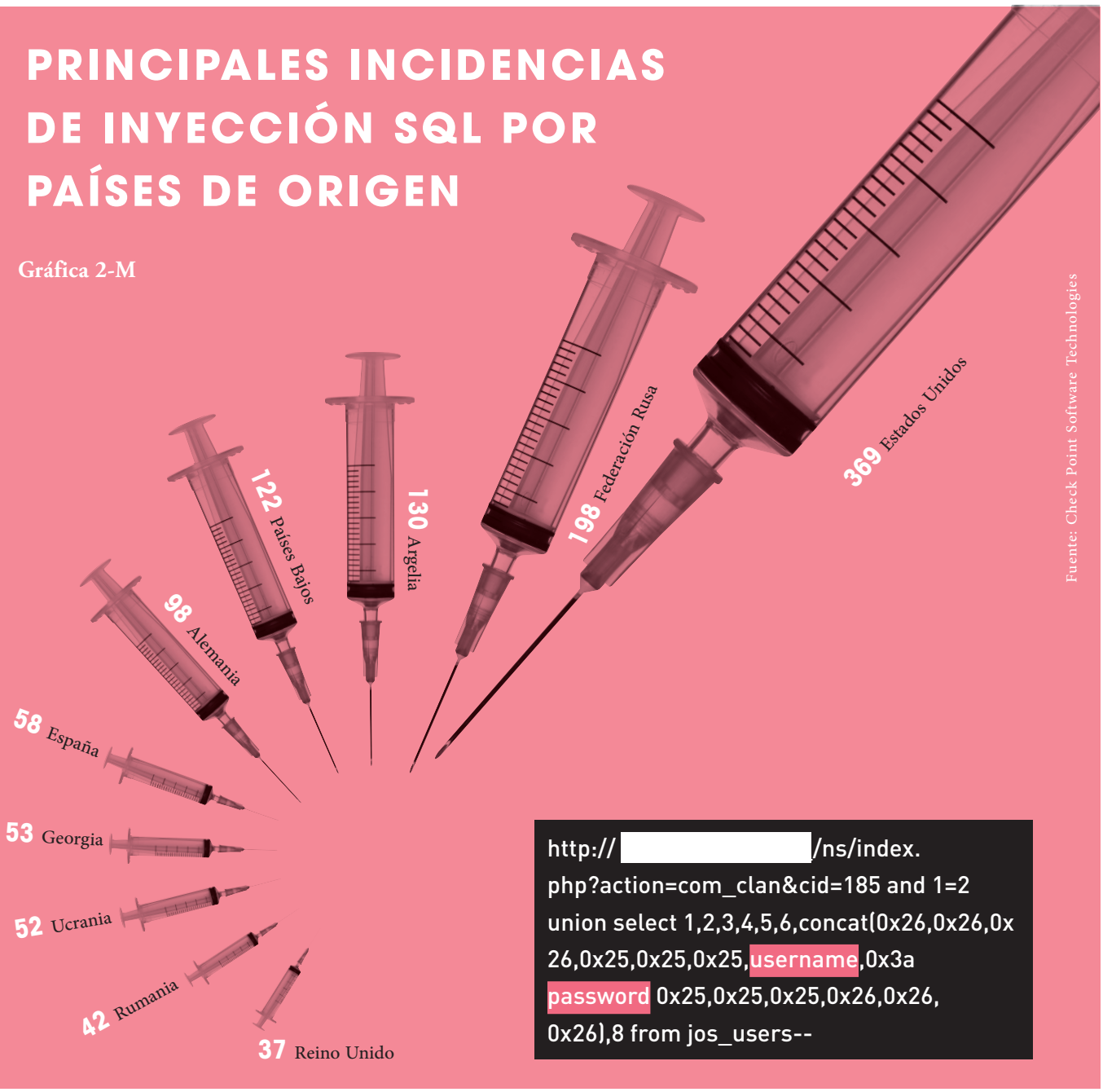
## Tasa de incidencias de inyección SQL




**Gráfica 2-L**

# PRINCIPALES INCIDENCIAS DE INYECCIÓN SQL POR PAÍSES DE ORIGEN

Gráfica 2-M




## RECOMENDACIONES DE SEGURIDAD MÚLTIPLES CAPAS DE SEGURIDAD

Dado que las amenazas cada vez son más y más sofisticadas, los desafíos de la seguridad continúan creciendo. Para maximizar la seguridad de las redes de las empresas, se necesita un mecanismo de protección multicapa para protegerse de los diferentes vectores de las amenazas y violaciones de la red:

- Antivirus para identificar y bloquear el malware
- Antibot para detectar y prevenir el daño por robots
- IPS para evitar intrusiones de forma proactiva
- Control Web - Filtrado URL y Control de aplicaciones para evitar accesos a sitios Web que contienen/distribuyen malware
- Inteligencia de seguridad en tiempo real y colaboración global
- Monitorización inteligente que proporciona análisis de datos proactivos

### Detener archivos maliciosos entrantes

Una organización necesita una solución Antimalware que analice los archivos entrantes en la red y pueda decidir, en tiempo real, si los archivos están infectados por malware. Esta solución debería evitar que archivos maliciosos infecten la red interna y también prevenir

## 2012, UN AÑO DE HACKTIVISMO

En 2012 las turbulencias del panorama político mundial que empezaron en 2010 con los levantamientos de muchos países árabes continúan con diversas protestas civiles en otros países. Como era de esperar, presenciamos una serie de ciberataques basados en motivaciones ideológicas. El proveedor de Apple establecido en Taiwan Foxconn fue atacado por un grupo autodenominado Swagg Security. Este grupo aparentemente protestaba informes en los medios sobre las pobres condiciones de trabajo en las fábricas de los fabricantes de electrónica en China[14].

El grupo hacktivista Anonymous declaró que había hackeado un servidor web del Departamento de Justicia de los EE.UU. para la Oficina de estadísticas de justicia de EE.UU. liberando 1,7 GB de datos robados. El grupo realizó la siguiente declaración sobre las información robada: "Liberamos esta información para terminar con la corrupción que existe, y liberar verdaderamente a aquellos que están siendo oprimidos"[15].

El Vaticano también descubrió que sus sitios Web y servidores de correo internos fueron objeto de un ataque durante una semana por el grupo Anonymous. El grupo declaró que su acción estaba justificada porque el Sistema de Radio Vaticana poseía potentes transmisores en las afueras de Roma que supuestamente constituían un riesgo para la salud. El grupo afirmó que los transmisores supuestamente podían causar "leucemia y cáncer" a la gente que vivía en las inmediaciones. El grupo también justificó su ataque y declaró que el Vaticano supuestamente ayudó a los Nazis, destruyó importantes libros históricos de gran valor, y que su clero había abusado sexualmente de menores[16].

En otro ciberataque, Anonymous derribó los sitios Web del grupo comercial U.S. Telecom Association y TechAmerica. Estos ataques fueron dirigidos por el apoyo de estas organizaciones al proyecto de ley de seguridad cibernética propuesto por el diputado Mike Rogers. Este proyecto permitiría a las empresas privadas y al gobierno compartir información "directamente relacionada con una vulnerabilidad o amenaza" en una red informática[17].

el acceso a sitios Web infectados con malware que intenten ejecutar descargas ocultas o no autorizadas.

### Protección multicapa frente a bots

La protección frente a bots comprende dos fases: detección y bloqueo.

Para maximizar la capacidad de detección de un bot en una red, se necesita un mecanismo multicapa de descubrimiento de bots para cubrir todos los aspectos del comportamiento de un bot. Una solución de seguridad para la detección de bots debería incluir un mecanismo de reputación que detecte la IP, URL y direcciones DNS que el operador remoto utiliza para conectarse a las redes de bots. También es muy importante que esta protección incluya la capacidad de detectar los patrones y protocolos de comunicación únicos para cada familia de redes de bots. Detectar las acciones de los bots es otra capacidad crítica de la protección frente a bots. La solución debería ser capaz de identificar las actividades de los bots, tales como el envío de spam, los clics fraudulentos y la autodistribución.

La segunda fase tras el descubrimiento de las máquinas infectadas es bloquear las comunicaciones salientes del bot a los servidores Command & Control. Esta fase neutraliza la amenaza y asegura que los agentes bot no pueden enviar información confidencial ni recibir ninguna instrucción para su actividad maliciosa. Con ello, el daño relacionado con el bot es inmediatamente mitigado. Este enfoque permite a las organizaciones mantener la continuidad del trabajo - los usuarios pueden trabajar normalmente, sin darse cuenta de que la comunicación específica del bot se ha bloqueado, y la organización está protegida sin haber causado un impacto en la productividad.

### Colaboración global en tiempo real

El problema de los ciberataques es demasiado importante para que lo gestione una organización por sí misma. Las organizaciones tienen una opción para vencer a este creciente desafío a través de la colaboración y la ayuda profesional. Dado que los ciberdelincuentes aprovechan

el malware, bots y otras formas avanzadas de amenazas, suelen apuntar a múltiples sitios y organizaciones para incrementar la probabilidad de éxito en el ataque. Cuando las empresas luchan contra estas amenazas de forma independiente, muchos ataques no son detectados y pasan inadvertidos, porque no hay modo para las corporaciones de compartir la información sobre las amenazas. Para estar por delante de las amenazas modernas, las empresas deben colaborar y compartir la información que poseen sobre amenazas. Sólo de forma conjunta pueden reforzar la seguridad y hacerla más efectiva.

## Prevención de intrusiones

La prevención de intrusiones es una capa de seguridad obligada en la lucha contra los diversos vectores de ciberataques. Se necesita una solución IPS para la inspección profunda del tráfico, de cara a prevenir intentos maliciosos de romper la seguridad y obtener acceso a los activos de las organizaciones. Una solución IPS adecuada proporcionará las siguientes capacidades:

- Detección de anomalías y validación de protocolos – Identificar y evitar el tráfico que no cumple con los estándares de protocolos y pueden crear malfuncionamientos en los dispositivos o problemas de seguridad.
- Evitar la transmisión de cargas útiles (payload) desconocidas que pueden aprovechar una vulnerabilidad específica.
- Prevenir una comunicación excesiva que pueda ser indicativo de un ataque Denial of Service (DoS).

## Ver el panorama de amenazas y tomar medidas

Tener una visión clara de las incidencias de seguridad y tendencias es otro componente clave en la lucha frente el cibercrimen. El administrador de seguridad debe tener una comprensión constante y clara del estado de seguridad de la red para estar alerta de las amenazas y ataques dirigidos contra la organización. Este entendimiento requiere una solución de seguridad que pueda proporcionar una perspectiva de alto nivel de las protecciones de seguridad y enfatizar la información crítica y los ataques potenciales. La solución debería ser también capaz de permitir dirigir investigaciones en profundidad sobre incidencias específicas. La capacidad de tomar medidas de forma inmediata basándose en esta información es otra premisa esencial que permite la prevención en tiempo real de ataques o el bloqueo de forma proactiva de futuras amenazas. La solución de seguridad debe disponer de una administración flexible y sencilla para simplificar el análisis de amenazas y reducir la sobrecarga operativa de los cambios.

## Actualizaciones de seguridad y soporte

En un entorno de amenazas constantemente cambiante, la defensa debe evolucionar con o por delante de las amenazas. Los productos de seguridad solamente pueden gestionar de forma efectiva el malware más reciente, vulnerabilidades y exploits, si el proveedor de seguridad es capaz de dirigir una investigación completa y proporcionar actualizaciones de seguridad frecuentes.
Un servicio de seguridad de calidad se basa en:

- Investigación y estudio interno del proveedor y obtención de información de múltiples fuentes.
- Actualizaciones de seguridad frecuentes para toda las tecnologías involucradas incluyendo IPS, antivirus y antibot
- Servicio de soporte sencillo y adecuado que pueda dar respuesta a las preguntas e incidencias específicas del entorno del cliente.

# 03 APLICACIONES EN EL ÁMBITO EMPRESARIAL

## Las reglas del juego han cambiado

Las reglas del juego han cambiado. Las aplicaciones de Internet fueron una vez consideradas una actividad para pasar el tiempo; un medio de ver imágenes de los últimos viajes de los amigos y de ver vídeos divertidos. Las aplicaciones Web 2.0 de Internet se han convertido en herramientas corporativas esenciales en las empresas modernas.

Nos comunicamos con nuestros compañeros, clientes y partners, compartimos información con otros, y accedemos a las últimas noticias, opiniones y puntos de vista. Las herramientas basadas en Internet como Facebook, Twitter, WebEx, LinkedIn, y YouTube por nombrar unas pocas, están ganando cada vez más presencia en las empresas que las consideran como elementos habilitadores del negocio.

En esta sección de nuestro informe, comentaremos los riesgos generales introducidos por las aplicaciones Web 2.0 y su infraestructura, y nos centraremos a continuación en aplicaciones específicas que hemos encontrado en uso en las organizaciones de nuestra investigación. Nuestros descubrimientos los ilustraremos con incidentes y ejemplos reales bien documentados.

## Las aplicaciones Web no son un juego

A medida que evoluciona la tecnología, así lo hacen los desafíos para la seguridad. Las herramientas de Internet introducen nuevos riesgos para la seguridad. Existe un número variado de útiles aplicaciones de Internet que se utilizan como herramientas de ataque contra organizaciones, o que pueden conducir a brechas en la seguridad de la red. Aplicaciones como anonimizadores, de almacenamiento e intercambio de archivos, intercambio de archivos Peer-to-Peer, herramientas de administración remota y redes sociales se utilizan para atacar a las organizaciones.

Existe una miríada de plataformas y aplicaciones que podrían utilizarse por razones personales o corporativas. Cada organización necesita estar al tanto de qué empleados las utilizan, y para qué propósitos, y entonces definir su propia política de Internet.

En el 91% de las organizaciones se encontró que los usuarios utilizaban aplicaciones que tenían el potencial de burlar los sistemas de seguridad, ocultar identidades, causar fugas de datos o incluso introducir infecciones de malware sin su conocimiento.

## DATOS CONFIDENCIALES COMPARTIDOS POR APLICACIONES DE INTERCAMBIO DE ARCHIVOS P2P EN EE.UU.

En junio de 2012, la US Federal Trade Commission (FTC) acusó a dos empresas por exponer información confidencial en redes de Intercambio de archivos Peer-to-Peer, poniendo miles de consumidores en riesgo. La FTC alegó que una de las organizaciones, EPN, Inc., una empresa de cobro de deudas establecida en Provo, Utah, expuso información confidencial, incluyendo los números de la Seguridad Social, números de seguros sanitarios y códigos de diagnósticos médicos de 3.800 pacientes de hospitales, al alcance de cualquier equipo conectado a una red P2P. La FTC alegó que la otra organización, un concesionario de automóviles de nombre Franklin's Budget Car Sales, Inc., expuso información de 95.000 consumidores en la red P2P. La información incluía nombres, direcciones, números de la seguridad social, fechas de nacimiento, y los números de las licencias de conducir de los conductores [18].

En 2010, la FTC notificó sobre 100 organizaciones que habían compartido información personal, incluyendo datos confidenciales sobre clientes y/o empleados, de sus redes y estaban disponibles en redes de intercambio de archivos peer-to-peer (P2P). Cualquier usuario de esas redes podría utilizar los datos para perpetrar robos de identidad o fraudes[19].

# EN EL 61 %

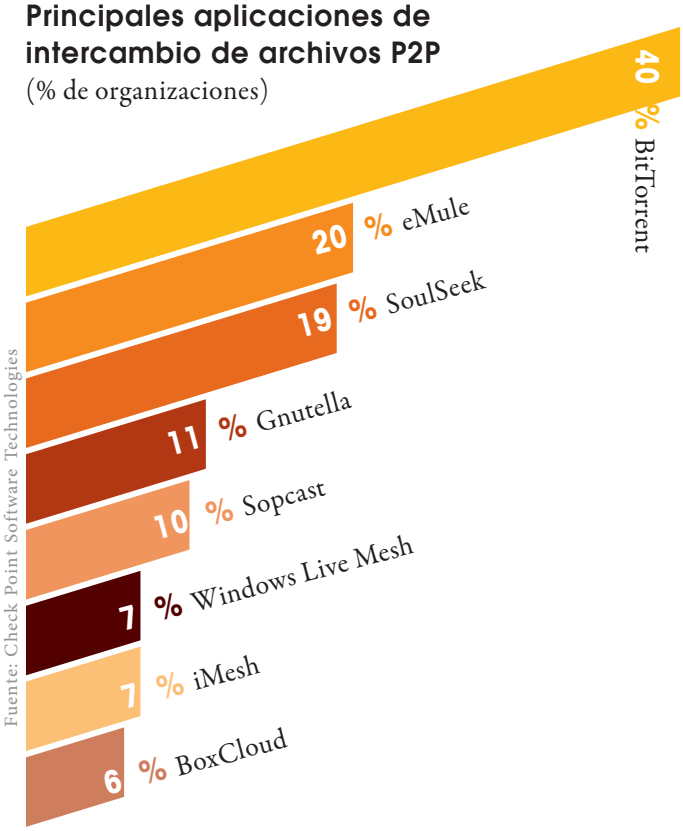
# DE LAS ORGANIZACIONES, SE UTILIZABA UNA APLICACIÓN DE INTERCAMBIO DE ARCHIVOS P2P

## Las aplicaciones P2P abren una puerta trasera para acceder a su red

Las aplicaciones Peer-to-Peer (P2P) se utilizan para compartir archivos entre los usuarios. P2P cada vez es más utilizado por los atacantes para distribuir malware entre los archivos compartidos. Las aplicaciones P2P en esencia abren una puerta trasera para acceder a las redes. Estas permiten a los usuarios el compartir carpetas que podrían dejar escapar información confidencial, pero además podrían hacer a las organizaciones responsables de la adquisición ilegal de recursos o medios a través de las redes P2P. Presenciamos una tasa de utilización de aplicaciones P2P muy elevada, más de la mitad de las organizaciones (61%) estaban utilizando aplicaciones P2P. Las herramientas de intercambio de archivos P2P más utilizada son los clientes BitTorrent. Desde el punto de vista regional, la siguiente gráfica muestra que en Asia Pacífico, las aplicaciones de intercambio de archivos P2P son más populares que en otras regiones.

### Principales aplicaciones de intercambio de archivos P2P

(% de organizaciones)

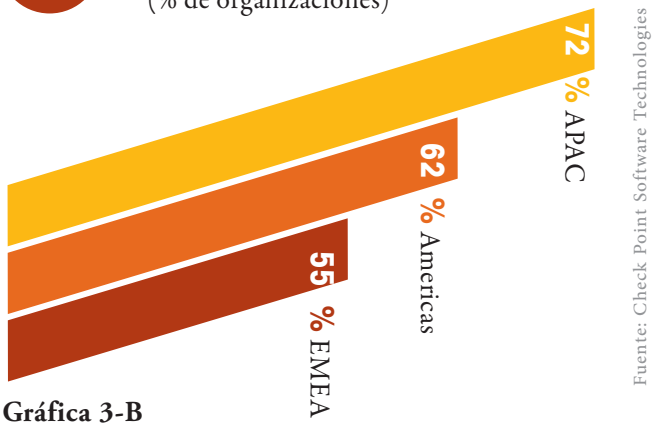



**Gráfica 3-A**

**Dispone de más información sobre las principales aplicaciones P2P en el Apéndice B.**

### Uso de aplicaciones de intercambio de archivos P2P por región

(% de organizaciones)




**Gráfica 3-B**

## Las aplicaciones anonimizadores eluden las políticas de seguridad de las organizaciones

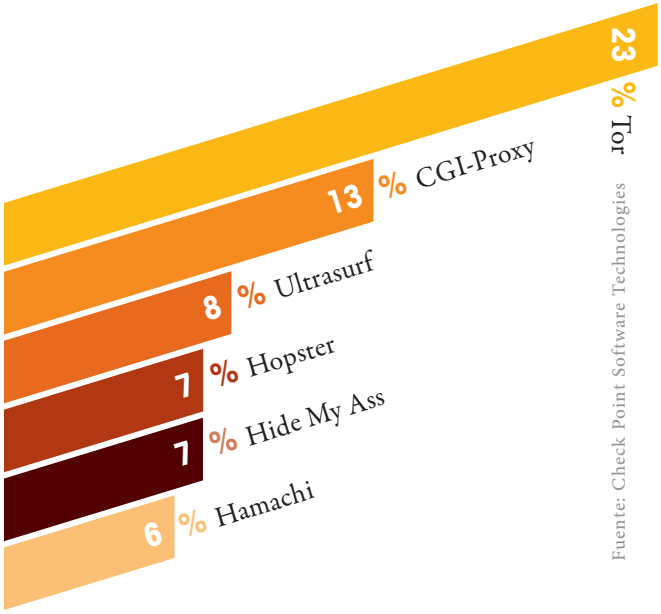
Un anonimizador (o proxy anónimo) es una herramienta que intenta hacer no rastreable la actividad del usuario en Internet. La aplicación anonimizador utiliza un servidor proxy que actúa como una máscara para la privacidad entre un equipo cliente y el resto de Internet. Acceder a Internet en nombre del usuario, escondiendo información personal mediante la ocultación de la información de identificación del equipo cliente y el destino que el usuario está intentando alcanzar. Las aplicaciones

anonimizadoras pueden utilizarse para saltarse las políticas de seguridad que están fundamentalmente creadas alrededor de las identidades de los usuarios y las URL/sitios de destino. Al usar anonimizadores, los usuarios parecen estar en una dirección IP diferente e intentando acceder a destinos distintos, con lo cual la política de seguridad no puede aplicarse para ese usuario con una dirección IP modificada y una dirección de destino alterada. En algunos casos los anonimizadores podrían utilizarse también para ocultar una actividad criminal.

Cuando miramos a las organizaciones en nuestro estudio, el 43% tenía al menos un empleado que utilizaba una aplicación anonimizadora, siendo Tor la más destacada. El 86% de las organizaciones donde fue descubierta la utilización de anonimizadores alegaron que se estaban utilizando de forma no legítima entrando en conflicto con las políticas de seguridad. Cuando nos fijamos en la utilización de aplicaciones anonimizadoras por región, podemos ver que son más populares en América y menos en Asia Pacífico.

## Aplicaciones anonimizadoras más populares

(% de organizaciones)

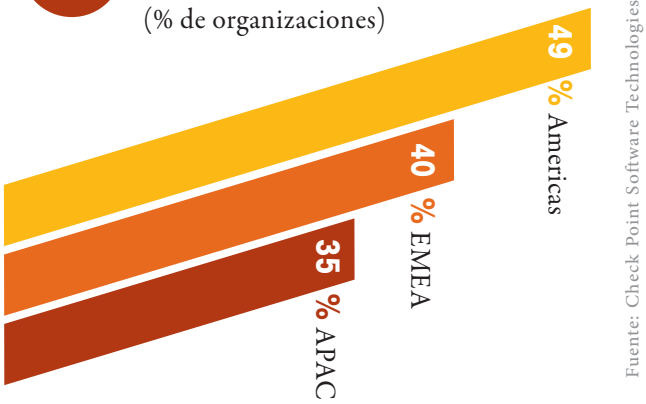



**Gráfica 3-C**

Dispone de más información sobre las principales aplicaciones anonimizadoras en el Apéndice B.

## Uso de aplicaciones anonimizadoras por región

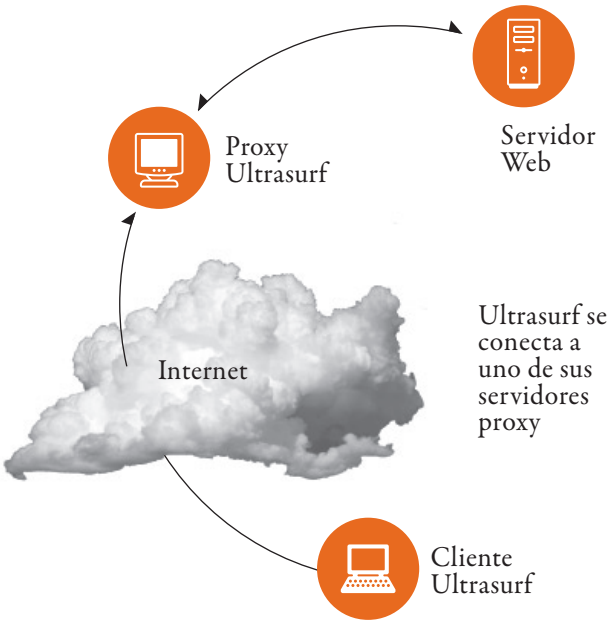
(% de organizaciones)




**Gráfica 3-D**

## ¿Cómo funciona el anonimizador Ultrasurf?

Ultrasurf es un anonimizador muy sofisticado que funciona como un cliente proxy, creando un túnel HTTP cifrado entre el equipo del usuario y un pool central de servidores proxy, permitiendo a los usuarios superar los cortafuegos y la censura. Ultrasurf posee un diseño muy elástico para descubrir servidores proxy que incluye un archivo de caché de IPs de servidores proxy, peticiones DNS que devuelven IPs codificadas de los servidores proxy, documentos cifrados en Google Docs y una lista codificada de forma fija de IPs de servidores proxy incorporada en el programa. Estas técnicas hacen que sea más difícil de ser detectados por los dispositivos de seguridad.



# EN EL 43% DE LAS ORGANIZACIONES SE UTILIZAN ANONIMIZADORES

## EL ANONIMIZADOR TOR COMPROMETE LA SEGURIDAD

Recientes investigaciones de seguridad identificaron una botnet que está controlada por atacantes de un servidor Internet Relay Chat (IRC) que ejecutan un servicio oculto dentro de la red anónima Tor. Las conexiones entre los usuarios y los nodos de Tor están cifrados de una forma multicapa, haciendo muy difícil para los sistemas de vigilancia que operan a nivel de la red local o a nivel ISP, determinar el destino previsto de un usuario[20]. El objetivo principal de la red Tor (también conocida como Onion Router) es básicamente proporcionar anonimato mientras se navega por Internet. A pesar de estar ampliamente difundida y disfrutar de una gran popularidad, cuando se utiliza en un entorno organizativo, plantea varios desafíos para la seguridad. Tor puede ser utilizado fácilmente para eludir las políticas de seguridad, dado que fue diseñado específicamente para proporcionar anonimato a sus usuarios. Cuando se utiliza para acceder a recursos de Internet, las peticiones enviadas desde el equipo de un usuario son redirigidas de forma aleatoria a través de una serie de nodos gestionados de forma voluntaria por otros usuarios de Tor.

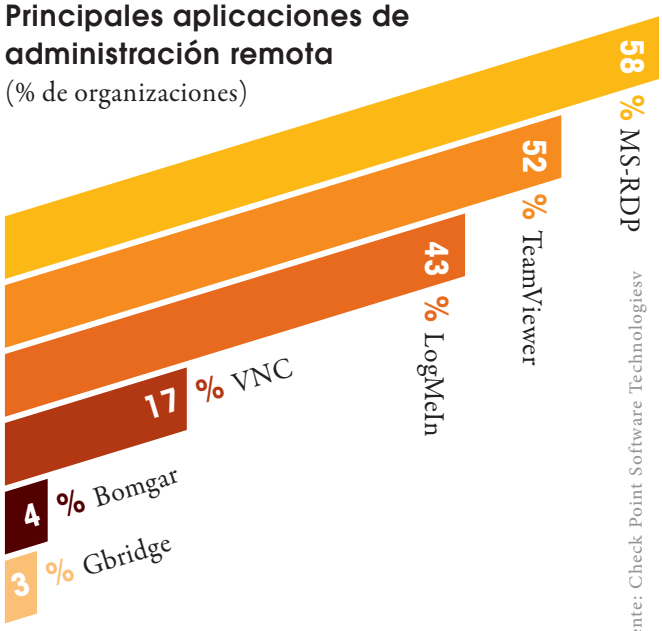
## EL 81% DE LAS ORGANIZACIONES UTILIZAN **HERRAMIENTAS DE ADMINISTRACIÓN REMOTA**

### Herramientas de administración remota utilizadas para realizar ataques maliciosos

Las Remote Administration Tools (RAT) o herramientas de administración remota, pueden ser herramientas legítimas cuando son operadas por administradores o por el personal de helpdesk. Sin embargo, diversos ataques durante los pasados años aprovecharon una RAT disponible para controlar remotamente equipos infectados, además de infiltrarse en redes, registrar pulsaciones de teclado, o robar información confidencial. Dado que las herramientas de administración remota son normalmente aplicaciones fundamentales para las empresas, no deberían bloquearse en todos los ámbitos; sin embargo su utilización debería estar supervisada y controlada para evitar malos usos potenciales.

Cuando nos fijamos en las organizaciones de nuestro estudio, el 81% utilizaba al menos una aplicación de administración remota, siendo Microsoft RDP la más popular.

**Principales aplicaciones de administración remota**
(% de organizaciones)




Fuente: Check Point Software Technologiesv

**Gráfica 3-F**

**Dispone de más información sobre las principales aplicaciones de administración remota en el Apéndice B.**

# HACKEADO POR HERRAMIENTAS DE ACCESO REMOTO

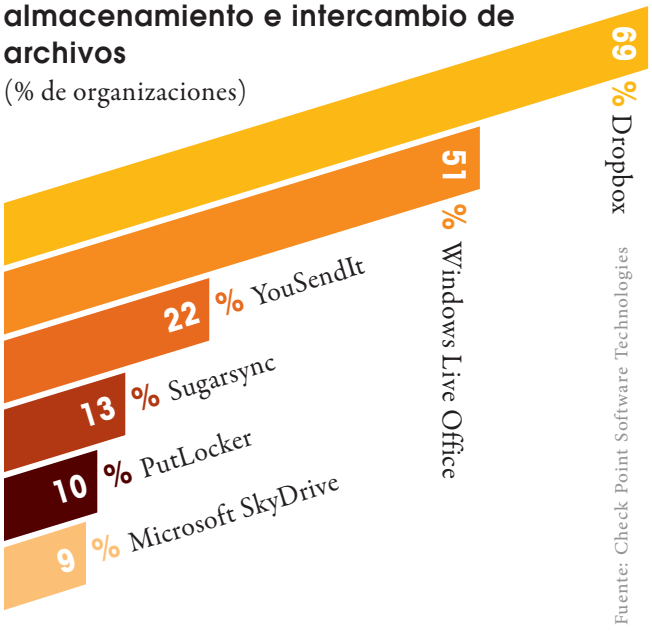
De julio a septiembre de 2011 tuvo lugar una campaña de ataques etiquetada como "Nitro". Los atacantes utilizaron la herramienta de acceso remoto de nombre Poison Ivy para husmear información secreta de cerca de 50 empresas, muchas de ellas de la industria química y de defensa. Poison Ivy fue implantada en PCs Windows cuyos propietarios fueron víctimas de un engaño perpetrado a través del correo electrónico. Los emails simulaban peticiones de reuniones de socios de negocio conocidos, o en algunos casos, actualizaciones del software antivirus o Adobe Flash Player. Cuando los usuarios abrían el adjunto del mensaje instalaban de forma inadvertida Poison Ivy en sus equipos. Desde ahí, los atacantes eran capaces de dar instrucciones a los equipos comprometidos, secuestrar contraseñas de alto nivel para ganar acceso a servidores que albergaban la información confidencial, y finalmente descargar el contenido robado a sistemas controlados por hackers. 29 de las 48 empresas que fueron atacadas con éxito pertenecían a la industria química y comercialización de materiales avanzados - algunas de estas con conexiones a vehículos militares – mientras que las otras 19 pertenecían a diversos campos, incluyendo el sector de la defensa[21]. Nitro no es el único ejemplo del mal uso de RAT, otros ejemplos son el RSA breach, ShadyRAT y Operation Aurora. En todos estos casos se utilizó Poison Ivy.

## Compartir no siempre es caritativo

El término "Compartir es caritativo" normalmente significa que si alguien comparte con otros, es caritativo con ellos. Cuando se comparten archivos usando aplicaciones de intercambio de archivos en entornos de trabajo, este no es siempre el caso. Una de las características más prominentes de la Web 2.0 es la capacidad de generar contenido y compartirlo, pero esto también representa un riesgo.

### Principales aplicaciones de almacenamiento e intercambio de archivos

(% de organizaciones)




**Gráfica 3-G**

**Dispone de más información sobre las principales aplicaciones de almacenamiento e intercambio de archivos en el Apéndice B.**

## El 80% DE LAS ORGANIZACIONES UTILIZAN **APLICACIONES DE ALMACENAMIENTO E INTERCAMBIO DE ARCHIVOS**

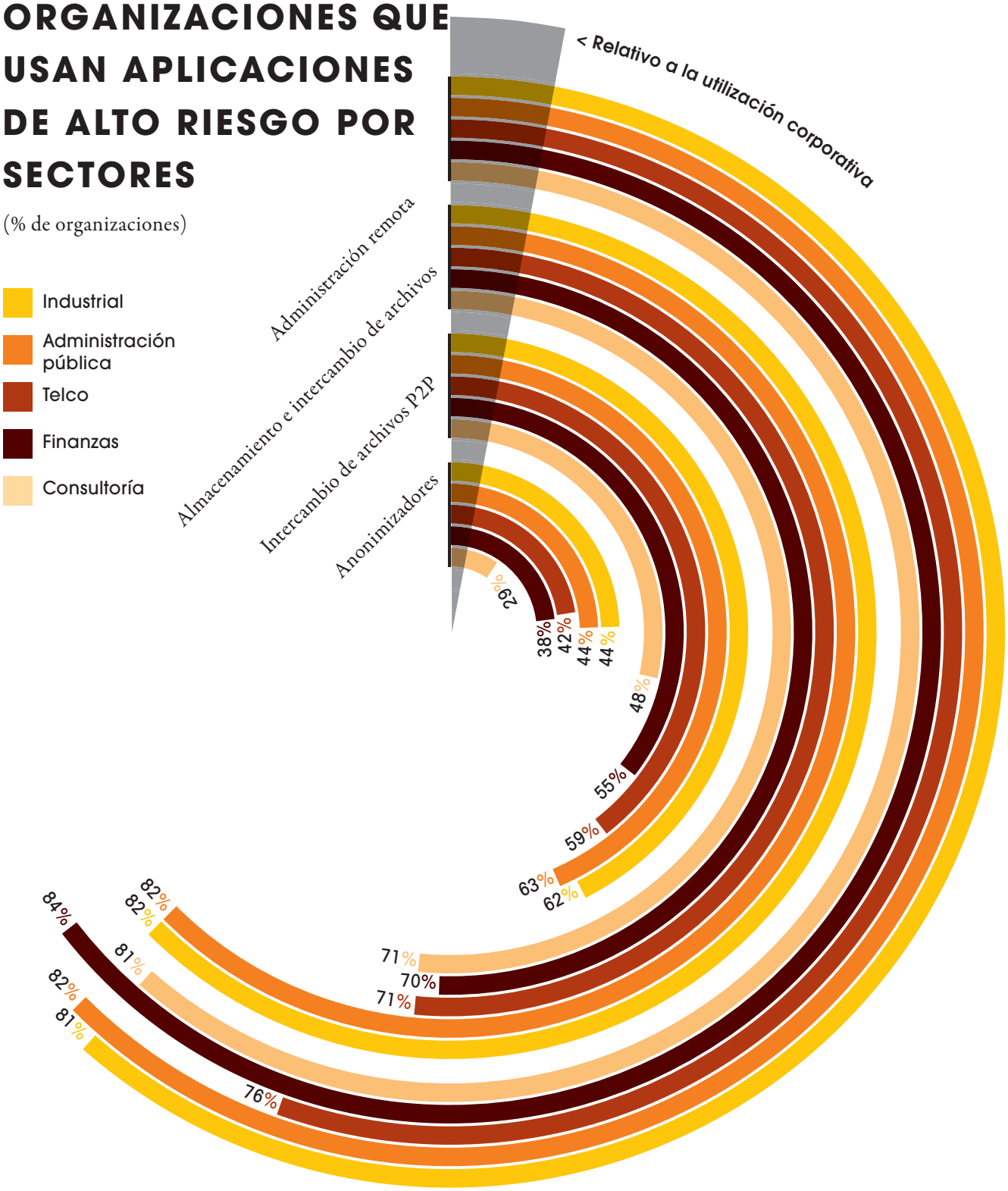
La información sensible puede caer en las manos equivocadas al compartir archivos confidenciales. Nuestra investigación incluye aplicaciones de intercambio y almacenamiento de archivos de alto riesgo que pueden causar la fuga de datos o infecciones malware sin el conocimiento del usuario. Nuestra investigación muestra que el 80% de las organizaciones tienen al menos una aplicación de almacenamiento de archivos o de intercambio ejecutándose en su red. Encontramos que el 69% de las incidencias fueron resultado del uso de Dropbox. Windows Live Office está en segundo lugar con un 51%.

## Aplicaciones de alto riesgo utilizadas por sectores

Check Point analizó la utilización de aplicaciones de alto riesgo desde el punto de vista de la industria. La gráfica Chart 3-indica que las organizaciones del sector industrial y gubernamental son los usuarios que más uso hacen de las aplicaciones de alto riesgo. Existen casos donde el uso de algunas de estas aplicaciones podría constituir un uso legítimo en una organización, por ejemplo el uso de herramientas de administración remota por los departamentos de helpdesk, por ello la barra horizontal de la gráfica indica el nivel de probabilidad de usos legítimos en un entorno empresarial.

# PORCENTAJE DE ORGANIZACIONES QUE USAN APLICACIONES DE ALTO RIESGO POR SECTORES

(% de organizaciones)




Fuente: Check Point Software Technologies

**Gráfica 3-E**

# DOS INCIDENTES DE SEGURIDAD PRINCIPALES CON DROPBOX EN DOS AÑOS

En julio de 2012 se produjo un ataque a usuarios de Dropbox. Los nombres de usuarios de Dropbox y sus contraseñas puestos en riesgo por la violación de otro sitio Web fueron probados en cuentas de Dropbox. Los hackers usaron una contraseña robada para iniciar sesión en la cuenta de Dropbox de un empleado que contenían documentos con las direcciones de correo de los usuarios. Los spammers usaron esas direcciones de correo para enviar spam[22].

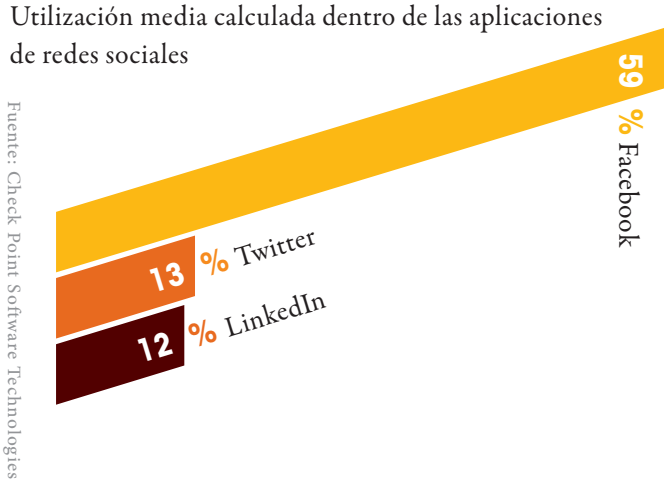
El incidente ilustra una táctica frecuente utilizada por los hackers. Los hackers normalmente roban nombres de usuarios y contraseñas de sitios que, a primera vista, pueden no tener ningún valor económico o contener información personal. Entonces, prueban dichas credenciales en los sitios Web oficiales de organizaciones financieras, cuentas de agencias de bolsa y, aparentemente, cuentas de Dropbox, donde puede encontrarse información potencialmente más lucrativa. En 2011, un error en el software de actualización de Dropbox hizo posible que cualquiera pudiera iniciar sesión en una cuenta de Dropbox con tal de que la persona tuviera la dirección de correo del usuario. Este error puso en riesgo los documentos e información compartidos por los usuarios. El problema se reparó en unas cuantas pero sirvió como advertencia para usuarios y corporaciones cuyos empleados usan los servicios de almacenamiento e intercambio de archivos, como Dropbox y Google Docs, para almacenar información corporativa confidencial[23].

## ¿Publicación legítima de Facebook o Virus?

Con el aumento de la popularidad de las redes sociales, en constante crecimiento, se presentan nuevos desafíos para las organizaciones. Publicar de forma inconsciente información confidencial de un proyecto en aplicaciones de redes sociales podría dañar la reputación de una organización, perder ventaja competitiva o producir una pérdida económica importante. Los hackers están aprovechando las nuevas técnicas de ingeniería social para impulsar sus actividades en las redes de bots. Los vídeos incrustados y enlaces en páginas de redes sociales se están convirtiendo en puntos de acceso muy populares para los hackers como medios de incrustar malware. Además de los riesgos para la seguridad, las aplicaciones de redes sociales generan un importante problema de consumo del ancho de banda de la red. Facebook es sin duda alguna la red social más visitada. Otras redes sociales visitadas durante un día laboral (pero significativamente menos que Facebook) son Twitter y LinkedIn. Un enlace de Facebook que dirige a un sitio malicioso:


## Utilización del ancho de banda de las principales redes sociales

Utilización media calculada dentro de las aplicaciones de redes sociales

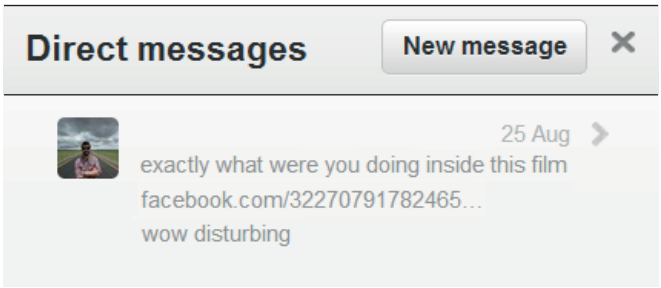



**Gráfica 3-H**

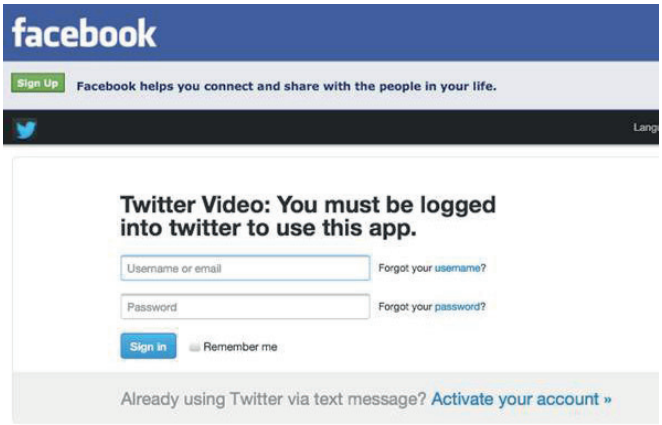
## Ataques de ingeniería social - Caso de estudio

Los últimos ataques indican que los hackers están cambiando el uso del correo electrónico normal a las redes sociales como canal de distribución. El siguiente caso se basa en un ataque real que tuvo lugar en agosto de 2012. Los hackers usaron técnicas de ingeniería social en Twitter y Facebook para distribuir contenido malicioso. Usando una cuenta puesta en compromiso, el hacker envió

mensajes directos a todos los seguidores del propietario de la cuenta hackeada. El mensaje rezaba: "exactly what were you doing inside this film [Facebook-URL]... wow disturbing".




La URL apuntaba a una app de Facebook que requería iniciar sesión "como Twitter". La pantalla de inicio de sesión en realidad era un servidor Web propiedad del hacker que era utilizado para recopilar las credenciales de Twitter de los destinatarios.




Usando las credenciales de twitter, el hacker ahora podía repetir el mismo proceso usando las nuevas cuentas hackeadas para conseguir de forma más fácil muchas más contraseñas. El hacker puede usar estas credenciales robadas con otros servicios como GMail, Facebook, etc. pero lo peor de todo es que puede usarse para iniciar sesión en cuentas bancarias o incluso en servicios relacionados con empresas como SalesForce y otros.
Tras distribuir el mensaje malicioso (pero esta vez a todos los seguidores del pobre usuario al que se hackeó la cuenta), la única cosa efectiva que podía hacerse en esta situación era publicar un educado post de disculpa.


## RECOMENDACIONES PARA ASEGURAR EL USO DE APLICACIONES WEB EN SU RED

### ¿Cómo puede activar una protección efectiva Web 2.0?

El primer paso para asegurar la utilización de las aplicaciones Web 2.0 en una organización es usar una solución de seguridad que proporcione control y haga cumplir todas las políticas de seguridad para todos los aspectos de la utilización Web. Es necesario tener visibilidad completa de todas las aplicaciones que se ejecutan en el entorno, junto con la capacidad de controlar su utilización. Este nivel de control tiene que mantenerse sobre las aplicaciones clientes (como Skype) y también sobre los aspectos más tradicionales basados en URL de la web – los sitios Web. Dado que muchos sitios (como Facebook) activan la ejecución de numerosas aplicaciones basadas en su URL, es fundamental tener granularidad más allá del nivel de URL – por ejemplo el chat de Facebook o las aplicaciones de juegos. Una vez conseguido esto por parte de las organizaciones, debería ser capaz de bloquear fácilmente las aplicaciones que puedan poner en peligro su seguridad corporativa.

### Habilitar las redes sociales para el negocio

Hay casos en donde las organizaciones deciden bloquear Facebook por completo, pero Facebook es una herramienta comercial fundamental para muchas empresas. Las empresas ofrecen publicar información sobre próximos seminarios, eventos, información sobre los últimos lanzamientos y productos, enlaces a artículos y vídeos de interés.
¿Cómo podemos activar el uso de las redes sociales en la organización sin comprometer la seguridad? Controlando las funciones y widgets dentro de las apps y plataformas. Al ser capaz de permitir Facebook mientras se bloquean las partes de él menos relevantes para el negocio, es posible permitir el uso viable de las redes sociales a la vez que se minimizan los riesgos de seguridad.

### Distintos usuarios tienen diferentes necesidades

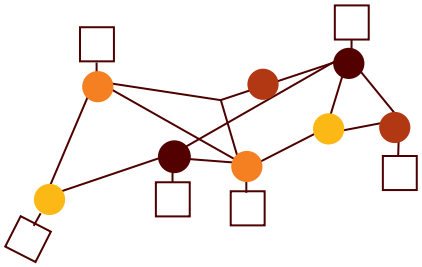
Distintos usuarios en la organización tienen diferentes necesidades, y la política de seguridad debería apoyar el negocio, no interferir con él. Por ejemplo, una persona de ventas puede usar Facebook para estar en contacto con los clientes y partners, donde un miembro del personal de TI puede usar Facebook para acceder a las últimas noticias de la industria. ¿Cómo podemos asegurar entonces que los usuarios obtienen el acceso que necesitan? ¿Es práctico esperar que el director de seguridad conozca a qué debería o no acceder cada usuario o grupo?

Una solución práctica necesita disponer de un reconocimiento de equipo, grupo, usuario granular para poder distinguir fácilmente entre unos empleados y otros (por ejemplo, invitados y contratistas).

Otro aspecto importante es la capacidad de educar y comprometer a los usuarios finales en tiempo real cuando utilizan las aplicaciones. Cuando un usuario termina en un sitio web o inicia una aplicación en entredicho, un mensaje emergente puede preguntarle al usuario que justifique el motivo empresarial para hacerlo, su respuesta puede quedar registrada y monitorizarse, mientras el mensaje también puede educar al usuario en la política de seguridad de la empresa, y hacerle consciente de que el uso de esa aplicación está siendo auditado.

### 'La comprensión' es un componente crítico del Control Web

Los administradores deben disponer de una visión general de las incidencias de seguridad Web para garantizar el control web. Una solución de seguridad puede proporcionar visibilidad clara y amplia en todos los asuntos de seguridad Web que se necesite. La solución debería proporcionar funciones de visibilidad y monitorización así como una línea temporal de eventos y una lista extensa de estos eventos que puedan filtrarse, agruparse y ordenarse por usuario, aplicación, categoría, nivel de riesgo, utilización del ancho de banda, hora y mucho más. También es importante ser capaz de generar informes online para mostrar las categorías principales, apps, sitios y usuarios para permitir planificar tendencias y capacidad.



**ASEGURAR LA WEB 2.0** REQUIERE UN ENFOQUE INTEGRADO DE FILTRADO URL, CONTROL DE APLICACIONES, CONCIENCIACIÓN DE LOS USUARIOS, EDUCACIÓN DE LOS USUARIOS Y UNA FORMA DE QUE EL ADMINISTRADOR DISPONGA DE TODA LA VISIBILIDAD SOBRE EL CONTROL WEB.

### Resumen

Las reglas del juego han cambiado. Asegurar la Web 2.0 ya no es un simple juego de bloquear una URL no adecuada. Ya no es una cuestión de evitar que se ejecute una aplicación. Asegurar la Web 2.0 requiere un enfoque integrado de protección multicapa: filtrado URL, control de aplicaciones, protección frente a malware y bots - todo ello incorporando la concienciación del usuario, la formación de este, monitorización sofisticada y herramientas de análisis de eventos para mantener a los administradores al control en todo momento.

# 04 INCIDENTES DE PÉRDIDA DE DATOS EN LA RED

## Datos corporativos: El activo más valioso de las organizaciones

Nunca antes los datos corporativos han resultado ser más accesibles y transferibles que actualmente, y la inmensa mayoría de los datos corporativos son sensibles en diferentes niveles. Algunos son simplemente confidenciales porque incluyen datos internos corporativos, lo que significa que no deben ser accesibles al público. Otros tipos de datos pueden resultar sensibles por requisitos corporativos, leyes nacionales y regulaciones internacionales. Sin embargo, en muchas ocasiones el valor de los datos es independiente de su confidencialidad – basta considerar la propiedad intelectual y la información que afecta a la competencia. Para hacer este asunto aún más complejo, además de la gravedad de la pérdida de datos, disponemos actualmente de herramientas y prácticas que hacen que resulte mucho más fácil que se produzca un error irreversible: servidores en nube, Google docs, así como el simple abuso no intencionado de los procedimientos de la compañía – como los empleados que se llevan el trabajo a casa. De hecho, la mayoría de los casos de pérdida de datos se producen por causas no intencionadas.

## Una pérdida de datos puede sucedernos a cualquiera de nosotros

La pérdida de datos puede producirse no sólo por la acción de los cibercriminales, sino también de forma no intencionada por alguno de los empleados. Puede enviarse un documento clasificado por error a la persona equivocada, podría compartirse en un sitio público un documento sensible o enviarse un archivo de trabajo a una cuenta de correo doméstica no autorizada. Alguno de estos escenarios se nos puede presentar a cualquiera de nosotros inadvertidamente, con efectos devastadores. La pérdida de datos sensibles puede ocasionar daños a la compañía, violaciones de normativas, menoscabo de beneficios e incluso sustanciosas multas.

## Nuestro estudio

Cuando una empresa necesita definir los datos que no deberían salir de la organización, deben tenerse en cuenta muchas variables. ¿De qué tipo de datos se trata? ¿Quién es su dueño? ¿Quién los envía? ¿Quién es el receptor previsto? ¿Cuándo se envían? ¿Cuál es el coste de que se interrumpan

**EL 54%**

**DE LAS ORGANIZACIONES DE NUESTRO ESTUDIO TUVO, AL MENOS, UN INCIDENTE POTENCIAL DE PÉRDIDA DE DATOS**

# ¡VAYA! ENVIÉ EL CORREO A UNA DIRECCIÓN EQUIVOCADA

Aquí tenemos algunos ejemplos de incidentes de pérdida de datos originados de forma no intencionada por empleados durante 2012:

En octubre de 2012, **el Ayuntamiento de Stoke-on-Trent City** del Reino Unido fue multado con 120.000 £ porque un miembro de su departamento legal envió correos con información sensible a la dirección equivocada. Once correos destinados a un abogado que trabajaba en un caso terminaron siendo enviados a otra dirección por un error al teclear.

El periódico japonés **Yomiuri Shimbun** despidió a uno de sus periodistas en octubre de 2012, por enviar accidentalmente información sensible sobre una investigación a personas equivocadas. El periodista pretendió enviar parte de sus hallazgos a colegas por correo, pero en su lugar dirigió los mensajes a varios medios de comunicación, desvelando la fuente de sus informaciones [24].

En abril de 2012, el **Virginia Military Institute** de Lexington, envió inadvertidamente calificaciones de graduación de sus estudiantes como adjuntos de correo. Se envió un correo al responsable de la clase que se graduaba conteniendo como adjunto una hoja de cálculo con las puntuaciones medias de cada integrante. Pasando por alto el contenido del adjunto adicional, el responsable reenvió el mensaje a 258 estudiantes. La intención original era enviar sólo una hoja de cálculo conteniendo los nombres y direcciones para que los alumnos pudiesen comprobar sus direcciones de correo [25].

**La Texas A&M University** envió accidentalmente un correo con un adjunto que contenía 4.000 números de la Seguridad Social de estudiantes, nombres y direcciones, a un destinatario que, seguidamente, notificó a la universidad del error. El incidente tuvo lugar en abril de 2012 [26].

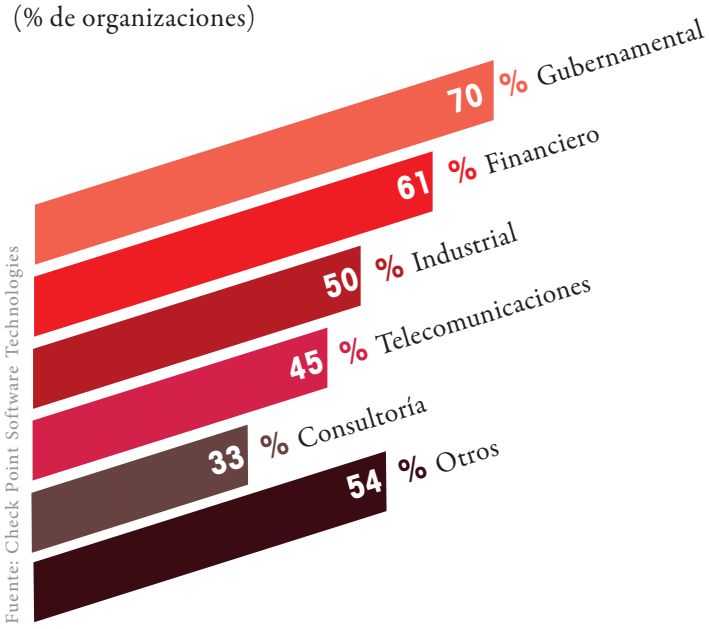
los procesos de negocio a causa de una política de seguridad más estricta de lo necesario? En nuestro estudio analizamos el tráfico enviado de dentro a fuera de las organizaciones. Analizamos tanto el trafico HTTP como el SMTP. Por ejemplo, en el caso de los correos enviados a destinatarios externos, un dispositivo Check Point se ocupó de analizar los cuerpos de los mensajes, los destinatarios de los correos y adjuntos de los mismos (incluso en ZIP). Analizamos también las actividades de navegación Web, como publicaciones y correo Web. Como política de seguridad de estos equipos, configuramos tipos de datos predefinidos para detectar datos sensibles, en formularios y plantillas (como números de tarjetas de crédito, código fuente, datos financieros y otros) que pudieran dar origen a una pérdida de datos potencial de caer en las manos equivocadas. En el Apéndice D ofrecemos una lista detallada de los tipos de datos.

## Pérdida potencial de datos en su organización

En nuestra investigación, encontramos que el 54% de las organizaciones habían tenido, al menos, un evento que podría indicar una pérdida potencial de datos durante un tiempo

**Porcentaje de organizaciones con, al menos, un evento potencial de pérdida de datos por sector**

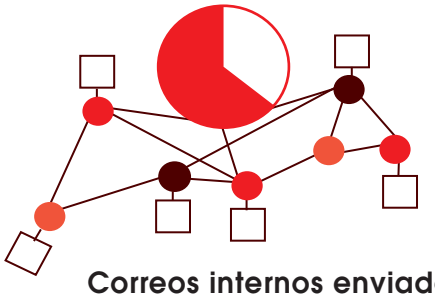
(% de organizaciones)




**Gráfica 4-A**

medio de seis días. Tuvimos en cuenta eventos que incluían información interna (ver la lista de tipos de datos en el apéndice D) que resultaba enviada a fuentes externas, bien sea por envío a un destinatario de correo externo o por publicación en línea. Nuestro informe indica que las organizaciones gubernamentales y financieras se encuentran en un alto riesgo de pérdida potencial de datos (ver Gráfico 4-A).

**EN EL 28% DE LAS ORGANIZACIONES** SE ENVIÓ UN CORREO INTERNO A UN DESTINATARIO EXTERNO



## Correos internos enviados fuera de la organización

En muchos casos, los eventos de pérdida de datos se producen de forma no intencionada al enviar un empleado un correo a un destinatario equivocado. En nuestro estudio contemplamos dos tipos de correos, que indicarían casos similares. El primer tipo está compuesto por correos enviados con destinatarios internos visibles (Para y CC) y destinatarios externos en el campo CCO. Este tipo de correos, en la mayoría de los casos, parecen ser internos pero en realidad abandonan la compañía. El segundo equipo se compone de correos enviados a varios destinatarios internos y a un único destinatario externo. Este tipo de correo se envía generalmente de forma no intencionada a un destinatario externo erróneo. Encontramos uno o ambos de estos tipos de eventos en el 28% de las organizaciones examinadas.

## ¿Qué tipos de datos pueden publicar en línea o enviar a destinatarios externos los empleados?

La gráfica 4-C muestra los tipos de datos más comunes enviados fuera de la organización. La información de tarjetas de crédito lidera la lista, mientras que le siguen el código fuente y los archivos protegidos con contraseña.

## ¿Se ajusta a PCI tu organización?

Los empleados se envían números de tarjetas de crédito a través de internet, los suyos propios y los de los clientes. Envían recibos de pago de los clientes que contienen un número de tarjeta de crédito como adjunto de correo. Responden a correos de clientes que contienen originalmente el número de tarjeta de crédito en el cuerpo del correo. En ocasiones, los empleados se envían, incluso, hojas de cálculo y contratos de los clientes a cuentas de correo privadas o a colaboradores del negocio. A menudo, los incidentes relativos a números de tarjetas de crédito son el resultado de romper los procedimientos de negocio o de la falta de la atención debida de los empleados. Incidentes como estos pueden indicar que la política de seguridad corporativa no se ajusta al objetivo de promover la seguridad y uso cuidadoso de los recursos empresariales. Más aún, enviar números de tarjetas de crédito por internet no se ajusta a los requisitos PCI DSS 4, que obligan a que los datos de las tarjetas de crédito se encripten para su transmisión a través de redes abiertas. La falta de cumplimiento de la norma PCI DSS puede perjudicar la reputación, originar pleitos, reclamaciones de seguro, cancelación de cuentas, problemas con los pagos por tarjeta y multas gubernamentales. En nuestro estudio se inspeccionó el tráfico saliente de organizaciones, analizando el contenido de todos los componentes de los mensajes, incluyendo adjuntos y archivos, para localizar correos que contuviesen números de tarjetas de crédito o datos de su propietario. Estas inspecciones se basaron en expresiones comunes, validación de dígitos de control y cumplimiento de la normativa PCI DSS.

**Porcentaje de organizaciones por sectores en las cuales se envió información de tarjetas de crédito a fuentes externas**

(% de organizaciones)

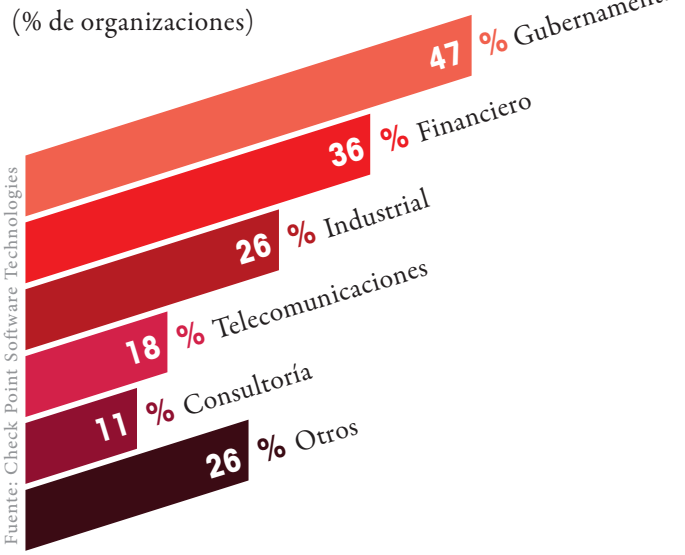



**Gráfico 4-B**

# EN EL 36% DE LAS ORGANIZACIONES FINANCIERAS SE ENVIABA INFORMACIÓN SOBRE TARJETAS DE CRÉDITO FUERA DE LA ORGANIZACIÓN

## INFORMACIÓN ENVIADA FUERA DE LA ORGANIZACIÓN POR LOS EMPLEADOS

(% de organizaciones)

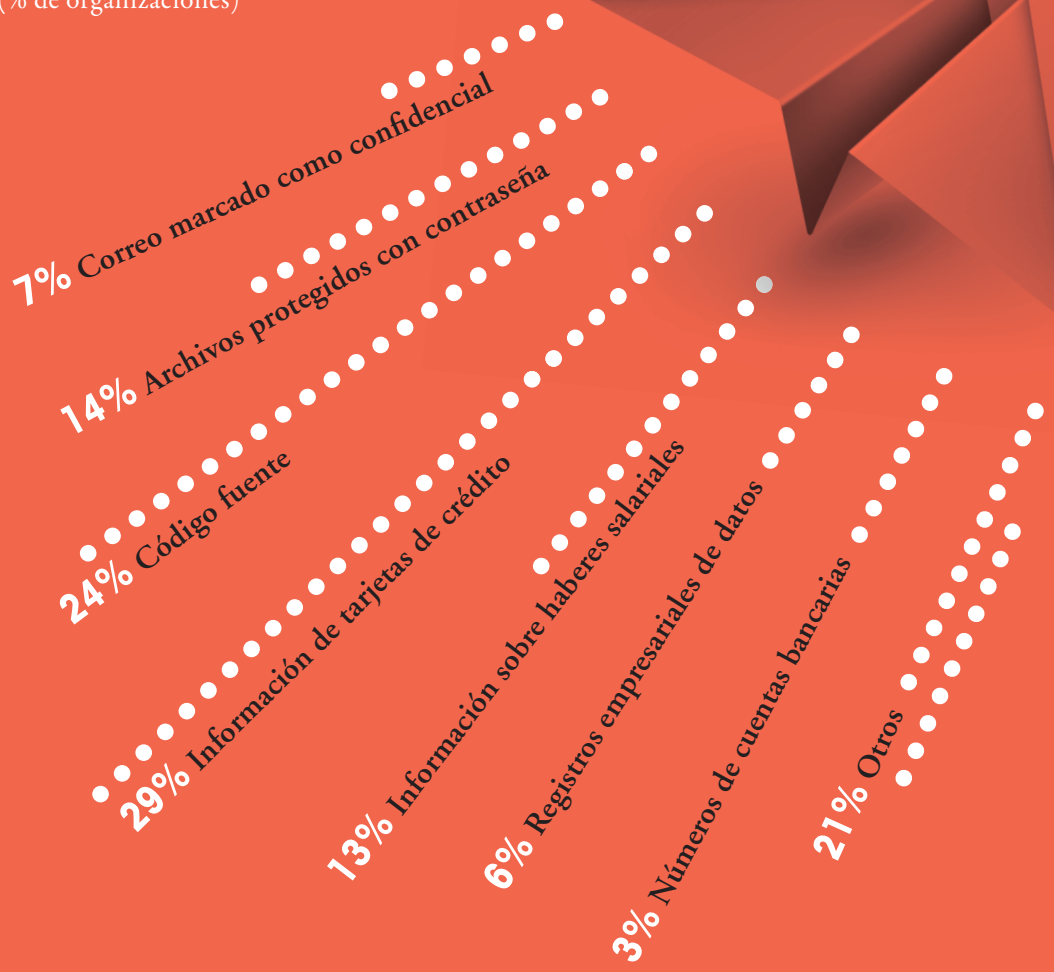



Gráfico 4-C

Fuente: Check Point Software Technologies

Nuestro estudio reveló que en el 29% de las organizaciones se produjo, al menos, uno de estos tipos de eventos durante el tiempo de análisis, lo que indicó que se enviaba fuera de la organización información relacionada con PCI. Se dio, al menos, un caso en el 36% de las organizaciones financieras, que normalmente están obligadas a cumplir la normativa PCI.

## HIPAA

La normativa de privacidad HIPAA proporciona protección federal para la información personal de salud, otorgando a los pacientes un repertorio de derechos respecto a esta información. Al mismo tiempo, esta normativa de privacidad está equilibrada, de modo que permite la utilización de datos personales sanitarios necesarios para el cuidado del paciente y otros propósitos importantes. [27]

La normativa de privacidad HIPAA permite a los centros sanitarios utilizar el correo para hablar de problemas de salud de sus pacientes, guardándose las medidas de seguridad adecuadas. Aunque no se requiere encriptación; sin embargo, deberían aplicarse otros medios de seguridad para proporcionar protección adecuada. ¿Cómo pueden mantenerse abiertos los canales de comunicación por correo con pacientes y colaboradores, protegiendo al tiempo la privacidad y manteniendo la observancia HIPAA de las organizaciones?

En nuestro estudio, monitorizamos el tráfico saliente de las organizaciones analizando los distintos componentes de los mensajes y adjuntos, buscando correos conteniendo información privada de pacientes mediante identificación de información personal (como números de la Seguridad Social) y terminología médica relacionada (términos CPT, ICD-9, LOINC, DME, NDC, etc.). Encontramos que en el 16% de las organizaciones de seguro médico, se enviaba información HIPAA - Protected Health Information fuera de las organizaciones, hacia destinatarios de correo externos o publicándose en línea.

## RECOMENDACIONES DE SEGURIDAD

En el mundo actual de pérdida incremental de datos, les quedan pocas opciones a las organizaciones que iniciar acciones para proteger sus datos sensibles. La mejor forma de prevenir pérdidas de datos no intencionadas es implementar una política corporativa automatizada, que capture la información protegida antes de abandonar la organización. Una solución como ésta se conoce como Data Loss Prevention (DLP). Los productos DLP basados en contenidos ofrecen un amplio repertorio de posibilidades, teniendo las organizaciones múltiples opciones al implantarlas. Antes de implantar una solución DLP, las organizaciones necesitan desarrollar estrategias claras DLP con requisitos concretos como qué se considera como información confidencial, quién puede enviarla y demás.

**EN EL 16%**

**DE ORGANIZACIONES DE CUIDADO Y SEGUROS DE SALUD SE ENVIABA FUERA DE LA ORGANIZACIÓN INFORMACIÓN HIPAA - PROTECTED HEALTH INFORMATION**

## Motor de clasificación de datos

La precisión a la hora de definir datos sensibles es un componente crítico de la solución DLP. La solución DLP debe poder detectar información personal identificable (PII), datos de cumplimiento (HIPAA, SOX, datos PCI, etc.) e información confidencial del negocio. Debería inspeccionarse el flujo de contenidos y reforzar políticas, no sólo en el caso del protocolo usado más ampliamente, como TCP, sino incluyendo SMTP, FTP, HTTP, HTTPS y correo Web. La solución DLP debería poder también inspeccionar por identificación de patrones y clasificación de archivos, para identificar tipos de contenidos con independencia de la extensión consignada al archivo o archivo comprimido. Además, la solución DLP debería poder reconocer y proteger formularios sensibles, basándose en plantillas predefinidas y coincidencia de archivo/formulario. Una importante característica de la solución DLP es su capacidad de crear tipos de datos personalizados para mayor flexibilidad, además de los tipos de datos estándar proporcionados por el proveedor.

## Ayudar a los usuarios a solventar incidentes

Las soluciones tradicionales DLP pueden detectar, clasificar e incluso reconocer documentos específicos y varios tipos de archivos, aunque no pueden conocer las intenciones del usuario que se encuentran detrás del hecho de compartir información sensible. No es suficiente contar sólo con la tecnología, puesto que no puede identificar esta intención y responder contra ella. Por lo tanto, una buena solución DLP necesita la colaboración de los usuarios para conseguir resultados óptimos. Una de estas maneras es enseñar a los usuarios a solucionar incidentes en tiempo real – la solución DLP debería informar al usuario de que su acción podría dar como resultado un incidente potencial de pérdida de datos, animando al usuario a decidir descartar el mensaje o enviarlo de todos modos. Esto mejora la seguridad junto con políticas de uso de datos sensibles alertando a los usuarios de errores potenciales y permitiéndoles corregir inmediatamente, mientras que se mantiene la rápida autorización de comunicaciones legítimas. Esto facilita también la administración. Mientras que el administrador puede seguir los datos DLP para su análisis, no se requiere atención personalizada en tiempo real para cada petición de envío de datos fuera de la compañía.

## Protección contra fuga interna de datos

Otra importante ventaja de DLP es la posibilidad, no sólo de controlar que los datos sensibles abandonen la compañía, sino inspeccionar y controlar los correos sensibles entre departamentos. Así, pueden definirse políticas para prevenir que lleguen datos confidenciales a departamentos equivocados. Ejemplos de datos que sería necesario proteger de pérdida accidental por envío a otros departamentos son planes de compensación, documentos confidenciales de recursos humanos, fusiones y documentos de adquisición o formularios médicos.

## Protección de datos para discos duros de portátiles

Las compañías deben asegurar la información alojada en sus portátiles como parte de una completa política de seguridad. De no proteger esta información, terceros podrían acceder a datos valiosos con la pérdida o robo de portátiles, lo cual podría dar como resultado repercusiones legales o financieras. Una solución adecuada sería prevenir el acceso no autorizado de los usuarios a la información codificando los datos en todos los discos duros de este tipo, incluyendo datos de usuario, archivos del sistema operativo y archivos temporales y eliminados.

## Protección de datos para soportes extraíbles

Para evitar las incidencias de que los datos corporativos residentes en medios de almacenamiento masivo USB y otros caigan en las manos equivocadas, se requiere en estas unidades, como prevención, la codificación de sus contenidos frente a acceso no autorizado. Los empleados suelen mezclar archivos personales como música, imágenes y documentos con archivos del trabajo, como archivos con contenido financiero o de recursos humanos, en soportes extraíbles, lo que supone un desafío mayor para mantener el control sobre los datos corporativos. La brecha de seguridad que suponen las unidades de almacenamiento extraíbles, puede minimizarse mediante la codificación en los casos en los cuales los contenidos puedan estar comprometidos.

## Protección de documentos

Los documentos de empresa se cargan en la Web mediante aplicaciones de almacenamiento de archivos, son enviados a smartphones personales, copiados a soportes extraíbles y compartidos externamente con colaboradores del negocio de forma regular. Cada una de estas operaciones coloca datos sensibles en el riesgo de perderse o ser utilizados de manera inadecuada, así como resultar accesibles a individuos no autorizados. Para mantener los datos corporativos seguros y protegidos, debe disponerse de una solución de seguridad en la forma de política de codificación de documentos para ofrecer acceso sólo a individuos autorizados.

## Gestión de eventos

Definir reglas DLP para crear las políticas de uso de datos de la organización debería acompañarse de buenas opciones de monitorización e informes. Para minimizar la pérdida de datos potencial en una organización, la solución de seguridad debería incluir la monitorización y análisis de los eventos DLP en tiempo real e históricamente. Esto proporciona al administrador de seguridad una visión clara y amplia de la información que se está enviando fuera, sus fuentes y la posibilidad de actuar en tiempo real de ser necesario.

# 05 RESUMEN Y ESTRATEGIA DE SEGURIDAD

CONCLUIREMOS EL INFORME CON OTRA CITA DE SUN ZI TOMADA DEL ARTE DE LA GUERRA: AQUÍ HAY UN CONSEJO PARA UN GENERAL DEL EJÉRCITO:

**"TRAS REUNIR UN EJÉRCITO Y CONCENTRAR SUS FUERZAS, DEBE FUNDIR Y ARMONIZAR LOS DISTINTOS ELEMENTOS ANTES DE LANZAR SU CAMPAÑA."[28]**

2.600 años más tarde, el mismo enfoque se ajusta perfectamente a la lucha actual de la guerra cibernética - la mejor seguridad de la red se consigue cuando las distintas capas de protección se han armonizado todas juntas para luchar contra todos los ángulos de las amenazas de la seguridad.

Este informe ha cubierto múltiples aspectos de los riesgos de seguridad que Check Point ha detectado en un amplio rango de organizaciones. Ha mostrado que bots, virus, violaciones de la seguridad y ataques son una constante y una amenaza real para la seguridad de las organizaciones'. El informe ha presentado que algunas aplicaciones Web usadas por los empleados pueden poner en compromiso la seguridad de la red. Para terminar, el informe ha desvelado que los empleados participan en muchas prácticas que pueden causar una fuga no intencionada de datos confidenciales o sensibles.

## En su estrategia de seguridad: La tecnología sólo no es suficiente

El enfoque de Check Point para conseguir el nivel de seguridad necesario para proteger una organización reconoce que la tecnología por sí sola no es suficiente. La seguridad necesita crecer desde una colección dispar de tecnologías y prácticas, hasta un proceso empresarial efectivo. Check Point recomienda que las organizaciones se fijen en las tres dimensiones a la hora de implementar una estrategia y solución de seguridad: Políticas, Personas y Cumplimiento.

## Políticas

La seguridad empieza con una política ampliamente entendida y bien definida — alineada estrechamente con las necesidades del negocio más que una simple colección de comprobaciones a nivel de sistema y tecnologías dispares. Las políticas deberían tener en cuenta que la prioridad es el negocio, y deberían sugerir formas de conducir el negocio de una forma segura, como parte de la política corporativa. Por ejemplo, durante el análisis encontramos que los empleados utilizan aplicaciones Web que son necesarias para el flujo del negocio pero también pueden comprometer la seguridad. Si implantamos sólo tecnologías que bloqueen el uso de este tipo de aplicaciones Web, lo que conseguiremos será inundar al administrador de seguridad con multitud de gente quejándose, o lo que es peor, buscando formas de burlar la política y generar situaciones de riesgo. En lugar de eso, Check Point recomienda crear una política que reconozca los casos donde el uso de estas aplicaciones sea necesario y definir el procedimiento para hacer cumplir su utilización de una forma segura. Los usuarios deberían ser aconsejados de forma automática de la política cuando sea necesario.

## Personas

Los usuarios de sistemas informáticos son una parte crítica del proceso de seguridad. Suelen ser los usuarios los que cometen errores que resultan en infecciones de malware y fuga de información. Las organizaciones deberían asegurar que los usuarios están comprometidos con los procesos

de seguridad. Los empleados necesitan estar informados y educados en la política de seguridad y lo que se espera de ellos cuando navegan por Internet o comparten datos sensibles. Al mismo tiempo, la seguridad debería ser todo lo continua y transparente que sea posible y no debería cambiar la forma en la que trabajan los usuarios.
La implementación de un programa de seguridad debería incluir:

- Un programa de educación o formación – que garantice que todos los usuarios son conscientes de que los sistemas son vulnerables a los ataques y de que sus propias acciones pueden permitirlos o ayudar a prevenirlos.
- Tecnología - asesorar a las personas en tiempo real de por qué determinadas operaciones son peligrosas y cómo podrían llevarlas a cabo de una forma segura.

## Cumplimiento

La implantación de soluciones tecnológicas de seguridad como software Security Gateways y Endpoint es crítica para proteger a las organizaciones de violaciones de la seguridad y pérdida de datos. Los Security Gateways deberían instalarse en todas las interconexiones, asegurando de que solamente tráfico relevante o autorizado entra o sale de la red. Esta validación debería hacerse en todas las capas de la seguridad y en todas las comunicaciones, protocolos, métodos, consultas, respuestas y cargas útiles usando el cortafuegos, control de aplicaciones, filtrado de URLs, DLP, IPS, soluciones de seguridad antivirus y antibot.

# 06 ACERCA DE CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies Ltd. (www.checkpoint.com), el líder mundial en seguridad en Internet, proporciona a los clientes protección sin compromiso frente a todo tipo de amenazas, reduce la complejidad de la seguridad y reduce el coste total de la propiedad. Check Point fue el pionero de la industria con FireWall-1 y su tecnología patentada Stateful Inspection. Hoy Check Point continua desarrollando nuevas soluciones basadas en la arquitectura Software Blade, que ofrece a los clientes las soluciones flexibles y sencillas que pueden personalizarse completamente para ajustarse a las necesidades de seguridad específicas de cualquier organización.

Check Point es el único proveedor que más más allá de la tecnología y define la seguridad como un proceso más del negocio. Check Point 3D Security combina de forma única políticas, personas y la aplicación de un mayor nivel de protección de los activos de información y ayuda a las organizaciones a implementar un plan de seguridad que se alinee con las necesidades del negocio. Entre sus clientes se incluyen decenas de miles de organizaciones de todos los tamaños, incluyendo todas las empresas Fortune y Global 100. Las galardonadas soluciones ZoneAlarm de Check Point protegen millones de consumidores de hackers, spyware y robos de identidad.

## Check Point 3D Security

Check Point 3D Security redefine la seguridad como un proceso del negocio de 3 dimensiones que combina políticas, personas y cumplimiento para lograr un protección más sólida en todas las capas de la seguridad —incluyendo la red, los datos y los puntos finales. Para lograr el nivel de protección necesario en el siglo 21, la seguridad necesita crecer desde una colección de tecnologías dispares a un proceso de negocio efectivo.

Con 3D Security, las organizaciones pueden ahora implementar un plan de seguridad que va más allá de las tecnologías para garantizar la integridad de toda la seguridad de la información.

Check Point 3D Security permite a las organizaciones redefinir la seguridad mediante la integración de estas tres dimensiones en el proceso del negocio:

**Políticas** que apoyan a las necesidades del negocio y trasforman la seguridad en un proceso más del negocio.

Seguridad que involucra a las **personas** en la definición de las políticas, educación y resolución de incidentes.

**Hacer cumplir**, consolidar y controlar todas las capas de la seguridad - redes, datos, aplicaciones, contenido y usuarios.

## Arquitectura Check Point Software Blade

Como herramienta clave para crear una seguridad 3D verdadera, la arquitectura Software Blade de Check Point™ permite a las empresas hacer cumplir las políticas de seguridad mientras ayuda a formar a los usuarios en esas políticas. La arquitectura Software Blade es la primera y única arquitectura de seguridad que suministra seguridad integral, flexible, y administrable a empresas de cualquier tamaño. Es más, a medida que aparecen nuevas amenazas la arquitectura Software Blade de Check Point amplía de rápidamente y de forma flexible sus servicios de seguridad bajo demanda — sin la adición de nuevo hardware o

complejidad de administración. Las soluciones se gestionan centralmente a través de una única consola que reduce la complejidad y la sobrecarga operativa. La protección multicapa es fundamental hoy en día para combatir las amenazas dinámicas como bots, troyanos, y amenazas persistentes avanzadas (APTs). Los cortafuegos son hoy en día más unas pasarelas o gateways multifunción pero no todas las empresas quieren el mismo nivel de seguridad en todos sitios.

Las empresas buscan flexibilidad y control en sus recursos de seguridad. Software Blades son aplicaciones de seguridad o módulos como un cortafuego, redes privadas virtuales (VPN), sistemas de prevención de intrusiones (IPS) o control de aplicaciones por nombrar unas pocas, que son independientes, modulares y administradas de forma centralizada. Ellos permiten a las organizaciones personalizar una configuración de seguridad que tiene como objetivo una mezcla correcta de protección e inversión. Software Blades puede habilitarse rápidamente y configurarse en cualquier gateway o sistema de administración con un simple clic de ratón — sin necesidad de actualizar hardware, firmware o drivers. A medida que necesite evolucionar, pueden activarse fácilmente Software Blades adicionales para ampliar la seguridad a una configuración existente en el mismo hardware de seguridad.

## Check Point Security Gateway SmartDashboard. Pantalla de activación de Software Blades


Check Point ofrece una gestión centralizada de eventos para todos los productos Check Point además de para dispositivos de terceros. Proporcionando vistas en tiempo real de las incidencias de seguridad ayuda comprender rápidamente la situación de seguridad y tomar medidas de forma inmediata, todo ello a través de la única consola. La vista de línea de tiempo (timeline) permite la visualización de las tendencias y propagación de los ataques. La vista de gráficas ofrece estadísticas de eventos en formato de diagrama circular o gráfico de barras. La vista de mapas muestra las amenazas potenciales por países.

## Gestión de incidencias de seguridad de Check Point SmartEvent. Vista en tiempo real.

## Feeds de inteligencia de seguridad en tiempo real de ThreatCloud™

ThreatCloud es una red colaborativa y base de datos de conocimientos basada en la nube que suministra inteligencia de seguridad dinámica en tiempo real a los gateways de seguridad. Esa inteligencia se utiliza para identificar infecciones nuevas y tendencias de amenazas. ThreatCloud potencia los Software Blade Anti-Bot permitiendo a los gateways investigar IPs siempre cambiantes, direcciones DNS y URL de donde se conocen los centros de control y comando. Dado que el procesamiento se realiza en la nube, pueden analizarse millones de formas y la protección malware en tiempo real.

La base de datos de conocimiento de ThreatCloud se actualiza dinámicamente usando feeds de una red global de sensores de amenazas, información de ataques de gateways de todo el mundo, los laboratorios de investigación de Check Point y los mejores feeds de malware de la industria. La información relacionada sobre amenazas de la seguridad se comparte entre todos los gateways de forma colectiva.


**Check Point 61000 Appliance**

THREATCLOUD

## Apliances de seguridad Check Point

En las redes empresariales de hoy en día, los gateways de seguridad son más como un cortafuego — son dispositivos que se encuentran ante un número siempre creciente de amenazas sofisticadas. Deben hacer uso de múltiples tecnologías para controlar el acceso a la red, detectar ataques sofisticados y proporcionar capacidades de seguridad adicionales como la prevención ante la pérdida de datos, protección de amenazas basadas en Web y la capacidad de asegurar el cada vez mayor número de dispositivos móviles como el iPhone y los tablets en las redes corporativas. Este número creciente de amenazas y capacidades de seguridad demandan un mayor rendimiento y versatilidad para los appliances de seguridad.

Equipados con Check Point GAiA, el sistema operativo de seguridad de la siguiente generación, los appliances de Check Point combinan alto rendimiento con capacidades multi-core con rápidas tecnologías de red que proporcionan el más alto nivel de seguridad de los datos, redes y empleados. Optimizados para la arquitectura ampliable Software Blades, cada appliance es capaz de ejecutar cualquier combinación de Software Blades, incluyendo Firewall, IPsec VPN, IPS, Application Control, Mobile Access, DLP, URL Filtering, Anti-Bot, Antivirus, Anti-spam, Identity Awareness y Advanced Networking & Clustering, proporcionando la flexibilidad u el nivel preciso de seguridad para cualquier negocio en cualquier lugar de la red.

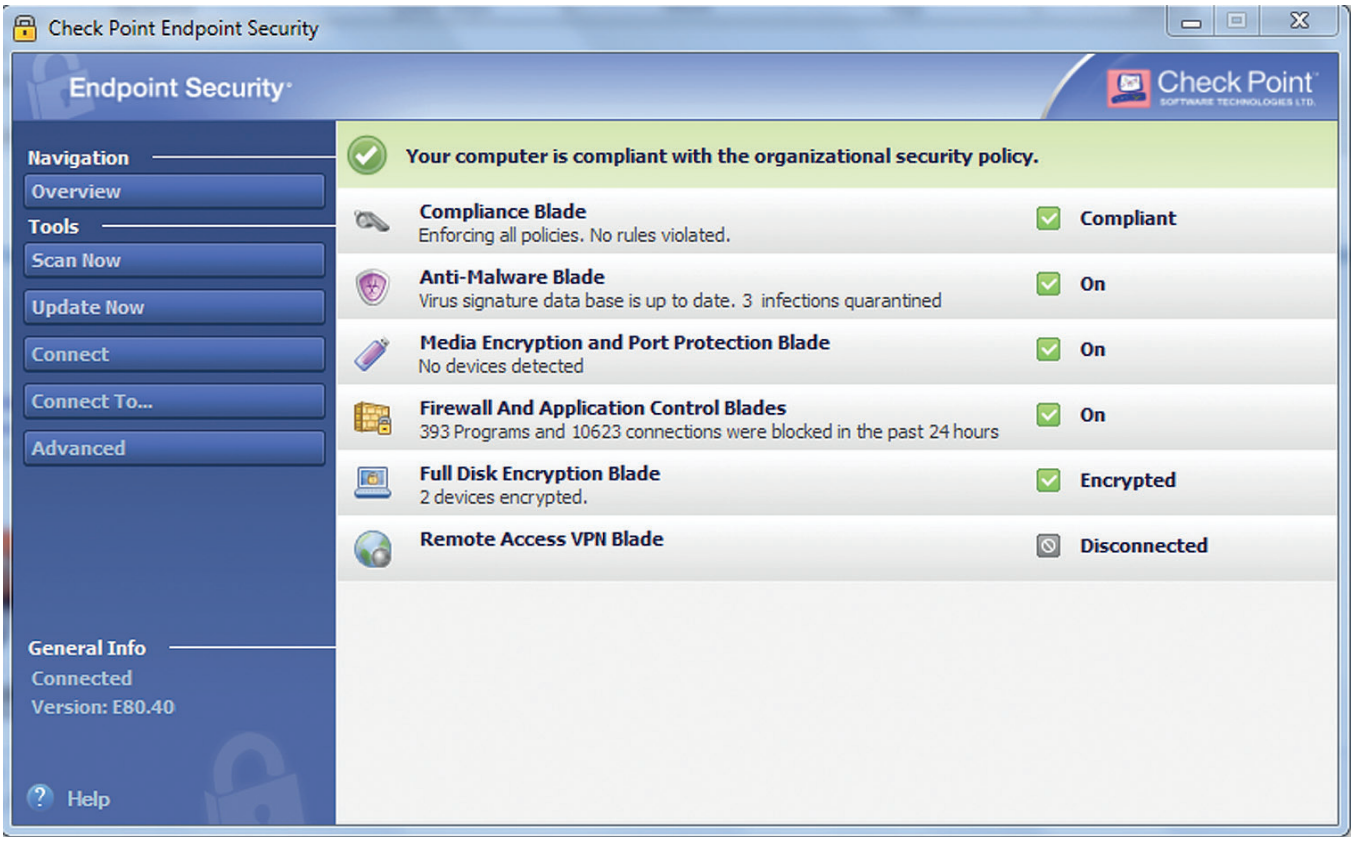
Al consolidar múltiples tecnologías de seguridad en un único gateway de seguridad, los appliances están diseñados para suministrar avanzadas soluciones de seguridad integradas para satisfacer todas las necesidades de seguridad empresarial de una organización. Presentado en agosto de 2011, SecurityPower™ es un indicador que mide la capacidad de un appliance para realizar múltiples funciones avanzadas en un volumen de tráfico específico. Proporciona un punto de referencia revolucionario que permite a los clientes seleccionar los appliances de seguridad adecuados para sus escenarios de implantación específicos. Las tasas SecurityPower se determinan basándose en el tráfico de clientes del mundo real, múltiples funciones de seguridad y una política de seguridad típica.

## Seguridad para puntos finales de Check Point

Endpoint Security Software Blades de Check Point trae un flexibilidad , control y eficiencia sin precedentes a la gestión e implantación de la seguridad para puntos finales. Los gestores de TI pueden elegir entre seis Endpoint Software Blades para implementar únicamente la protección que necesitan, con la libertad de incrementar la seguridad en cualquier momento. **Full Disk Encryption Software Blade** asegura automáticamente y de forma transparente toda la información en los discos duros de dispositivos de punto final. La autenticación previa al arranque de múltiples factores asegura la identidad del usuario. **Media Encryption Software Blade** proporciona cifrado aplicable de forma centralizada para medios de almacenamiento extraíbles, con la granularidad necesaria para cifrar únicamente datos relacionados con la empresa mientras fomenta la participación y educación del usuario final. **Remote Access VPN Software Blade** proporciona a los usuarios acceso seguro continuo a redes y recursos corporativos mientras viaja o trabaja de forma remota. **Anti-Malware y Program Control Software Blade** detecta y elimina de forma eficiente malware de puntos finales con un único análisis. Program Control asegura que únicamente programas legítimos y validados se ejecutan en los puntos finales. **Firewall y Security Compliance Verification Software Blade** proporciona protección proactiva para el tráfico entrante y saliente evitando que el malware pueda infectar los sistemas de puntos finales, bloqueando ataques dirigidos y deteniendo el tráfico no deseado. Security Compliance Verification asegura que sus puntos finales siempre satisfacen las políticas de seguridad de la organización.

**WebCheck Secure Browsing Software Blade** le protege frente a las últimas amenazas basadas en Web incluyendo las descargas ocultas, sitios de phishing y ataques de día cero. Las sesiones del navegador se ejecutan en un entorno virtual seguro.

## Cliente Check Point Endpoint Security



# A APÉNDICE A: MALWARE MÁS IMPORTANTE

Este apéndice proporciona más información relacionada con los principales tipos de malware encontrados en nuestro estudio. La base de datos completa de malware de Check Point está disponible en threatwiki.checkpoint.com

**Zeus** es un agente bot de puerta trasera dirigido a la plataforma Windows. Una puerta trasera (backdoor) es un método de superar los procedimientos de autenticación. Una vez que un sistema se ha puesto en riesgo, pueden instalarse una o más puertas traseras de cara a facilitar el acceso en el futuro29. Nuestra investigación detectó bots Zeus generados usando la versión 2.0.8.9 del toolkit Zeus. Zeus es una extensa familia de troyanos bancarios con un número considerable de versiones y variantes in-the-wild. El malware proporciona al atacante acceso remoto a los sistemas infectados. Su objetivo principal es robar las credenciales bancarias utilizadas por los usuarios objetivo cuando acceden a sus cuentas.

**Zwangi** es un adware cuyo objetivo es la plataforma Microsoft Windows. Se registra como un objeto complemento para el navegador en el sistema infectado. Puede crear una barra de herramientas personalizada dentro de Internet Explorer y presenta al usuario mensajes publicitarios no deseados. Este malware infecta los sistemas a través de paquetes de software.

**Sality** es un virus que se distribuye a sí mismo mediante la infección y modificación de archivos ejecutables copiándose también a unidades extraíbles o carpetas compartidas.

**Kuluoz** es un bot cuyo objetivo es la plataforma Microsoft Windows. Este bot, según se informa, se envía en mensajes de spam que simulan ser del servicio postal de EE.UU. Envía al exterior información del sistema y acepta instrucciones de un servidor remoto para descargar y ejecutar archivos maliciosos en el equipo infectado. Es más, crea una entrada en el registro para iniciarse tras un reinicio del sistema.

**Juasek** es un bot de puerta trasera dirigido a la plataforma Microsoft Windows. Este malware permite a un atacante remoto no autenticado realizar acciones maliciosas como abrir un shell de comando, descargar o subir archivos, crear nuevos procesos, listar/finalizar procesos, buscar/crear/borrar archivos, y recuperar información del sistema. Además, instala un servicio para sobrevivir a los reinicios del sistema.

**Papras** es un troyano bancario que se dirige a las plataformas Microsoft Windows de 32 y 64 bits. Este malware envía al exterior información del sistema y solicita información de la configuración desde un host remoto. Conecta con las funciones de red y monitoriza las actividades en internet del usuario‘ para robar información financiera crítica. Además, posee una funcionalidad de puerta trasera para proporcionar a los atacantes remotos acceso no autorizado a los equipos infectados. Los comandos de control aceptados incluyen la descarga de archivos maliciosos, recopilar cookies e información de certificados, reiniciar y apagar el sistema, enviar al exterior información de inicio de sesión, tomar capturas de pantalla, configurar una conexión socket a un host remoto para otras actividades, etc. Por otra parte el malware se inyecta a sí mismo en los procesos y puede inyectar también otros archivos maliciosos en los procesos del objetivo.

# B APÉNDICE B: LAS APLICACIONES DE MAYOR RIESGO

Este apéndice proporciona más información relacionada con las principales aplicaciones encontradas en nuestro estudio. La base de datos completa de aplicaciones de riesgo de Check Point se encuentra en appwiki.checkpoint.com

## Anonimizadores

**Tor** es una aplicación cuyo objetivo es permitir el anonimato cuando se está online. El software cliente Tor direcciona el tráfico de Internet a través de una red de servidores mundial para ocultar la ubicación del usuario' o utilización de cualquiera que esté vigilando la red o haciendo un análisis del tráfico. Usando Tor se dificulta el rastreo de la actividad en Internet de usuario, incluyendo "visitas a sitios Web, publicaciones online, mensajería instantánea y otras formas de comunicación".

**CGI-Proxy** es un paquete software Common Gateway Interface. Aparece para el usuario como una página Web que permite el acceso a un sitio diferente. Entre los protocolos soportados se incluye HTTP, FTP y SSL.

**Hopster** es una aplicación para eludir cortafuegos y servidores proxy, permitiendo la navegación y chat anónimo.

**Hide My Ass** es un servicio de proxy gratuito web que enmascara las direcciones IP que permite a los usuarios conectarse a sitios web de forma anónima.

**Hamachi** es una aplicación shareware de red privada virtual (VPN). Se utiliza para establecer una conexión en Internet que simula la conexión sobre una red de área local (LAN).

**Ultrasurf** es una herramienta proxy gratuita que permite a los usuarios eludir los cortafuegos y el software de bloque de contenidos de Internet.

**OpenVPN** es una aplicación gratuita de software libre que implementa técnicas de red privada virtual (VPN) para crear conexiones seguras punto a punto o sitio a sitio en configuraciones enrutadas o bridge e instalaciones de acceso remoto.

## Intercambio de archivos P2P

**BitTorrent** es un protocolo de comunicación P2P para el intercambio de archivos peer-to-peer. Es un método de distribuir grandes cantidades de datos de forma amplia sin que el distribuidor original incurra en los costes de los recursos de hardware, hosting y ancho de banda. En lugar de eso, cuando se distribuyen los datos usando el protocolo BitTorrent, cada destinatario proporciona fragmentos de de los datos a los nuevos destinatarios, reduciendo el coste y la carga de cualquier fuente individual, proporcionando redundancia frente a problemas del sistema, y reduciendo la dependencia del distribuidor original. Existen numerosos clientes compatibles con BitTorrent, escritos en diversos lenguajes de programación y que se ejecutan en diversas plataformas informáticas.

**eMule** es una aplicación de intercambio de archivos peer-to-peer que se conecta a las redes eDonkey y Kad. El software proporciona intercambio directo de fuentes entre los nodos cliente, recuperación de descargas corruptas y la utilización de un sistema de crédito para recompensar a los usuarios que frecuentemente suben datos. eMule transmite los datos con compresión zlib para ahorrar ancho de banda.

**Soulseek** es una aplicación de intercambio de archivos peer-to-peer. Se utiliza principalmente para el intercambio de música, aunque los usuarios pueden intercambiar otro tipo de archivos.

**Gnutella** es una conocida red de intercambio de archivos, y uno de los protocolos peer-to-peer más populares, lo utilizan aplicaciones como BearShare, Shareaza, Morpheus y iMesh. Se utiliza normalmente para intercambiar archivos de música MP3, vídeos, aplicaciones y documentos.

**Sopcast** es una aplicación de streaming de medios que permite hacer streaming a través de redes P2P. Sopcast permite a los usuarios la difusión de medios a otros usuarios o ver streams emitidos por otros usuarios.

## Herramientas de administración remota

**Remote Desktop Protocol (RDP)** es una aplicación propietaria desarrollada por Microsoft que proporciona al usuario una interfaz remota a otro equipo.

**Team Viewer** permite a los usuarios controlar equipos remotos usando un software cliente o iniciando sesión en un sitio Web.

LogMeIn es una suite de servicios software que proporciona acceso remoto a equipos a través de Internet. Las diversas versiones de producto están diseñadas tanto para usuarios finales como personal profesional de help desk. Los productos de acceso remoto LogMeIn usan un protocolo de escritorio remoto propio que se transmite vía SSL. Los usuarios acceden a los escritorios remotos usando un portal Web basado en Internet y, opcionalmente la aplicación independiente LogMeIn Ignition.

**VNC** es un software que consiste en un servidor y aplicación cliente para el protocolo Virtual Network Computing (VNC) para controlar otro equipo de forma remota. El software puede ejecutarse en Windows, Mac OS X, y sistemas operativos tipo Unix. VNC también se ejecuta en la plataforma Java y en el iPhone, iPod touch o iPad de Apple.

## Aplicaciones de intercambio y almacenamiento de archivos

**Dropbox** es una aplicación que permite a los usuarios compartir archivos. Dropbox es un servicio de hosting de archivos operado por Dropbox, Incque ofrece almacenamiento cloud, sincronización de archivos y software cliente. En resumen, Dropbox permite a los usuarios crear una carpeta especial en cada uno de sus equipos, que Dropbox sincroniza de forma que aparezca como la misma carpeta (con el mismo contenido) independientemente del equipo en el que se vea. Los archivos depositados en esta carpeta también son accesibles a través de un sitio web y de aplicaciones de teléfonos móviles.

**Windows Live Office** es una herramienta de edición, intercambio y almacenamiento de documentos de Microsoft Office creada por Microsoft. Con Office Web Apps, los usuarios pueden crear, ver, editar, compartir, ser coautores o colaborar en los documentos, hojas de cálculo, presentaciones y notas online, desde cualquier lugar a través de una conexión de Internet.

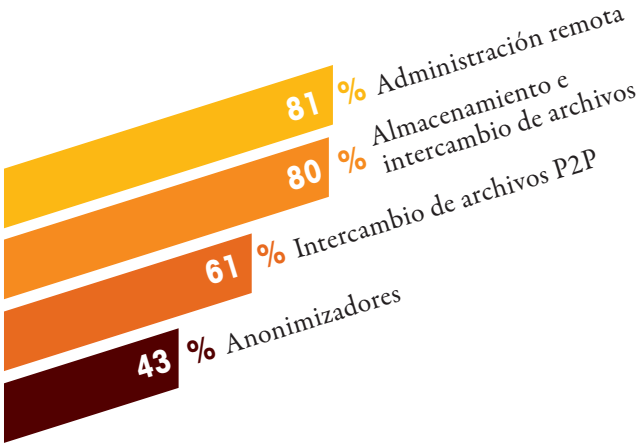
**Curl** es una herramienta de línea de comando que permite a los usuarios transferir datos con sintaxis URL. Soporta FILE, FTP, HTTP, HTTPS, certificados SSL y otros protocolos de transferencia.

**YouSendIt** es un servicio de envío de archivos digitales. El servicio permite a los usuarios enviar, recibir y hacer el seguimiento de archivos bajo demanda.

# C APÉNDICE C: RESULTADOS ADICIONALES DE LA UTILIZACIÓN DE APLICACIONES WEB

La siguiente información proporciona datos adicionales a los hallazgos presentados en la sección "Aplicaciones en el espacio de trabajo empresarial".
Las gráficas C-A y C-B resumen la utilización de aplicaciones por categorías y por regiones.

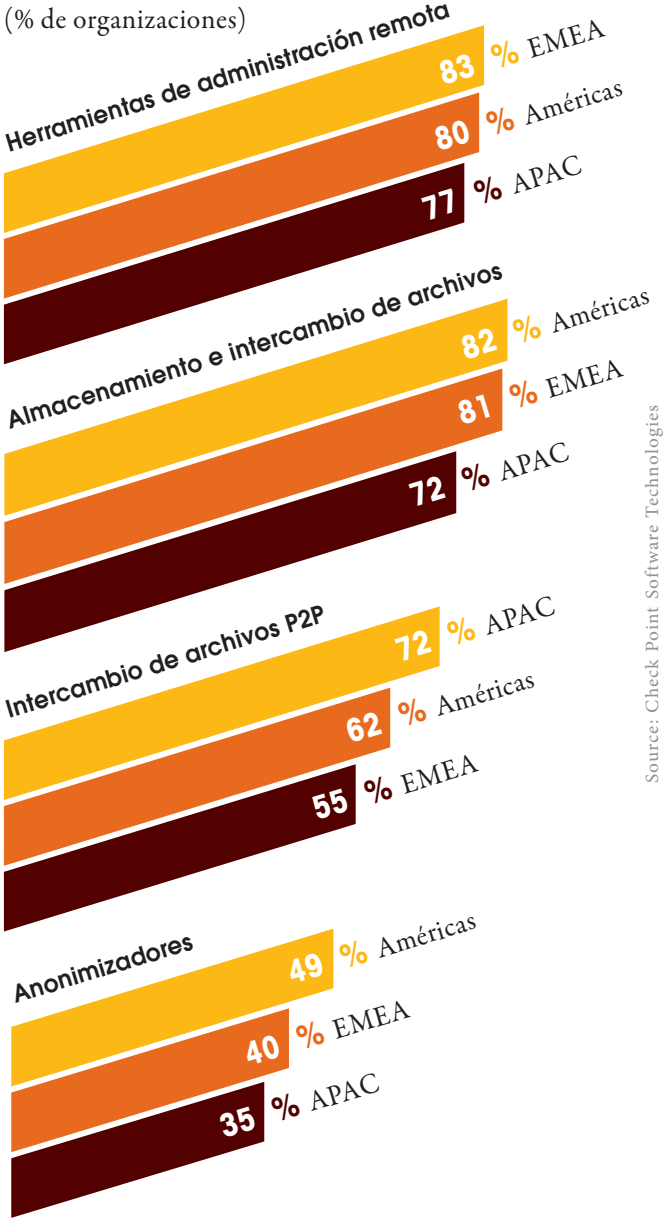
## Uso de aplicaciones por categoría
(% de organizaciones)




Fuente: Check Point Software Technologies

**Gráfica C-A**

## Uso de aplicaciones por región
(% de organizaciones)




Source: Check Point Software Technologies

**Gráfica C-B**

Las siguientes tablas proporcionan información adicional sobre los clientes BitTorrent y Gnutella más conocidos

| clientes Principales BitTorrent | Número de organizaciones |
|---|---|
| Vuze | 108 |
| Xunlei | 74 |
| uTorrent | 55 |
| BitComet | 25 |
| FlashGet | 21 |
| QQ Download | 8 |
| Pando | 7 |
| P2P Cache | 7 |
| Transmission | 6 |
| Other | 242 |

| Principales clientes Gnutella | Número de organizaciones |
|---|---|
| BearShare | 52 |
| LimeWire | 23 |
| FrostWire | 16 |
| Foxy | 2 |
| Other | 31 |

La tabla inferior ofrece información sobre las aplicaciones más utilizadas por categoría y región

| Categoría de aplicación | Región | Nombre de aplicación | % de organizaciones |
|---|---|---|---|
| Anonymizer | Américas | Tor | 24% |
| | | CGI-Proxy | 16% |
| | | Hamachi | 8% |
| | | Hopster | 8% |
| | | Ultrasurf | 7% |
| | EMEA | Tor | 23% |
| | | CGI-Proxy | 12% |
| | | Hamachi | 4% |
| | | Hopster | 7% |
| | | Hide My Ass | 7% |
| | APAC | Tor | 20% |
| | | Hopster | 6% |
| | | CGI-Proxy | 6% |
| | | Hamachi | 6% |
| | | Hide My Ass | 7% |

| Categoría de aplicación | Región | Nombre de aplicación | % de organizaciones |
|---|---|---|---|
| Intercambio de archivos P2P | Américas | Clientes BitTorrent | 35% |
| | | SoulSeek | 23% |
| | | eMule | 21% |
| | | Windows Live Mesh | 8% |
| | | Sopcast | 8% |
| | EMEA | Clientes BitTorrent | 33% |
| | | SoulSeek | 19% |
| | | eMule | 15% |
| | | Sopcast | 12% |
| | | iMesh | 10% |
| | APAC | Clientes BitTorrent | 62% |
| | | eMule | 26% |
| | | SoulSeek | 11% |
| | | Sopcast | 10% |
| | | BearShare | 8% |
| Almacenamiento e intercambio de archivos | Américas | Dropbox | 73% |
| | | Windows Live Office | 52% |
| | | Curl | 28% |
| | | YouSendIt | 26% |
| | | ZumoDrive | 12% |
| | EMEA | Dropbox | 71% |
| | | Windows Live Office | 51% |
| | | Curl | 22% |
| | | YouSendIt | 21% |
| | | ImageVenue | 18% |
| | APAC | Dropbox | 57% |
| | | Windows Live Office | 50% |
| | | Curl | 26% |
| | | YouSendIt | 16% |
| | | Hotfile | 10% |

| Categoría de aplicación | Región | Nombre de aplicación | % de organizaciones |
|---|---|---|---|
| Administración remota | Américas | MS-RDP | 59% |
| | | LogMeIn | 51% |
| | | TeamViewer | 45% |
| | | VNC | 14% |
| | | Bomgar | 8% |
| | EMEA | MS-RDP | 60% |
| | | TeamViewer | 55% |
| | | LogMeIn | 44% |
| | | VNC | 20% |
| | | pcAnywhere | 3% |
| | APAC | TeamViewer | 58% |
| | | MS-RDP | 51% |
| | | LogMeIn | 26% |
| | | VNC | 16% |
| | | Gbridge | 3% |

# D APÉNDICE D: TIPOS DE DATOS DLP

Nuestra investigación incluyó el análisis de docenas de tipos de datos en la búsqueda de incidencias potenciales de pérdida de datos La siguiente lista presenta los principales tipos de datos inspeccionados y detectados por Check Point DLP Software Blade.

**Código fuente** - Incluye datos que contienen líneas de lenguajes de programación, como C, C++, C#, JAVA y otros; indica fugas de propiedad intelectual.

**Información de tarjetas de crédito** - incluye dos tipos de datos: números de tarjetas de crédito y PCI - Datos de autenticación sensibles.

- **Números de tarjetas de crédito:**

**Criterio de selección:** Relativos a la Industria de Tarjetas de pago (Payment Card Industry - PCI); coincide con datos que contienen números de tarjetas de crédito de MasterCard, Visa, JCB, American Express, Discover y Diners Club; la coincidencia se basa en el patrón (expresión normal) y validación de los dígitos de control en el esquema definido en el Anexo B de la ISO/IEC 7812-1 y en JTC 1/ SC 17 (Luhn MOD-10 algorithm); indica la fuga de información confidencial.

**Ejemplo:** 4580-0000-0000-0000.

- **PCI - Datos sensibles de autenticación:**

**Criterio de coincidencia:** Relativos a la industria de las tarjetas de pago (Payment Card Industry - PCI); coincide con información que es clasificada como datos sensibles de autenticación (Sensitive Authentication Data) según el PCI Data Security Standard (DSS). Dichos datos, al contrario de los datos del titular de la tarjeta, son extremadamente confidenciales y el PCI DSS no permite su almacenamiento. Se ajusta a los datos que contiene la cinta magnética de la tarjeta de crédito (pista 1, 2 o 3), un PIN cifrado o no cifrado y un Card Security Code (CSC).

**Ejemplos:**%B4580000000000000^JAMES /L.^99011200000000000?, 2580.D0D6.B489.DD1B, 2827.

**Archivos protegidos por contraseña** - se ajusta a archivos que están protegidos o cifrados con contraseña. Este tipo de archivos contienen información confidencial.

**Archivos de nómina** - Se ajusta a archivos que contienen la nómina, carta de pago, recibo de sueldo, etc.; indica pérdida de información personal.

Email confidencial - Se ajusta a mensajes de Microsoft Outlook que fueron marcados por el remitente como <Confidencial>; este tipo de emails normalmente contienen información sensible. Nota: Microsoft Outlook permite al remitente marcar los emails enviados con distintos valores de sensibilidad; este tipo de datos coinciden con emails marcados como <Confidencial> con la opción de Outlook.

**Información de compensación de salarios** - Coincide con documentos que contienen palabras y frases con datos de compensación de empleados como: salarios, bonus, etc.

**Otros tipos de datos detectados durante la investigación:** Documento de identidad de Hong Kong, Términos de informes financieros¸ números de cuentas bancarias, IBAN Finlandia, Números de seguros sociales de Canadá, FERPA - Confidential Educational Records, Códigos Postales de EE.UU., Números de registro VAT UK, Números de la seguridad social de México, Números de la seguridad social de EE.UU., Calificaciones de estudiantes – GPA, Informes de Salesforce, Códigos de identificación personal de Finlandia, ITAR - International Traffic in Arms Regulations, Registros personales sensibles, Diseños o archivos de diseño gráfico CAD-CAM, HIPAA - Información sanitaria protegida, Números de la seguridad social de Francia, Nombres de empleados, PCI - Datos de titulares, Números de licencias de conducir EE.UU., HIPAA - Números de registros sanitarios, Números de seguros sociales de Canadá, IBAN Finlandia, HIPAA - ICD-9, IBAN Dinamarca, Registros VAT Finlandia, Códigos de identidad personal de Finlandia, Números de cuentas bancarias internacionales, y otros.

# REFERENCIAS

[1] The Art of War By Sun Tzu, http://suntzusaid.com/artofwar.pdf
[2] http://www.checkpoint.com/campaigns/3d-analysis-tool/index.html
[3] http://www.checkpoint.com/products/threatcloud/index.html
[4] http://supportcontent.checkpoint.com/file_download?id=20602
[5] http://www.nytimes.com/2012/03/05/technology/the-bright-side-of-being-hacked.html?pagewanted=2&ref=global-home
[6] http://edition.cnn.com/video/#/video/bestoftv/2012/10/01/exp-erin-cyberattack-nuclear-networks-leighton.cnn?iref=allsearch
[7] http://www.networkworld.com/news/2012/071312-security-snafus-260874.html?page=4
[8] http://www.businessweek.com/news/2012-10-18/bank-cyber-attacks-enter-fifth-week-as-hackers-adapt-to-defenses
[9] http://arstechnica.com/security/2012/09/blackhole-2-0-gives-hackers-stealthier-ways-to-pwn/
[10] http://www.networkworld.com/slideshow/52525/#slide1
[11] http://www.ihealthbeat.org/articles/2012/10/30/breaches-at-uks-nhs-exposed-nearly-18m-patient-health-records.aspx
[12] http://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf
[13] http://cve.mitre.org/index.html
[14] http://www.networkworld.com/news/2012/020912-foxconn-said-to-have-been-255917.html
[15] http://news.cnet.com/8301-1009_3-57439718-83/anonymous-attacks-justice-dept-nabbing-1.7gb-of-data/
[16] http://news.cnet.com/8301-1009_3-57396114-83/vatican-anonymous-hacked-us-again/
[17] http://news.cnet.com/8301-1023_3-57411619-93/anonymous-hacks-into-tech-and-telecom-sites/
[18] http://www.ftc.gov/opa/2012/06/epn-franklin.shtm
[19] http://www.ftc.gov/opa/2010/02/p2palert.shtm
[20] http://www.networkworld.com/news/2012/091212-botnet-masters-hide-command-and-262402.html
[21] http://www.computerworld.com/s/article/9221335/_Nitro_hackers_use_stock_malware_to_steal_chemical_defense_secres
[22] http://bits.blogs.nytimes.com/2012/08/01/dropbox-spam-attack-tied-to-stolen-employee-password/
[23] http://news.cnet.com/8301-31921_3-20072755-281/dropbox-confirms-security-glitch-no-password-required/
[24] http://japandailypress.com/newspaper-reporter-fired-for-emailing-sensitive-info-to-wrong-people-159277
[25] http://www.roanoke.com/news/roanoke/wb/307564
[26] http://tamutimes.tamu.edu/2012/04/13/am-acting-on-email-message-that-inadvertently-included-some-alumni-ss-numbers/
[27] www.hhs.gov/ocr/privacy/hipaa/index.html
[28] The Art of War By Sun Tzu, http://suntzusaid.com/artofwar.pdf
[29] http://en.wikipedia.org/wiki/Malware#Backdoors

INFORME DE SEGURIDAD 2013 DE CHECK POINT


www.checkpoint.com

## CONTACTE CON CHECK POINT

**Oficinas centrales mundiales**
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

**Oficinas en EE.UU.**
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com



Febrero de 2013



Design: RoniLevit.com