Hewlett Packard Enterprise

# CIBERRIESGO
## Informe de 2016

El Informe de Ciberriesgo anual de HP Security Research sirve para que las organizaciones comprendan mejor el entorno de las amenazas y suministra los recursos que pueden ayudar a minimizar los riesgos en la seguridad. El informe de este año presenta perspectivas obtenidas de un análisis de datos avanzado y presta especial atención a varias tecnologías como, por ejemplo, las de fuente abierta, móvil y el Internet de las cosas.

35%

Más de un tercio de las aplicaciones exploradas, el 35%, mostraron al menos una vulnerabilidad crítica o de alta importancia.

Casi el **86%** de las empresas encuestadas indicaron que utilizan IDS.

Se ha incrementado el uso de componentes de código abierto en aplicaciones. **14%**

**153%**

Se detectaron más de 10.000 nuevas amenazas diariamente en la plataforma Android, lo que alcanzó un incremento total interanual del 153%.

**80%**

Más del 80% de las aplicaciones de código abierto y comerciales sufren vulnerabilidades de funciones de seguridad con graves implicaciones para la gestión de datos privados.

Con el 95% de las muestras de malware de nuevo descubrimiento y el 42% de las vulnerabilidades de seguridad dirigidas a Windows, este Sistema Operativo siga siendo la plataforma predominante para los ataques.

Las aplicaciones móviles que sufren fugas de información de sistemas internos destacan la preocupación por el almacenamiento de datos críticos para el negocio en dispositivos fáciles de perder.

El 29% de todas las muestras de vulnerabilidades de seguridad detectadas en 2015 continuaron utilizando un vector de infección 2010 Stuxnet que se ha parcheado dos veces.


### El año de daños colaterales

El problema de seguridad de los datos ya no reside únicamente en la obtención de información de tarjetas de pago. Reside en la **obtención de información que puede cambiar la vida de una persona para siempre.**

### Las normativas excesivas desincentivan la investigación

Diversas normativas propuestas que rigen la ciberseguridad desincentivan la investigación legítima sobre seguridad. En lugar de esto, estas normativas deben proteger e incentivar la investigación para el beneficio de todos.

### Pasar de soluciones puntuales a soluciones de amplio impacto

El año 2015 supuso un cambio de los proveedores hacia el desarrollo de medidas defensivas que evitan todas las clases de ataques.

### Las presiones políticas intentan desvincular las iniciativas de privacidad y de seguridad

Muchos legisladores de EE.UU., Reino Unido y de otros países reivindicaron que la seguridad solo puede conseguirse si se reducen los derechos fundamentales de privacidad y de proceso debido.

### La industria no aprendió nada sobre los parches en 2015

La vulnerabilidad nº 1 más explotada en 2015 tiene más de cinco años de antigüedad, fue la más explotada en 2014 y ha sido parcheada por el proveedor... dos veces.

### Los atacantes han desviado sus esfuerzos para atacar directamente las aplicaciones

Ahora, las aplicaciones se ven como la ruta más sencilla por la que los atacantes pueden acceder a datos empresariales sensibles.

### La rentabilización del malware

El malware relacionado con ATM se ha convertido en el más habitual, ya que permite que los ciberdelincuentes consigan dinero con mayor rapidez.

Para disponer del informe completo, visite www.hpe.com/software/cyberrisk