Telefónica

TREND REPORT_

# Estado de la Ciberseguridad de las empresas españolas_

05.10.2017

CYBER SECURED BY ElevenPaths

elevenpaths.com

# Índice

# Resumen ejecutivo

El presente estudio tiene como objetivo reflejar el estado de ciberseguridad tanto de las empresas españolas a nivel general, como de las englobadas en el IBEX 35. La información ha sido proporcionada por la compañía BitSight, que calcula los *ratings* de seguridad de las empresas tomando como base información externa a las propias organizaciones. El conjunto de datos sobre el que se ha realizado el informe engloba alrededor de 1.000.000 de direcciones IPs atribuidas a un total de 850 organizaciones. Teniendo en cuenta este contexto, se puede afirmar que:

1. «El nivel de seguridad de las empresas españolas se sitúa por debajo de la media europea.»
2. «Las dos empresas del IBEX 35 con mejor *rating* pertenecen al sector Financiero y al de Energía / Recursos.»
3. «Más de un 85% de las empresas del IBEX 35 son vulnerables a POODLE, Logjam, DROWN y FREAK.»
4. «Las amenazas dirigidas al canal móvil se han abierto paso hasta la tercera posición en la clasificación de las infecciones más extendidas en las empresas españolas.»
5. «Solo 6 empresas del IBEX 35 no presentaron ningún compromiso en el último año.»

¿SABES CUÁL ES EL POSICIONAMIENTO DE TU ORGANIZACIÓN FRENTE A ESTOS RETOS?

Si quieres **conocer tu *rating* de seguridad** y compararte con el sector, ponte en contacto con securityrating@11paths.com para recibir tu informe.

# 1. Introducción

En los últimos años se ha vivido un desarrollo exponencial en el campo de las Tecnologías de la Información y la Comunicación (TIC). Como resultado, los ecosistemas se han vuelto más globales y las organizaciones requieren estar permanentemente interconectadas. Paralelamente, las infraestructuras TI se ven incrementadas en número y complejidad, los servicios se externalizan y los modelos de negocio dependen cada vez más de proveedores y *partners*.

Esta evolución conlleva **nuevos riesgos y un potencial impacto cada vez mayor** para las organizaciones, ya que, al mismo tiempo, los cibercriminales han evolucionado sus tácticas y objetivos. De este modo, todo tipo de organizaciones, independientemente de su tamaño y sector de actividad, se ven sometidas a una amplia variedad de ataques, cada vez más sofisticados.

Ha transcurrido mucho tiempo desde que en 1903 se tuviera conocimiento de la que es considerada como la primera fuga de información de la historia. Por aquel entonces, el Southern California Hospital for the Insane sufrió la desaparición de registros con información personal y médica de sus pacientes, supuestamente sustraídos por uno de los trabajadores [1].

En la actualidad, España ha sufrido recientemente los ataques globales de WannaCry [2] y Adylkuzz [3]. Aunque a nivel nacional no han trascendido otros ataques con la misma notoriedad, internacionalmente cada vez es más frecuente encontrar noticias de todo tipo de empresas e instituciones afectadas por ataques de diversa índole. Si bien la tipología de estos incidentes es muy variada, las **fugas de información** son, posiblemente, los **ataques con mayor impacto**. Ello se debe a que la sensibilidad de la información expuesta y el volumen de registros filtrados es cada vez mayor, **alcanzando ya un coste medio de $ 3,62 millones** [4] (que incluye los gastos tanto directos como indirectos en los que incurre una organización a consecuencia de una fuga de información).

Mientras las cifras relacionadas con la ciberdelincuencia van en aumento, la inversión en ciberseguridad no se queda atrás. Según las últimas predicciones de Gartner, el gasto en seguridad de la información a nivel mundial alcanzaría los $ 93 000 millones en 2018 [5]. En el caso de España, la inversión media en ciberseguridad ha pasado de $ 3.1 a $ 3,9 millones en los últimos cinco años [6].

## ¿Son seguras las empresas y organismos españoles? ¿Somos más o menos seguros que otros países de nuestro entorno? ¿Es suficiente el incremento medio en la inversión en seguridad? ¿Invertimos nuestros recursos en seguridad de forma eficiente?

En ElevenPaths **estamos convencidos de que el conocimiento macro de la seguridad** del país es un claro valor diferencial que nos permite, de manera anticipada, apoyar a nuestros clientes a afrontar los retos particulares a los que se enfrentan día a día.

Para ello hemos creado este informe, cuyo objetivo es proporcionar una visión ejecutiva del **estado de la ciberseguridad de las empresas españolas**.

Para dotar al informe de información más relevante se elaborará de forma periódica para poder analizar las tendencias e indicar a las organizaciones dónde deben poner el foco.

# 2. Metodología

El presente informe se ha realizado en colaboración con BitSight, analizando información proveniente de sus *ratings* de seguridad, un sistema desarrollado para medir el nivel general de seguridad de las organizaciones de todo el mundo. Estos *ratings*, actualizados a diario, califican a las organizaciones en una escala de 250 a 900, clasificándolas en tres categorías en función del *rating*: Básica, Intermedia o Avanzada.

Los *ratings* de seguridad se calculan usando un algoritmo propietario que se basa en la información de diversos vectores de riesgo distribuidos en las siguientes categorías:

- **Sistemas comprometidos:** Hace referencia a los compromisos en la red de la organización, típicamente causados por software malicioso.
- **Diligencia:** Medidas observables que una empresa ha tomado para prevenir ataques.
- **Comportamiento del empleado:** Busca actividad de intercambio de archivos de usuario que pueda introducir software malicioso en una organización, por ejemplo, mediante la descarga de un archivo comprometido.
- **Fugas de información:** Se refiere a incidentes divulgados públicamente de pérdida o robo de datos. Estos incluyen la pérdida de datos a través de ataques exitosos, negligencia de empleados y robo de hardware.

Es importante señalar que este *rating* es una **visión ejecutiva externa** del desempeño de seguridad de una organización, pero no representa todo lo que engloba la seguridad de una organización.

BitSight recopila y procesa grandes cantidades de datos para proporcionar los *ratings* de seguridad. La base de esta investigación se construye sobre la capacidad para identificar los eventos de seguridad y atribuirlos con precisión a las organizaciones, lo que a su vez permite la agregación entre industrias. Esta atribución se determina identificando los bloques CIDR (*Classless Inter-Domain Routing*), dominios y números AS (*Autonomous System*) pertenecientes a las organizaciones. El proceso para construir estos mapas de red ha demostrado una precisión superior al 95%, incluso para organizaciones con cientos de miles de direcciones IP.

En el análisis del IBEX 35, para aquellas empresas que son multinacionales, se ha tomado como referencia la información de su infraestructura global, dado que se entiende que cualquier incidente a nivel global tiene repercusión para toda la compañía.

# 3. Visión general

Según los datos aportados por BitSight, el nivel de ciberseguridad en las empresas españolas se sitúa **levemente por debajo de la media europea**. Liderando el *ranking* europeo encontramos a países como Alemania, Reino Unido o Francia (Grupo A), con un nivel de seguridad encuadrado en el rango intermedio. Portugal e Italia (Grupo B) son ejemplos de países cuyo nivel de seguridad se asemeja al de las empresas españolas.

Ampliando el alcance a nivel mundial, se puede observar que los países europeos lideran el *ranking* de seguridad obteniendo cierta ventaja con respecto a Estados Unidos de América, Australia y Japón (Grupo C). Por otro lado, Perú, Colombia o Brasil (Grupo D) mantendrían niveles de seguridad similares en América del Sur.

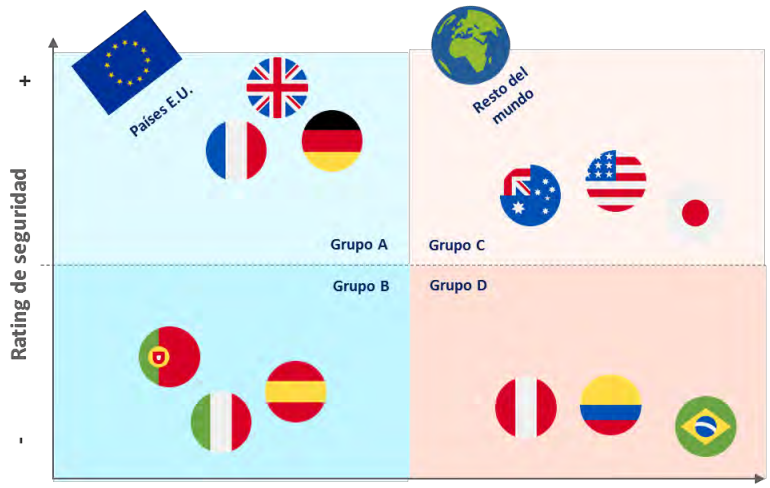


Figura 1 Comparación del *rating* de seguridad de las empresas españolas con el resto de países

Tras un análisis a nivel general de las empresas españolas, se observa que los **tipos de infección más extendidos** son las ***botnets*** (Conficker, AndroidBauts, Nivdort, ZeroAccess, y Necurs) y las **aplicaciones potencialmente no deseadas** (CrossRider, Sprotect, Grayware, y Genieo). El tipo «Spam Bot» representa una infección no identificada que resulta en el envío masivo de *spam*.

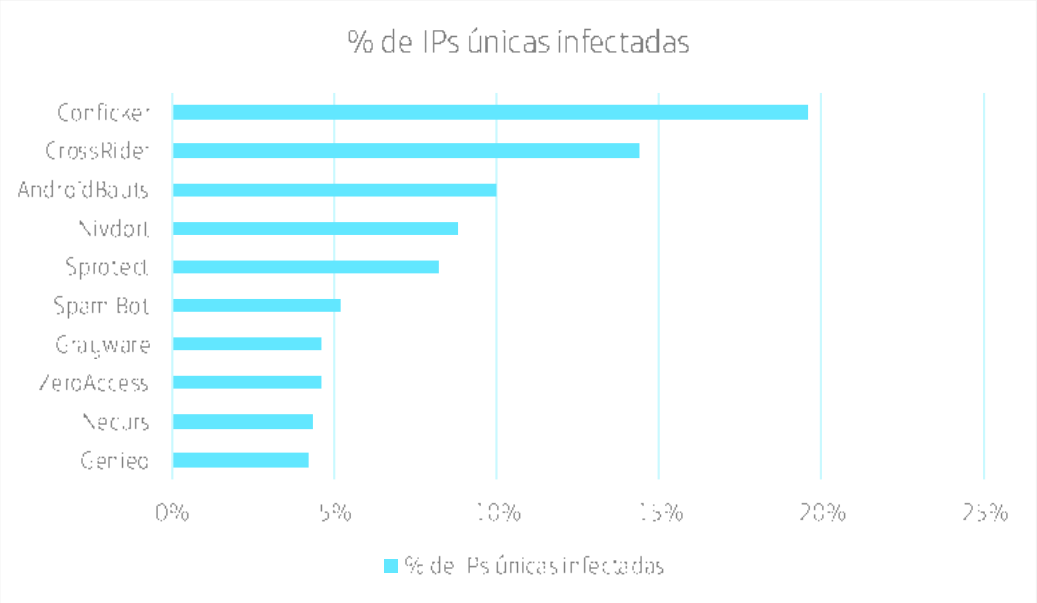


Figura 2. Top de infecciones en los últimos 30 días en las empresas españolas

En el caso de las vulnerabilidades, las registradas en los últimos 30 días están relacionadas con **configuraciones TLS/SSL deficientes** (Logjam, POODLE, DROWN, FREAK, Heartbleed, Ticketbleed) o con **configuraciones de servidor** (DOUBLEPULSAR, CVE-2017-0144, CVE-2017-7269), como ya sucedía el pasado año, de acuerdo al informe de Tendencias en vulnerabilidades del segundo semestre de 2016.

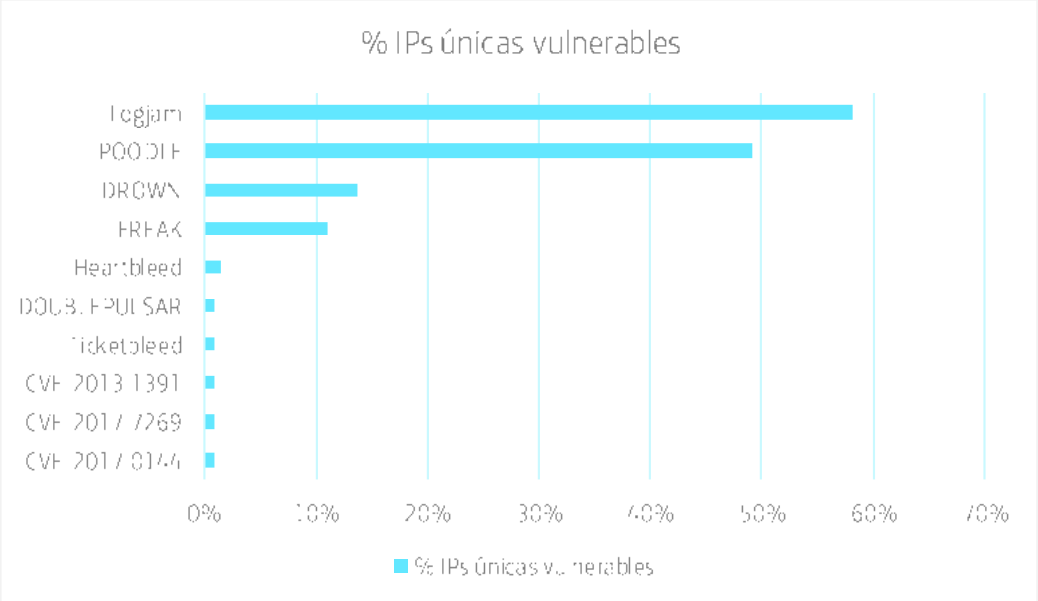


Figura 3. Top de vulnerabilidades en los últimos 30 días en las empresas españolas

Con respecto a los puertos abiertos, se identifican puertos con los servicios **SMTP sin STARTTLS, FTP sin STARTTLS** y **Telnet**, lo que sin duda supone un riesgo de seguridad.

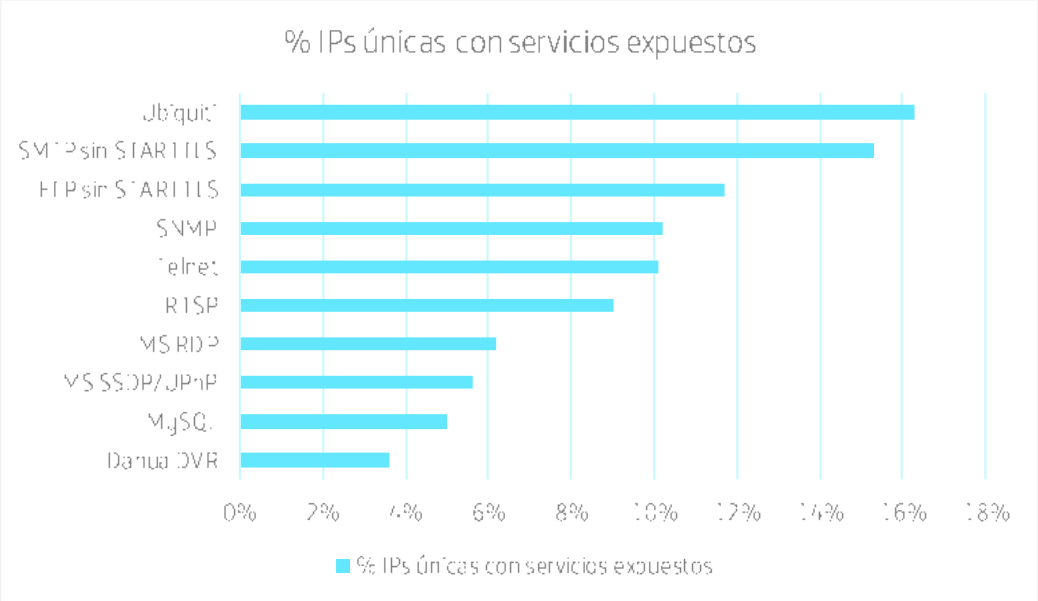


Figura 4. Top de puertos abiertos con servicios expuestos en los últimos 30 días en las empresas españolas

Hasta este punto, el informe ha proporcionado una visión global del riesgo en las empresas españolas. Para contextualizar más esta imagen, se ha decidido poner el foco en un conjunto de empresas que generen un volumen significativo de negocio y que sean críticas para la economía del país, e incluso para la cadena de suministro de otras organizaciones. Para ello se ha escogido el IBEX 35, el índice bursátil de referencia de la bolsa española.

Dado que el sector B2B de grandes empresas ocupa un lugar importante dentro de ElevenPaths, con esta elección se pretende presentar unas conclusiones que resulten lo más relevantes posibles para nuestros clientes.

Por todo ello, de ahora en adelante, el informe se centrará en analizar la postura de seguridad de las empresas del IBEX 35.

# 4. Sistemas comprometidos

La mayoría de los incidentes que se detectan en el IBEX 35 se corresponden con infecciones de equipos por medio de software malicioso, comúnmente conocido como *malware*.

Los riesgos derivados de las infecciones de *malware* pueden resultar en la **interrupción de la continuidad de negocio** y el aumento del riesgo de sufrir una **fuga de información**. De ahí la importancia de evaluar los sistemas comprometidos en las organizaciones. En este sentido, se observa que las infecciones más extendidas entre las empresas del IBEX 35 a lo largo del último año son:

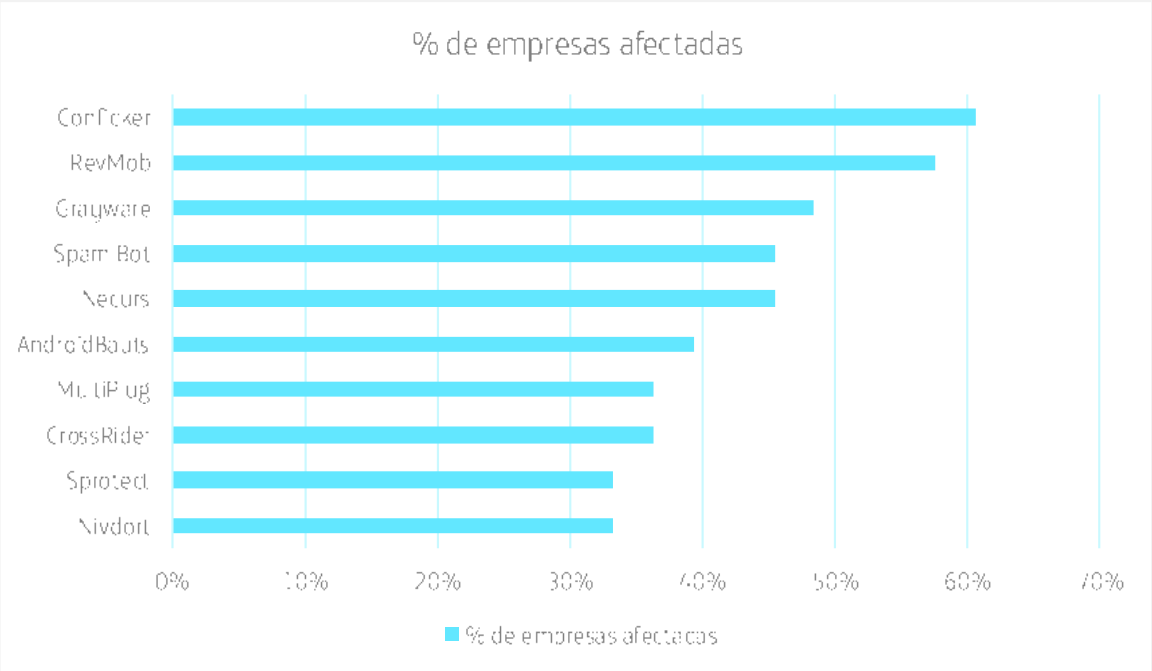


Figura 5. Top de infecciones en el IBEX 35 a lo largo del último año

A nivel individual, de entre todas estas infecciones destacan Conficker y AndroidBauts. Ambas, conocidas *botnets*, con distintos objetivos y métodos de infección.

En el caso de Conficker, se propaga a través de una vulnerabilidad en el servicio Server de Windows o de unidades USB infectadas, y su principal objetivo es robar información del dispositivo infectado y realizar campañas de envío de correos masivos. Resulta especialmente significativo que siga estando tan extendido a lo largo de tantos sectores, puesto que, en el año 2008, Microsoft liberó una actualización que soluciona la vulnerabilidad empleada para propagarse. Este dato evidencia que el **ritmo al que las empresas parchean las vulnerabilidades conocidas no siempre es el más conveniente** para evitar este tipo de situaciones.

Mientras que en el caso de AndroidBauts, la infección se produce a través de aplicaciones maliciosas instaladas desde mercados oficiales y no oficiales, y se dedica principalmente a mostrar anuncios, además de sustraer información del teléfono que permita la instalación de aplicaciones de terceros. La entrada en el top 10, así como la presencia en más de la mitad de los sectores, de este ***malware* especialmente dirigido a dispositivos móviles Android**, refleja la dimensión cada vez más importante que está adquiriendo el uso del canal móvil en las empresas y los riesgos que entraña.

Poniendo el foco en sectores, también pueden obtenerse datos significativos. Por ejemplo, se observa la presencia de Spam Bot, un tipo de infección no identificada que resulta en el envío masivo de *spam*, en un 68,7 % de los sectores. Este dato es importante dado que algunos de estos **sectores (Financiero, Energía / Recursos)** están orientados al cliente final y **podrían estar generando campañas de *phishing* en su contra** para sus propios clientes.

Si se analizan los sectores con más peso en el IBEX 35, en términos de número total de empresas, se obtiene que en el sector Financiero también hay otras infecciones con gran presencia: Necurs y Grayware, afectan a más de un 65 % de las organizaciones; y CrossRider y Conficker a la mitad del sector. Aunque también hay cabida para datos más positivos. En este sentido, la presencia de Zeus, una familia de *malware* que lleva repitiendo cerca de diez años como una de las mayores amenazas para el sector Financiero a nivel global, se reduce a una tercera parte de las organizaciones.

Por otro lado, en el sector Energía / Recursos, la mitad de las empresas se ven afectadas por RevMob y Conficker. Mientras en el caso del sector *Utilities*, Grayware afecta al 50% de las empresas.

En general, como se puede ver, **los tipos de infección más extendidos son las *botnets*** (Conficker, Necurs, AndroidBauts y Nivdort) **y las aplicaciones potencialmente no deseadas** (RevMob, Grayware, MultiPlug, CrossRider y Sprotect).

En el caso de las *botnets*, los dispositivos infectados pueden estar participando como *bots* o como servidores Command & Control (C&C) de una enorme red de equipos infectados que se dedican a realizar DDoS, enviar *spam*, distribuir *malware* o minar criptodivisas.

Por otra parte, las aplicaciones potencialmente no deseadas suelen ser *adware* o *spyware* que instalan software adicional no deseado, modifican la página de inicio de los navegadores o el proveedor de búsqueda, inyectan publicidad o realizan otras acciones sin consentimiento del usuario.

# 5. Vulnerabilidades

El problema anteriormente mencionado de las vulnerabilidades conocidas y no parcheadas es común a todos los sectores. Sin embargo, no es el único problema al que se enfrentan las organizaciones hoy en día.

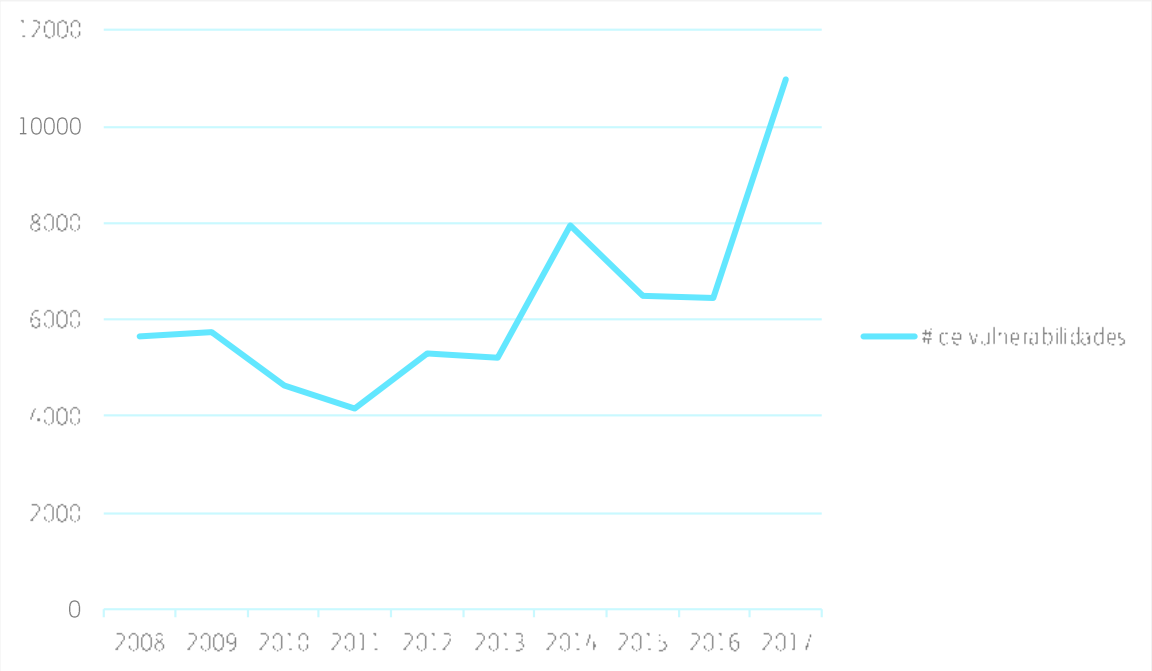


Figura 6 Evolución del número de vulnerabilidades publicadas en los últimos diez años

Analizando la evolución del número de vulnerabilidades de los diez últimos años [7], resulta especialmente significativo el aumento en lo que va de año con respecto al año pasado. De continuar la tendencia, **se podría duplicar el número de vulnerabilidades antes de finalizar el año.**

De todas estas vulnerabilidades, las más representativas en el IBEX 35 son las que se recogen en la Figura 7:

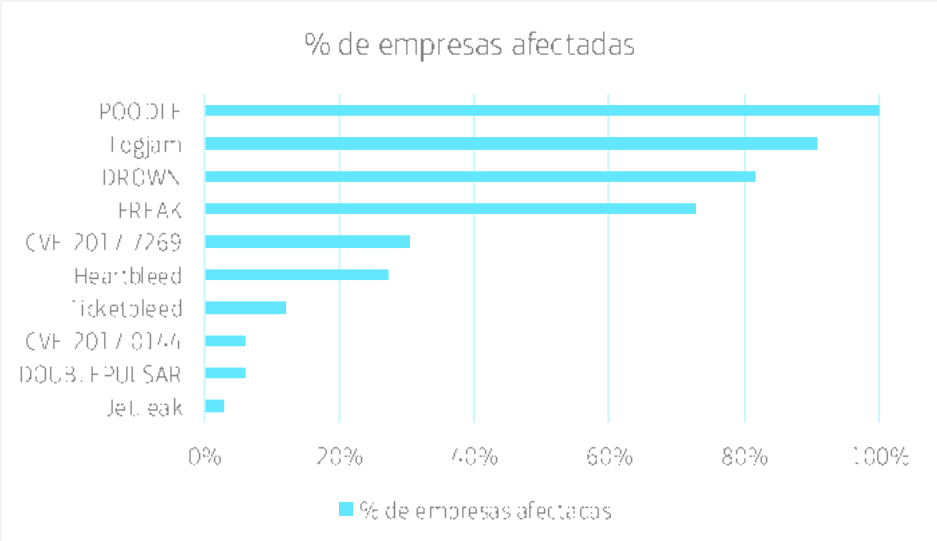


Figura 7. Top de vulnerabilidades en el IBEX 35 a lo largo del último año

**Más de un 85% de las empresas** del IBEX 35 **se ven afectadas por** las 4 vulnerabilidades más extendidas (**POODLE, Logjam, DROWN y FREAK**). Estas vulnerabilidades de tipo criptográfico permiten obtener datos sin cifrar por medio de ataques de intermediario o Man-in-the-Middle (MitM, por sus siglas en inglés), y descifrar datos cifrados que se transmiten por TLS.

También resulta interesante ver cómo **DOUBLEPULSAR**, que fue utilizado como puerta trasera para instalar el *ransomware* WannaCry, **se mantiene presente en dos empresas del** IBEX 35 a pesar de que Microsoft publicó hace meses un parche de seguridad para corregir la vulnerabilidad.

Sin embargo, el dato más significativo que se obtiene tras analizar cada una de las **vulnerabilidades** que componen este top 10 es que el **70% son públicas** desde hace más de un año, llegando incluso a alcanzar los tres años de antigüedad en algún caso. Este hecho pone de manifiesto la **falta de políticas de parcheo actualizadas**.

Además, la severidad de estas vulnerabilidades, de acuerdo al estándar Common Vulnerability Scoring System (CVSS) en su versión 3.0, es Alta o Crítica en al menos la mitad de los casos. Y existen *exploits* públicos para un 60% de ellas.

# 6. Puertos abiertos

Si bien hay determinados puertos que deben estar abiertos para dar soporte a funciones de negocio, otros, en los que hay corriendo servicios innecesarios y vulnerables expuestos a Internet, resultan un perfecto vector de entrada para los cibercriminales.

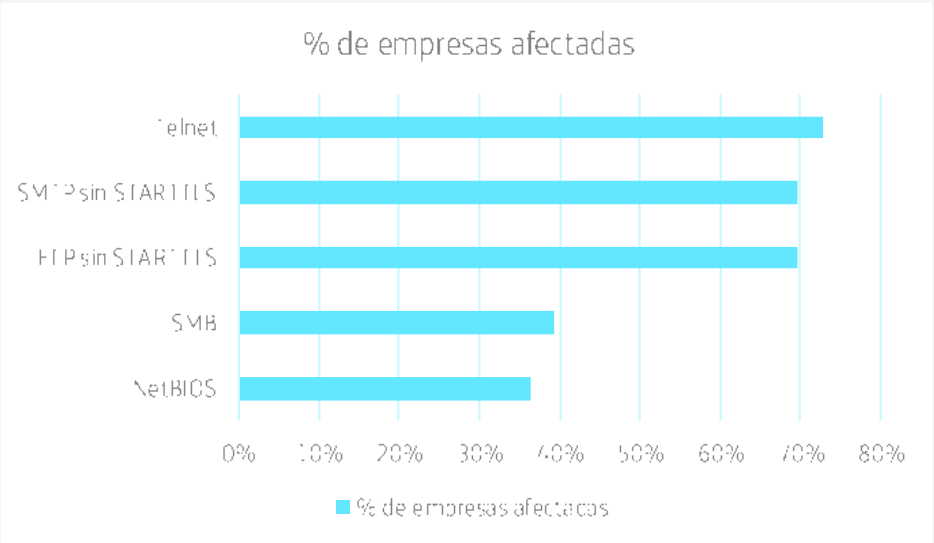


Figura 8. Top de puertos abiertos con servicios expuestos más críticos en el IBEX 35 a lo largo del último año

De entre estos 5 servicios que se han seleccionado por ser los más críticos de entre todos los observados, Telnet merece una mención aparte. Su presencia en casi tres cuartas partes del IBEX 35, a lo largo de más de un 80 % de los sectores, resulta preocupante. Se trata de un protocolo de comunicación que no cifra el tráfico y que tiene conocidas vulnerabilidades que debería ser sustituido, en la medida de lo posible, por SSH.

Se han hallado otros protocolos de comunicación bastante comunes (SMTP y FTP) corriendo sin cifrado en un gran número de sectores (13 y 14, respectivamente), resultando un perfecto vector de entrada para *malware*, además de los riesgos propios de la falta de cifrado.

SMB, famoso por ser utilizado por DOUBLEPULSAR, es un protocolo que, inapropiadamente configurado, permite acceder a carpetas compartidas, y que ha sido encontrado en casi un 40 % de las empresas.

Por último, llama la atención que NetBIOS siga utilizándose en 12 empresas de más de la mitad de los sectores del IBEX 35. Es cierto que determinadas aplicaciones *legacy* siguen dependiendo de su uso, pero tiene vulnerabilidades conocidas y es objeto de muchos ataques.

Por otro lado, también cabe destacar que **populares servidores de bases de datos**, como MySQL (muy extendido en todos los sectores, estando presente en 15 empresas) sigan **expuestos al exterior debido a configuraciones erróneas.**

# 7. Recomendaciones

A pesar de que en la actualidad la mayoría de las organizaciones disponen de numerosas soluciones de seguridad, muchas presentan infecciones o vulnerabilidades y servicios expuestos, por lo que podrían resultar víctimas de avanzados ciberataques. Es por ello que se hace necesario realizar una serie de recomendaciones a tener en cuenta para evitar estos incidentes o mitigar su impacto, en caso de ocurrir.

En primer lugar es importante incidir en que las organizaciones necesitan afianzar los aspectos básicos de seguridad con objeto de crecer sobre una base sólida y protegerse contra amenazas más avanzadas. Alinear la seguridad de la información como parte del modelo de gestión del riesgo corporativo, definir y actualizar los procedimientos de seguridad, actualizar el inventario de activos o establecer mecanismos de comunicación eficaces con los equipos de IT, siguen siendo los pilares en los cuales se debe asentar la política corporativa de seguridad de la información de las grandes compañías. Simplificando: «**La seguridad debe estar en el ADN de la compañía**».

Con respecto a las vulnerabilidades y puertos abiertos, se hace necesario que la **gestión de vulnerabilidades** evolucione más allá de ser un simple ejercicio programado que se ejecuta unas pocas veces al año, pasando a ser un **proceso continuo que identifique de forma proactiva los problemas**. Proporcionar una imagen actualizada del inventario de activos, analizar de forma continua las vulnerabilidades que afectan a los activos IT y disponer de herramientas que permitan centralizar el ciclo de vida de las vulnerabilidades, se han convertido en elementos base para realizar una gestión holística y eficiente de las vulnerabilidades que afectan a una organización. Por otro lado, es necesario concienciar a los órganos de gestión de la compañía del impacto en el negocio que supondría un error de seguridad, facilitando la creación de mecanismos eficientes de comunicación entre las figuras de CISO y CIO, que permitan resolver y gestionar las vulnerabilidades de forma rápida.

En el ámbito de los sistemas comprometidos, se observa **que la mayoría de infecciones podría prevenirse**, o resolverse, por medio del establecimiento de medidas de **políticas IT básicas**. Sin embargo, hay que tener en cuenta que este informe se ha basado en datos de eventos detectados, pero hay otros incidentes que pasan desapercibidos para las defensas convencionales de muchas organizaciones. Para estar preparados **ante ataques más sofisticados**, se recomienda a las organizaciones la instalación de **herramientas de detección y respuesta de *malware*** (EDR) que les permitan, tanto incluir capacidades de detección de *malware* de nueva generación e integrar **IoCs externos de alto valor**, como facilitar la respuesta ante incidentes, dotando a los equipos de los CSIRT corporativos de información de contexto de las amenazas que les han afectado.

Relacionado con el canal móvil, los datos recogidos en el informe advierten del **incremento de familias de *malware*** específicamente **dirigidas a dispositivos móviles** (AndroidBauts, por ejemplo). Por otro lado, fuentes propias de ElevenPaths indican que, de las más de ocho millones de aplicaciones recopiladas en los mercados, más de cinco millones contienen vulnerabilidades, siendo en más de un millón de los casos vulnerabilidades críticas. Ante esta realidad se abren dos vías de recomendación: por un lado, el refuerzo de todas las políticas de seguridad en torno al uso de los dispositivos móviles en entornos corporativos, para **proteger el acceso a la información corporativa sensible**. Por otro lado, el uso de soluciones que permitan la **identificación de fallos de seguridad en aplicaciones propias**, así como la detección de aplicaciones de terceros que puedan poner en riesgo a las organizaciones o a sus clientes.

# 8. Bibliografía

[1] ««Oldest Data Loss Incident – Contest Winners», DataLossDB. 31-may-2009. [En línea]. Disponible en: https://blog.datalossdb.org/2009/05/31/oldest-data-loss-incident-contest-winners/. [Accedido: 19-sep-2017].».

[2] «F. Palazuelos, «How the WannaCry ransomware attack affected businesses in Spain». EL PAÍS. 19-may-2017. [En línea]. Disponible en: https://elpais.com/elpais/2017/05/19/inenglish/1495181037_355348.html. [Accedido. 19-sep-2017].».

[3] «Alexander Chiu, «Cisco Coverage for AdylKuzz, Uiwix, and EternalRocks» Talos Intelligence Blog, 22-may-2017. [En línea]. Disponible en: http://blog.talosintelligence.com/2017/05/adylkuzz-uiwix-eternalrocks.html. [Accedido. 19-sep-2017].».

[4] ««Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview». 19-jun-2017. [En línea]. Disponible en: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&. [Accedido: 19-sep-2017].».

[5] ««Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017». [En línea]. Disponible en: //www.gartner.com/newsroom/id/3784965. [Accedido. 19-sep-2017].».

[6] ««Encuesta Mundial sobre ciberseguridad 2017». PwC. [En línea]. Disponible en: https://www.pwc.es/es/digital/encuesta-mundial-estado-seguridad-informacion-2017.html. [Accedido. 19-sep-2017].».

[7] ««Browse cve vulnerabilities by date». [En línea]. Disponible en: https://www.cvedetails.com/browse-by-date.php. [Accedido. 19-sep-2017].».

## Acerca de ElevenPaths

En ElevenPaths, la unidad de Ciberseguridad de Telefónica, creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre la seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y de esta manera, ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

## Más información

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com

## Acerca de BitSight

BitSight está transformando la forma en que las empresas gestionan los riesgos de seguridad de la información con *ratings* de seguridad objetivos, verificables y accionables. Fundada en 2011, la compañía desarrolló su Security Rating Platform para analizar de forma continua grandes cantidades de datos externos sobre cuestiones y comportamientos de seguridad con el fin de ayudar a las organizaciones a gestionar el riesgo de terceros, suscribir pólizas de ciberseguros, comparar el rendimiento con competidores y otros grupos de interés, llevar a cabo la *due diligence* de fusiones y adquisiciones y evaluar el riesgo agregado. Siete de las 10 principales ciberaseguradoras, 60 compañías de la lista Fortune 500 y 3 de los 5 principales bancos de inversión confían en BitSight para gestionar su ciber riesgo.

## Más información

www.bitsighttech.com
@BitSight
blog.bitsighttech.com