Nuevos retos y tendencias en ciberseguridad para 2019

En Penteo hemos analizado los nuevos retos a los que se enfrentan las organizaciones en materia de ciberseguridad. En base a nuestras investigaciones realizadas podemos identificar tendencias que se están dando en esta práctica, como, por ejemplo:

- Que el conocimiento que muestran los directivos de TI resulta considerable en ámbitos que llevan más tiempo presentes en la ciberseguridad (seguridad de contenidos, control de accesos), pero resulta aún algo limitado en ámbitos como el de las brechas de seguridad causadas por fuga de información y su mitigación mediante sistemas DLP.

- Los comités de dirección priman por encima de otros aspectos el cumplimiento con las regulaciones que impactan dentro del sector.

- El compromiso de la dirección y el creciente peso del CISO son considerados factores de éxitos clave para que la ciberseguridad tenga mayor recorrido dentro de las organizaciones.

- Las organizaciones españolas ignoran en gran medida el peligro de los nuevos ciberataques que se están originando en los últimos tiempos, sobre todo los que pueden afectar a dispositivos IoT o los que hacen uso de tecnologías emergentes como la IA, creyendo no ser casi vulnerables a este tipo de ataques.

Alejandro Arias,
Analista de Penteo

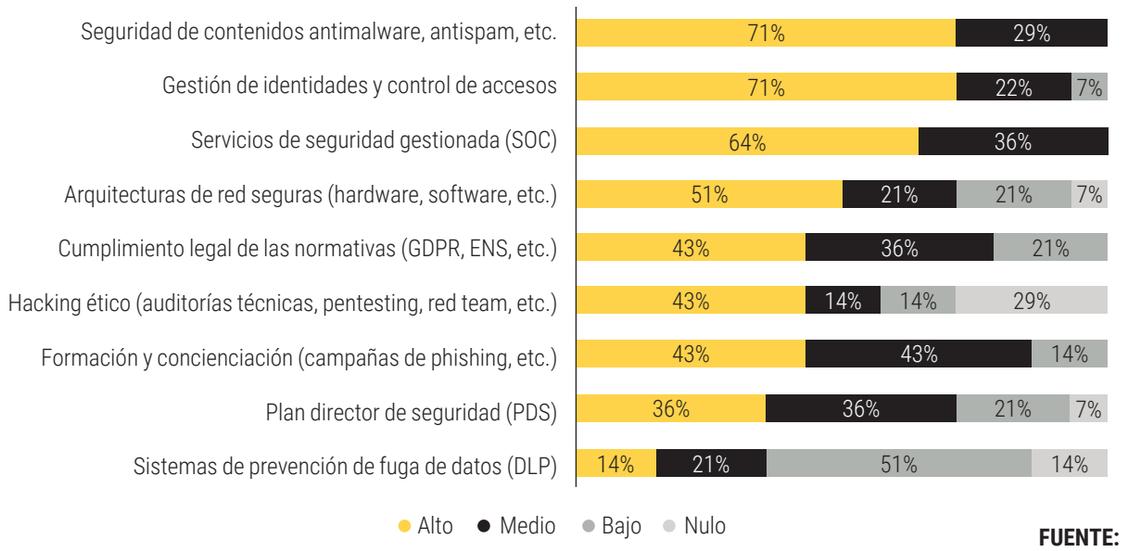
Principales ciberataques: malware, phishing, denegación de servicio

A lo largo del año pasado, una palabra ha predominado por encima de otras muchas en cuanto a ciberataques hacia las organizaciones: ransomware, programas maliciosos de secuestro de información y posterior cifrado que solicitaba un rescate económico a cambio, y que no han dejado de propagarse por los sistemas informáticos de multitud de organizaciones a nivel mundial.

La falta de concienciación y formación de los empleados provoca que ciertos ataques de phishing continúen materializándose. También ataques distribuidos de denegación de servicio (DDoS) materializados ya no únicamente por ciberdelincuentes, sino por redes de botnets que consiguen saturar una página web.

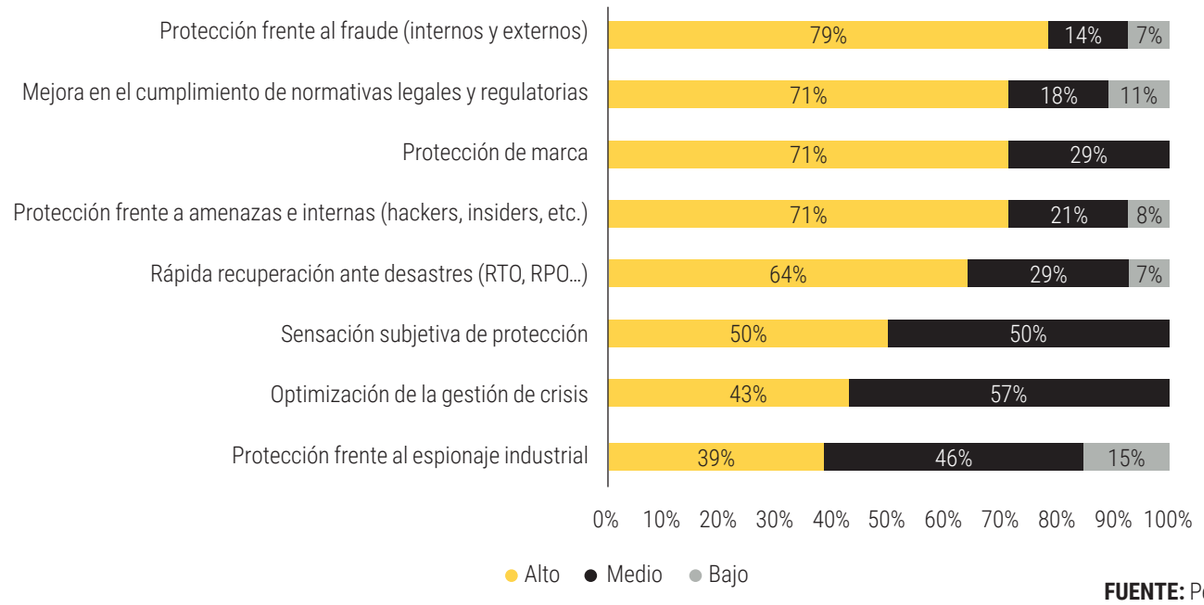
Además, los fabricantes de soluciones de ciberseguridad han dejado de centrarse únicamente en la seguridad perimetral y de contenidos (control de accesos mediante soluciones IAM y tecnología NAC, antivirus, antispam, etc.) y de infraestructura de red (cortafuegos, VPN seguras, filtrado web…). Cada vez se le da más importancia también a servicios de vigilancia a través de

Nivel de implantación de soluciones y servicios



FUENTE: Penteo

¿Qué beneficios esperan obtener las compañías?



FUENTE: Penteo

herramientas SIEM o de hacking ético (escaneo de vulnerabilidades, pentesting, etc.) e incluso herramientas GRC de gobierno y cumplimiento de las normas que aplican dentro del sector.

La privacidad de los datos, en el punto de mira

Una de las obligaciones que se les presenta a las empresas este año es el cumplimiento con el nuevo Reglamento de Protección de Datos (GDPR) a partir de mayo. Hasta ahora la privacidad y seguridad de los datos se habían mantenido

> *El beneficio que esperan obtener la mayoría de las organizaciones es la protección frente al fraude, interno y externo*

como áreas separadas dentro de la ciberseguridad, pero todo ello cambiará, especialmente en el sector en el que operan las pymes.

Un aspecto importante de la evolución de las soluciones de seguridad de privacidad de los datos es que se ha ido pasando de centrar los esfuerzos y la tecnología de protección en dispositivos, infraestructuras y aplicaciones, a enfocarla en la información como activo estratégico; por ejemplo, en la implantación de soluciones DLP para evitar el filtrado de datos, o en soluciones de cifrado de la información.

40%

de las organizaciones piensan que están bien protegidas frente a posibles ataques

Nivel de implantación de soluciones y servicios

En las investigaciones realizadas por Penteo, la protección ante ataques de código malicioso mediante soluciones de antivirus, antispam, etc., siempre ha tenido una alta presencia en la mayoría de las empresas desde que se producían los primeros ciberataques. Tres de cada cuatro organizaciones tienen un grado de implantación de este tipo de soluciones bastante alto.

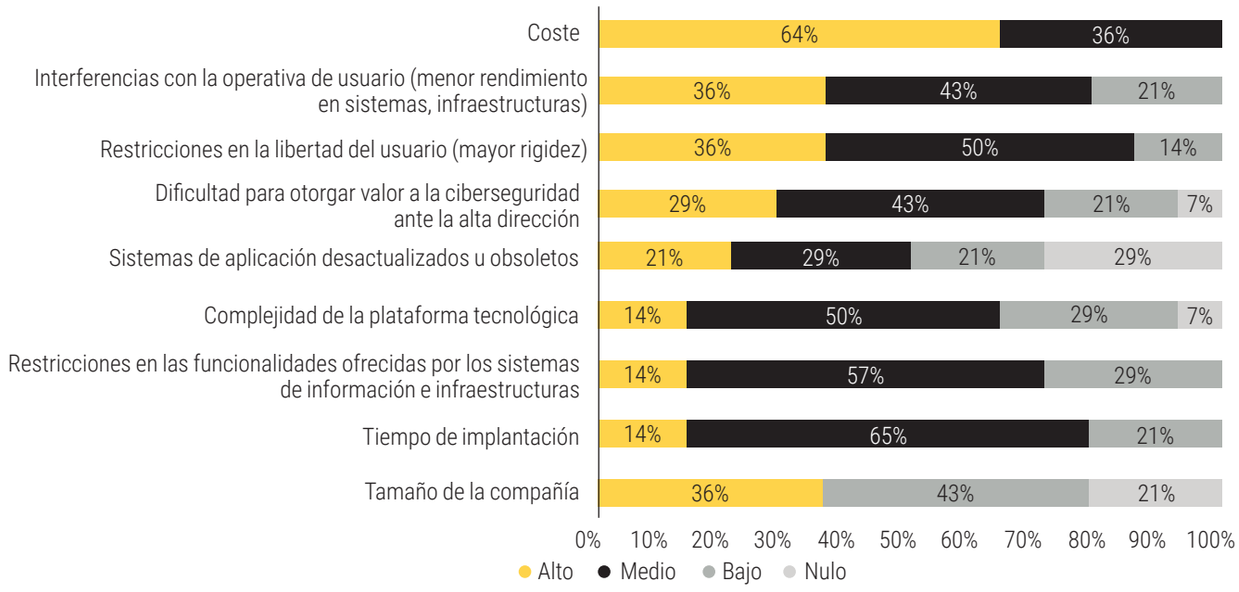
Además, muchas organizaciones consideran importante la adecuada gestión del control de accesos mediante soluciones tecnológicas innovadoras relativas a NAC (Network Access Control) e IAM (Identity and Access Management).

La implantación de herramientas para la prevención de la fuga de información (DLP) sigue siendo puntual, sobre todo centrada en el endpoint, y restringida, en la mayoría de los casos, a puestos de trabajo y medios de almacenamiento en los que el nivel de criticidad de la información contenida se considera alta.

Beneficios como la protección y cumplimiento normativo, los más esperados

El beneficio que esperan obtener la mayoría de las organizaciones es la protección frente al fraude tanto interno como externo. El posible descontento de algunos empleados puede ocasionar que los mismos originen ataques contra la propia empresa o incluso filtren información confidencial muy útil para organizaciones que se dedican al cibercrimen o, incluso, de la competencia, y así puedan dar origen a ataques que pongan en ries-

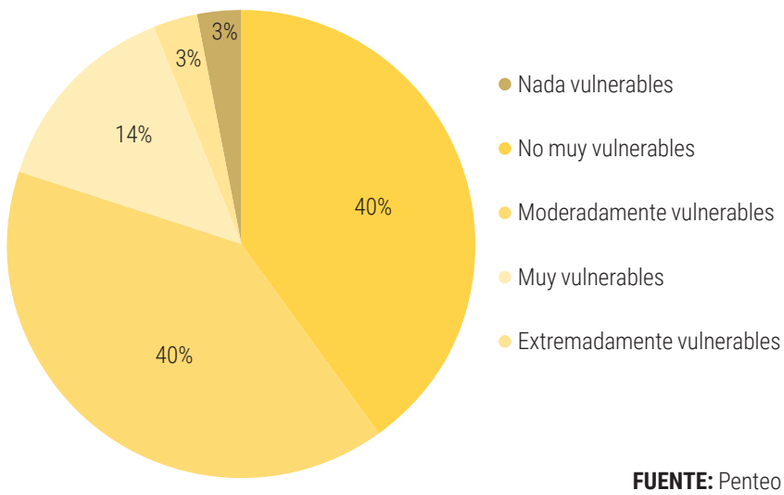
Principales barreras para la adopción de soluciones de seguridad



FUENTE: Penteo

Para invertir más, hay que hacer entender a la alta dirección la existencia de amenazas sobre los activos críticos

Percepción de vulnerabilidad que tienen los CIO



FUENTE: Penteo

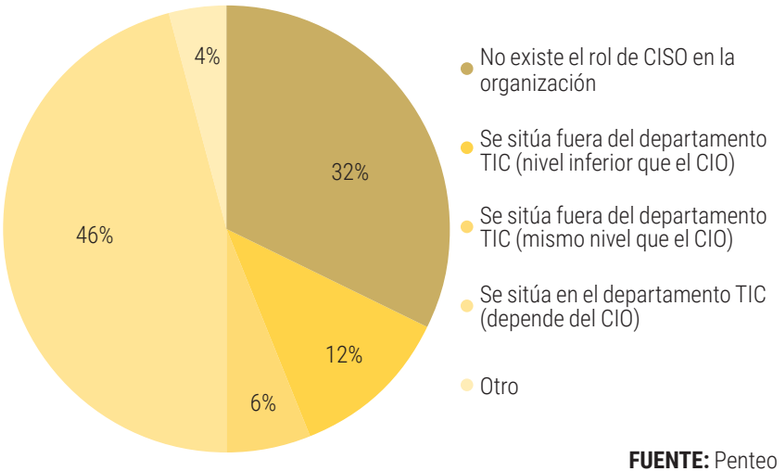
go la imagen de marca de la compañía. La mejora en el cumplimiento de las normativas del sector es otro de los beneficios esperados, ya que las sanciones en caso de incumplimiento de alguna de las regulaciones pueden suponer una pérdida económica considerable para la compañía.

Coste e indisponibilidad temporal de los equipos, principales barreras

En la investigación realizada, se han identificado las principales barreras en la adopción de soluciones de ciberseguridad, como son los costes que supone la implantación de este tipo de soluciones. La dificultad de hacer entender a la alta dirección las consecuencias de que a corto plazo se materialicen amenazas sobre los activos críticos de información, y la necesidad de mantener permanentemente actualizados los controles y medidas de seguridad, son dos de las causas que dificultan la inversión en soluciones de ciberseguridad.

Otra de las barreras que aparecen en este apartado son las interferencias con la operativa de usuario y las restricciones en la libertad de este, ya que supone tomar algunos riesgos en cuanto al rendimiento de los sistemas e infraestructuras implicadas en la implantación de soluciones de ciberseguridad.

Nivel de presencia del CISO dentro de la empresa



FUENTE: Penteo

La mayor vulnerabilidad que presentan las empresas y CIO en materia de ciberseguridad es el desconocimiento absoluto que hay acerca del peligro. Protegerse de los ciberataques es responsabilidad tanto de las empresas como del empleado, pero debe estar respaldado por un marco regulatorio que proteja aún más las operaciones que se llevan a cabo dentro de una compañía. En Penteo hemos analizado el grado de vulnerabilidad al que las propias compañías creen que están expuestas. La mayoría no cree que sean vulnerables a ciberataques sobre sus activos de información críticos. Dos de cada cinco encuestados afirman estar bien protegidos ante posibles ataques.

El peso de la figura del CISO, reto a abordar

Existe el consenso de que el CISO no puede desempeñar correctamente sus funciones si no se sitúa en un lugar de la organización con capacidad para supervisar todos los procesos tecnológicos (producción de sistemas, controles de cambios, desarrollo de aplicaciones, planes de continuidad…), o bien no es dotado por parte de la Dirección con una suficiente autoridad normativa y de control. Todo ello sitúa teóricamente al CISO en una posición, como mínimo, de staff dependiendo directamente del CIO, o bien fuera del propio DTIC (para extender su capacidad normativa a todas las UUNN, cada vez más protagonistas en la adquisición de tecnología).

Si continuamos analizando la situación organizativa, podemos observar que un porcentaje considerable (18%) sitúa al CISO fuera del departamento de Tecnología, ya sea al mismo nivel o a un nivel inferior que el CIO. En el resto de los casos, una de las situaciones que más se da es que el CIO y el CISO son la misma persona dentro de la compañía. A pesar de estos datos, podemos concluir que el CISO está ganando cada vez más peso dentro de las compañías.

La ciberseguridad cada vez más prioritaria en la estrategia

La ciberseguridad ha ido adquiriendo cada vez mayor peso en las empresas en comparación con otras prácticas del área de TI, sobre todo a la hora de tomar decisiones que pueden afectar a la estrategia corporativa de la compañía y de acuerdo a las nuevas tendencias que se están consolidando en el mercado como la especialización del cibercrimen (CaaS o CyberCrime-as-a-Service). Muchas empresas están cada vez más concienciadas respecto a cambios que se están dando en el sector y todo esto está dando como resultado mayores inversiones destinadas a proteger y salvaguardar los activos propios de la compañía.

Sin embargo, la percepción del peligro que conlleva la aparición de nuevas amenazas en el mundo de la ciberseguridad es aún mejorable. Entretanto, el riesgo de exposición a los nuevos vectores de ataque que emergen y surgen cada día sigue siendo inherente a cualquier medida de ciberseguridad adoptada por las organizaciones.

La seguridad en dispositivos IoT es uno de los futuros retos a abordar por parte de las organizaciones, debido al desconocimiento tanto de fabricantes y proveedores acerca de las vulnerabilidades y errores que pueden tener este tipo de dispositivos por defecto, y que los cibercriminales se encargan de explotar. Herramientas de big data o machine learning a la hora de establecer modelos predictivos pueden ayudar en la prevención de la materialización de futuros ciberataques.

Además, adquiere cada vez mayor importancia la seguridad en cloud, ya que es tendencia que muchas organizaciones migren su información a este tipo de tecnología, y por tanto es imprescindible que los proveedores tengan aseguradas sus herramientas, plataformas e infraestructuras para cumplir con las medidas de seguridad que establece el sector y no incurrir en posibles sanciones e incumplimientos de contratos con los clientes. ■

> *Big data o machine learning pueden ayudar a crear modelos predictivos frente a los ciberataques*

18%

de los encuestados por Penteo sitúa al CISO fuera del departamento de Tecnología