FORO it Digital Security

# NUEVOS MODELOS DE CIBERSEGURIDAD PARA PROTEGER A LA EMPRESA GLOBAL


©freepik

PATROCINADORES GOLD

BFY TU BIOMETRÍA SOLO CONTIGO

Crayon

eset Digital Security Progress. Protected.

SAMSUNG

SONICWALL

SOPHOS

TREND MICRO

PATROCINADOR SILVER

kaspersky

# NUEVOS MODELOS DE CIBERSEGURIDAD

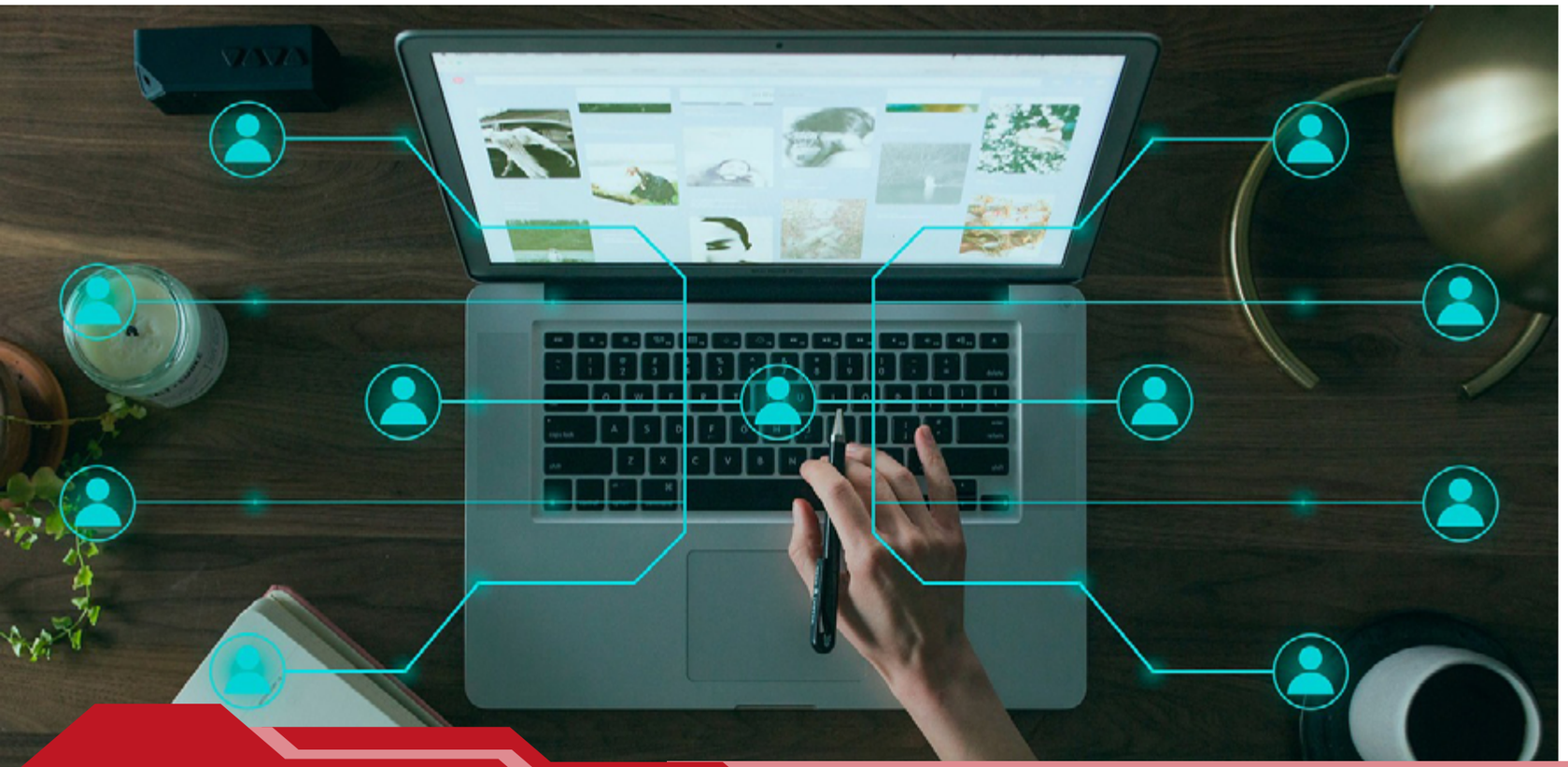
## PARA PROTEGER A LA EMPRESA GLOBAL

Bajo el lema “Nuevos modelos de seguridad para proteger a la empresa global” el pasado 24 de octubre celebramos la V edición del **#ForoITDS** en la que analizamos los desafíos a los que se enfrentan las empresas y cómo mejorar su protección. Y es que, cada vez son más las empresas atacadas y los puntos que proteger. Proteger una empresa es cada día un reto mayor. Así lo estamos viendo en los últimos años en los que tanto las amenazas como los vectores a tener en cuenta se han multiplicado exponencialmente. ¿Qué aspectos se han de tener en cuenta para mejorar la protección en un momento como el que estamos viviendo?

Esta fue una de las grandes cuestiones que abordamos de la mano de los participantes en esta quinta edición del Foro IT Digital Security en la que quedó claro que el principal desafío en este momento es adelantarse a un posible ataque. La visibilidad y el control han tomado protagonismo y lo han hecho porque prevenir se ha convertido en una obligación.

En este contexto, no es de extrañar que la seguridad esté evolucionando y que surjan nuevos modelos que buscan dar seguridad a la empresa y su ecosistema desde todos los elementos que componen la infraestructura corporativa. El uso de la tecnología supone un nuevo paradigma digital, donde la ubicación del usuario, el dispositivo desde el que se conecte o la idiosincrasia de la infraestructura a la que acceda pasa a un segundo plano. En este nuevo escenario ha de primar la planificación, la prevención, la proactividad y la gestión de medidas de ciberseguridad de forma global e inteligente, permitiendo al negocio avanzar y asegurar la continuidad pase lo que pase.

Así, para proteger la empresa global de forma eficiente actualmente no se ha de tener en cuenta únicamente la necesidad de proteger la red, el perímetro o los dispositivos, se tiene que abordar la seguridad desde un enfoque proactivo que incluya todos los elementos que componen el entorno de trabajo y eso implica a aplicaciones críticas para el negocio, infraestructura de mensajería y colaboración, servicios en la nube, comercio electrónico y aplicaciones de fabricación, plantas de producción... y un largo etcétera que llega hasta los empleados y la necesidad inminente de que se conviertan en aliados de la seguridad y no un vector de ataque más.



En 2023 se ha visto cómo la digitalización acelerada de los últimos años ha provocado un nivel de exposición sin precedentes en las empresas. Y esto, unido al incremento del número y la sofisticación de los ataques, ha derivado en que la ciberseguridad haya ascendido a la categoría de elemento crítico pues el volumen y la variedad de amenazas cibernéticas mantienen, desde hace meses, en alerta a las empresas y a los equipos de ciberseguridad que, a pesar de la desaceleración, la falta de presupuesto y de personal adecuadamente formado, reman contracorriente para desarrollar una estrategia de ciberseguridad sostenible y duradera que permita a las empresas estar a salvo de los, cada vez más numerosos, ataques de los cibercriminales.

Pero ¿cómo equilibrar la necesidad de protección con una buena experiencia de usuario y productividad? Este equilibrio es, sin duda, el mayor reto al que se ha enfrentado el tejido empresarial español en mu-

cho tiempo. Y precisamente este desafío fue el eje central de la V edición del Foro IT Digital Security celebrado el pasado 24 de octubre en el que quisimos conocer los mejores modelos, estrategias y prácticas para alcanzar la ciberseguridad global.

## CAMINOS PARA MEJORAR LA SEGURIDAD

La naturaleza cambiante de las amenazas a lo largo de los años hace que medidas de seguridad tradicionales como cortafuegos o el antivirus cada vez sean menos eficaces debido al creciente número de brechas y malware. ¿Qué hacer entonces para adaptarse al entorno actual que, lejos de mejorar, parece ir a peor? Muchos apuntan a que la solución está en la tecnología: IA y Machine Learning podrían se postulan como remedio a los problemas de escasez de talento y fatiga que arrastra el sector. Sin embargo, esta tecnología es, en parte, la culpable de la proliferación de ataques que acusamos. Entonces, ¿hacia dónde mirar? Para muchos CISO la clave no está en la tecnología sino más bien en la estrategia, en cambiar de enfoque y favorecer un modelo holístico y global que vaya de arriba hacia abajo y de abajo hacia arriba, que implique a toda la compañía y que haga entender a todo el tejido empresarial su papel en la mejora de la postura de ciberseguridad.

**EN 2023 SE HA VISTO CÓMO LA DIGITALIZACIÓN ACELERADA DE LOS ÚLTIMOS AÑOS HA PROVOCADO UN NIVEL DE EXPOSICIÓN SIN PRECEDENTES EN LAS EMPRESAS**

Entre sus muchas funciones, los CISO tienen la difícil tarea de diseñar los planes de ciberseguridad de su empresa. Elegir entre diversas soluciones, entre multitud de posturas... esta tarea es, sin duda, una de las más básicas, pero también una de las más complejas de la vida de un CISO. Y es que, aunque muchos de los ataques que vemos día a día pueden ser detectados por la tecnología y soluciones avanzadas, lo cierto es que muchos de ellos siguen pasando desapercibidos o son difíciles de detectar. Por ello, conocerse bien sigue siendo la base para consolidar la seguridad pero hacerlo de forma eficiente no es algo fácil en un momento en el que la infraestructura empresarial se complejiza a medida que la compañía crece. Sin embargo esta tarea de autoconocimiento y prevención es, sin duda, vital.

Una vez que tengamos claro el status quo, toca implementar soluciones capaces se asegurar la continuidad de negocio en caso de ciberataque. Aquí es donde entran en juego las diferentes tecnologías de protección, detección y securización y los diferentes modelos y estrategias a seguir.

Si quieres conocer qué modelos están adoptando las empresas para mejorar su seguridad y cómo implementar una estrategia de seguridad global con la que protegerse a día de hoy, no te pierdas el siguiente especial en el que analizamos todo lo ocurrido durante la V edición del Foro IT Digital Security y cuáles han sido sus principales conclusiones. ■

## CONTENIDO RELACIONADO

Ciberresiliencia

La ciberseguridad impulsa el crecimiento del mercado de servicios gestionados

Este es el estado de la seguridad en cloud 2023

**La ciberdelincuencia en España representa el 15,6% de los hechos delictivos*.**

**No dejes que los ciberdelincuentes acaben con tu negocio.**

b FY

TU BIOMETRÍA
SOLO CONTIGO

b-fy.com

**b-fy.com**

*** Informe sobre la Criminalidad en España 2021.**

ADRIAN LÓPEZ, SENIOR DIGITAL ADVISOR EN PENTEO

# "EN ESPAÑA SE TARDA UNOS 287 DÍAS EN DETECTAR Y EN CONTENER ATAQUES"

La seguridad es un elemento esencial para las empresas y estar al tanto de la situación del panorama de la ciberseguridad, las amenazas y las técnicas que más utilizan los cibercriminales es ahora más vital que nunca.

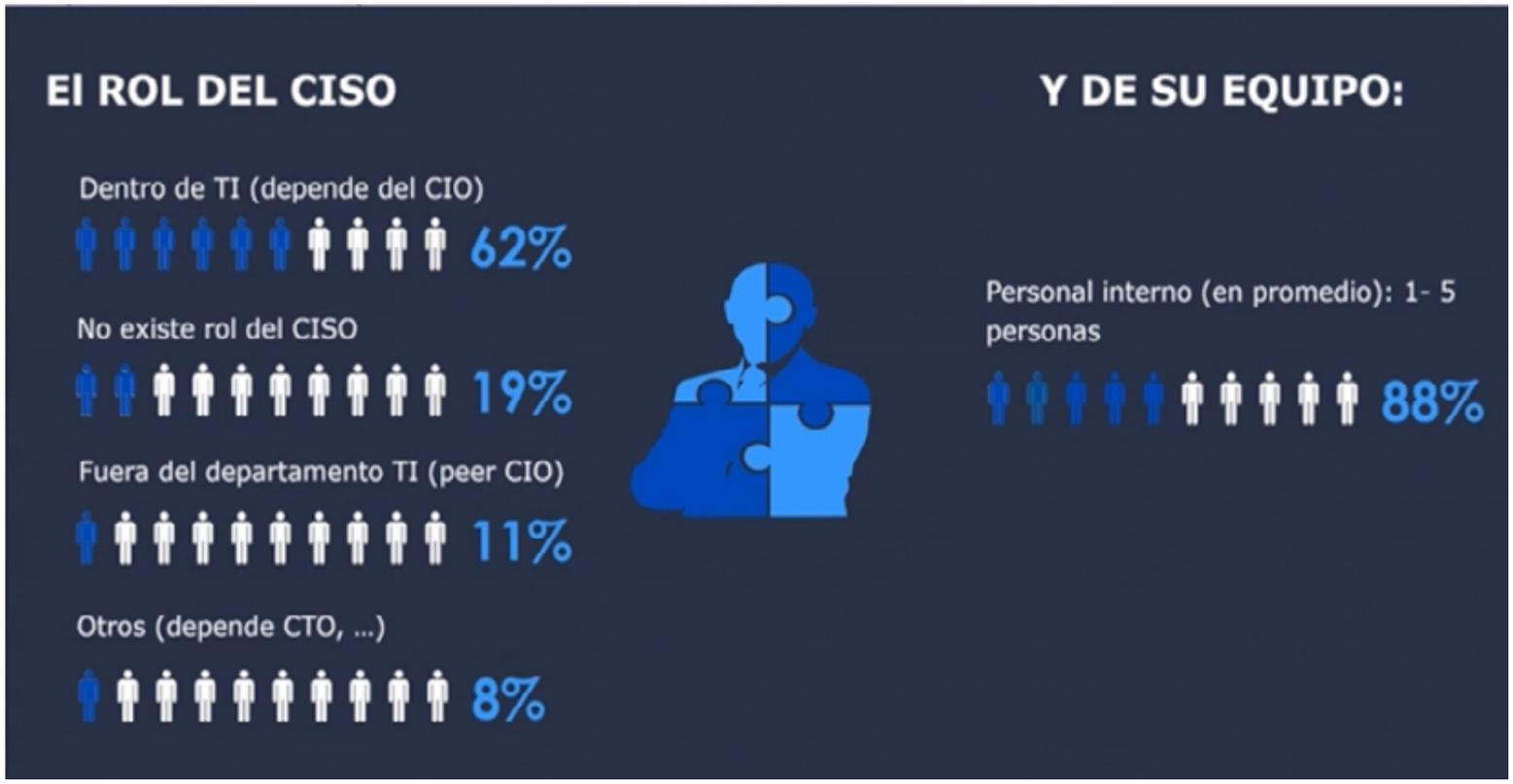
Para profundizar en el estado de la ciberseguridad a día de hoy, en la V edición del Foro IT Digital Security: Nuevos modelos de ciberseguridad para proteger a la empresa global, contamos con la participación de Adrián López Jareño, senior digital advisor de Penteo, quien compartió con nosotros las conclusiones del último estudio de la compañía en que se establece cómo ha cambiado el rol del CISO, cuáles son su mayores preocupaciones o a dónde van los presupuestos en IT y ciberseguridad.

La ciberseguridad es un elemento esencial para el negocio, y, como tal, presenta una serie de retos y oportunidades que es necesario

Panorama de la Ciberseguridad en España 2023/2024. Adrián López Jareño, Penteo

afrontar. Para verlos con más detalle, Penteo realiza cada año una investigación para conocer las previsiones y extraer algunos sobre las previsiones de inversión de cara a 2024 a nivel de ciberseguridad.

En su intervención, Adrián explicó que las organizaciones "para este 2023 tenían previsto invertir aproximadamente el 9% del total del presupuesto TI, en ciberseguridad, aunque, dentro de este promedio un 31% afirmaba estar por debajo de la media y una parte más pequeña del 20% por encima de la media".




## 2024 TRAERÁ MÁS INVERSIÓN EN CIBERSEGURIDAD

"Si preguntamos a las compañías españolas si va a haber mayor inversión en ciberseguridad para el 2024, el 87% declara que sí y este aumento además está previsto que sea de alrededor de un más 23% versus la partida de este año". Y es que, como explicaba en su ponencia el portavoz de Penteo, en muchos casos, esta necesidad de inversión es "fruto de cómo se han ido realizando estas inversiones en materia de ciberseguridad, pues muchas veces parece que la métrica que usamos al invertir en cualquier tipo de proyecto TI, y especialmente en ciberseguridad también, es el ROI, qué retorno vamos a obtener de la inversión en ciberseguridad". Llegados a este punto, Adrián reflexionaba sobre la necesidad de cambiar de enfoque y hablar más bien de RONI: "Creo que históricamente se enfocaba mal y a mí me gusta más hablar de RONI, de Risk of Non-Investment, pues si no acometemos estas inversiones en ciberseguridad, las consecuencias a nivel económico pueden ser mucho mayores".

¿A qué se dedica esta inversión? Pues, en datos de Penteo, principalmente a "abordar amenazas y vulnerabilidades existentes, a revisar las políticas y procedimientos internos de ciberseguridad, cumplimiento normativo, ciberseguridad a terceros y mejora de aplicativos y servicios a clientes. Además, pudimos conocer qué es lo que más le preocupa al CISO. "Aquí destaca la evaluación de riesgos, normativa, el cumplimiento legal, el inventariado, la formación (tanto interna del equipo como a nivel concienciación general de la organización) y la detección o prevención de incidentes. Dentro de este apartado vemos que, si en nuestro estudio de 2016 el 40% de los encuestados se consideraba, al menos, moderadamente vulnerable; En el 2023 el 86% ya se considera moderadamente vulnerable y además es el 14% restante se declara

**“SE DEBERÍA HABLAR MÁS DE RONI, DE RISK OF NON-INVESTMENT, PUES SI NO ACOMETEMOS ESTAS INVERSIONES EN CIBERSEGURIDAD, LAS CONSECUENCIAS A NIVEL ECONÓMICO PUEDEN SER MUCHO MAYORES”**

directamente muy vulnerable. Ha habido un viraje un poco más humilde acerca de cómo consideramos que estamos preparados y esto también nos hace estar un poco más alerta ante todas las amenazas”.

## CASI LA MITAD DE LAS EMPRESAS YA HAN SIDO ATACADAS

En base a esta clasificación, “un 40% de las compañías han sido afectadas por un ciberataque y se producen 1.252 ataques de media a la semana en España”. En lo que respecta al tiempo de respuesta, “se tarda unos 287 días en detectar y en contener ataques, que más o menos son 212 días de media para detectar y los 75 restantes para contener”.

Teniendo en cuenta estos datos, se preguntó a los participantes por la percepción que, en su organización, se tiene de la ciberseguridad y parece que se ha detectado una mejora en este aspecto pues “se está detectando mayor involucración de la Dirección General pues un 80% declara que la dirección está más involucrada y, por suerte también en muchos casos, la ciberseguridad se ve como un must have dentro de la organización y en pocos casos nice to have. Aunque, sigue habiendo parte de la muestra en la que la ciberseguridad se sigue viendo como gasto y no como inversión”.

## CONCLUSIONES

Por finalizar, el responsable de Penteo quiso extraer algunas conclusiones relativa a los cinco retos “que venimos arrastrando desde hace años”:

- La concienciación sigue siendo un reto: “una concienciación top down debe ir desde que cae en los comités de dirección hasta los desarrolladores que deben embeber la seguridad en sus diseños y hasta el último empleado que debe estar entrenado para prevenir ciertas malas praxis. Como se suele decir, la conciencia del peligro es ya la mitad de la seguridad y la salvación”.
- “El compromiso es el driver clave para cometer los proyectos de ciberseguridad. La dirección debe ser capaz de ver que la ciberseguridad puede ser un activo más de la compañía y que la falta de ella puede provocar un impacto tremendo en el negocio”.
- Estrategia y cultura: “es importante la gestión de la cultura o la higiene cibernética se integre adecuadamente para garantizar que la salud cibernética está en óptimas condiciones”.
- Ciberseguridad como una ventaja común: “la ciberseguridad como activo estratégico en las organizaciones puede marcar la diferencia”.
- Y el rol del CISO: “El CISO es una palanca fundamental. El CISO debe ser visto como un facilitador, como un partner para el negocio, para conseguir que los sistemas sean seguros, pero no como un stopper. Debe ser visto en las organizaciones como estratega o advisor influencer, como esa persona que hace que todos los proyectos puedan llegar a buen puerto y menos como un guardián de la tecnología”. ■

## CONTENIDO RELACIONADO

CyberTrends – Penteo

Crayon

# ¿Están protegidos tus entornos cloud o híbridos?

Inicia tu viaje seguro hacia la nube entendiendo el estado de tu seguridad.

Acceder a la guía

# SERVICIOS DE CIBERSEGURIDAD GESTIONADOS: LA LLAVE PARA UNA SEGURIDAD REAL

El contexto actual de transformación digital obliga a redefinir los planteamientos establecidos tradicionalmente para hacer frente a las amenazas de ciberseguridad, obligando a las organizaciones a reforzar, más aún si cabe, las medidas de protección frente a un entorno cada vez más hostil. Vivimos envueltos en una revolución tecnológica que requiere que especialización y actualización constante por lo que, a pesar de que, hasta ahora, las empresas han tratado de confiar la seguridad a departamentos internos, muchas están cambiando de perspectiva con el objetivo de abordar las necesidades de protección que existen hoy en día.

En este sentido no es de extrañar que el mercado de servicios gestionados de TI esté creciendo a un ritmo muy superior al gasto general en tecnología. Esto se debe en parte a una mayor demanda en determinadas áreas, como la ciberseguridad. De hecho, los ingresos mundiales procedentes de los ser-

**En este debate analizamos, de la mano mano de AENOR, IESE BUSINNES SCHOOL, RACC, PERNOD RICARD, HOLCIM , con la colaboración de CRAYON y SOPHOS, el papel de los servicios gestionados en la estrategia de ciberseguridad de las organizaciones.**


**“Los servicios gestionados son un apoyo al CISO, un apoyo muy importante”**
Diego Durantes, responsable de seguridad de la Información, **AENOR**


**“Cuando tienes 4 players encima de la mesa, lo que marca la diferencia es la confianza”**
Arsenio Tortajada,
CISO, **IESE BUSINNES SCHOOL**

vicios gestionados en el sector tecnológico aumentarán un 12,7% en 2023, casi cuadruplicando el crecimiento previsto del 3,5% del gasto general en TI para el mismo periodo.

Los nuevos modelos de protección de la empresa global incluyen ahora la opción de contar con servicios gestionados que ayuden a la compañía gestión de su estrategia de seguridad y es por eso que el primer panel de expertos de la V edición del Foro IT Digital Security: Nuevos modelos de ciberseguridad para proteger a la empresa global se centró, precisamente, en este punto. Para hablar sobre esta problemática contamos con la participación de responsables de seguridad de **Aenor, IESE Businnes School, RACC, Pernod Ricard** y **Holcim**; quienes tuvieron la oportunidad de conocer la propuesta de valor de **Crayon** y **Sophos** para hacer frente a sus problemas.

Los servicios gestionados surgen como una solución que permite seguir desarrollando el negocio eliminando las habituales problemáticas de asumir planificación, gestión de proyectos, contratación de equipos profesionales. ¿Por qué externalizar los servicios se ha convertido en la clave para muchas empresas? Esta fue la primera pregunta que se lanzó a los participantes para conocer los motivos que han llevado a muchas empresas a adoptar este modelo.

Para Diego Durantes, responsable de seguridad de la Información de Aenor, los servicios gestionados son “un apoyo al CISO, un apoyo muy importante”, de hecho, explicaba que “están fuera, pero para mí forman parte de mi empresa y son como un compañero más, lo único que no los tengo tan cerca, pero si es verdad que nos apoyamos mucho en los servicios de seguridad gestionada”. De la misma opinión es Carles Travé, CISO-Transformación Digital de RACC quien expuso que “para las empresas que somos medianas, pequeñas, es muy difícil contar con unos profesionales con un alto nivel de especialización. Estamos hablando de cibercrimen porque hay una tendencia de cibercrimen, el crime as a service, que hace necesario el surgimiento de los servicios gestionados”.

## EL GRAN ÉXITO DE LOS SERVICIOS DE SEGURIDAD GESTIONADOS

Los servicios gestionados surgen, entonces, para cubrir una necesidad del sector que, en pleno auge, necesita un nivel de especialización cada vez mayor. Con la incorporación de servicios gestionados de seguridad, las organizaciones se benefician claramente del acceso a profesionales altamente cualificados y con una gran experiencia, en un campo tan complejo como es el de la ciberseguridad.


**“Para las empresas medianas, pequeñas, es muy difícil contar con unos profesionales con un alto nivel de especialización”**
Carles Travé, CISO-Transformación Digital, **RACC**

Como consecuencia de la contratación de servicios de seguridad supone múltiples ventajas que van desde un claro ahorro de costes a corto plazo, ya que las organizaciones no deberán de realizar la contratación de profesionales, dotarlos de formación, como una mayor especialización y eficacia. El éxito de los servicios gestionados reside en una serie de ventajas:

Para Antonio Delgado, Global IT Security Officer, de Holcim son “útiles a la hora de disponer, diría que, de forma rápida, eficiente y a un costo razonable, de capacidades según surja la necesidad en la empresa”. Y compartía su caso: “en primer lugar destacaría los costos, ya que pongamos, por ejemplo, que decidimos implementar gestionar on-premise, una solución SIEM o DLP. Hablamos de invertir en licencias, tener que desplegar la solución, mucho trabajo de ajustarla y configurarla y disponer de personal capacitado. Al final, todo esto son recursos en los que se va a tener que invertir. Y todo esto se traduce en tiempo, en trabajo y en esfuerzo. Sin embargo, al optar por una solución gestionada de un proveedor externo, acceder de forma mucho más eficiente y probablemente con menos quebrados de cabeza a un servicio de ciberseguridad como solución de forma on-premise”. También compartía su caso Borja Carroquino, Head of IT Solutions, Mediterranean Countries en Pernod Ricard: “en mi compañía, cuando por fin se empezó a tomar en serio la ciberseguridad, obviamente por un ciberataque importante, ayudó mucho contar con una empresa que realmente sabe lo que tienes que hacer, que nos fue guiando y así empezamos a modificar todos nuestros procedimientos internos para ir incorporando la ciberseguridad”. A lo que añadió: “creo que hubiera sido absolutamente imposible si no hubiéramos contado con una empresa como servicio gestionado”. A lo que Arsenio Tortajada, CISO de IESE BUSINNES SCHOOL apuntó: “(los servicios gestionados) ayudan a todo tipo de organizaciones, quizás en organizaciones como IESE o similares, es una manera de disponer de estos servicios que de otra manera sería inviable, por falta de estructura, por costes, etc. En una mediana empresa es impensable disponer de un SIEM, un SOC, todos estos servicios más especializados que requiere perfiles técnicos muy formados, y una gran cantidad de recursos, es inviable y sin estos servicios gestionados sería imposible”.


**“Valoro que los servicios gestionados den otro punto de vista, pongan sobre la mesa el expertise”**
Borja Carroquino, Head of IT Solutions, Mediterranean Countries, **PERNOD RICARD**

Esta accesibilidad es, para el directivo de Holcim una de las claves del éxito de este tipo de servicios: “como la ciberseguridad no para de cambiar cada día, estos proveedores de servicios nos permiten acceder a capacidades de forma más rápida que si las queremos implementar desde cero, in-house”. Además, añade, “La escalabilidad es una de las grandes ventajas de estos servi-

**“Los servicios gestionados son útiles a la hora de disponer, diría que, de forma rápida, eficiente y a un costo razonable, de capacidades según surja la necesidad en la empresa”**
Antonio Delgado, Global IT Security Officer, **HOLCIM** ESPAÑA

cios. En cualquier momento, bajo demanda puedo ampliar capacidades de un servicio de forma mucho más rápida y eficaz según la demanda y la necesidad”. Para Durante la clave está en la accesibilidad “considero importante que los servicios que se hayan gestionados hoy en día sean tan accesibles para poder contratar”.

## SERVICIOS GESTIONADOS ¿EL MODELO A SEGUIR?

Preguntados por si este modelo es el futuro de la ciberseguridad, los participantes se mostraron dubitativos pues, como apuntaba el gerente de la seguridad en Holcim, “es arriesgado afirmarlo rotundamente porque la ciberseguridad es una especialidad que está en constante cambio y evolución y no para de sorprendernos”. Sin embargo, aunque prever hacia dónde vamos en cualquier sector, y más en ciberseguridad es complejo, el panorama de amenazas en rápida evolución y la gran escasez de profesionales que acusa el sector hace que este tipo de modelos estén crecimiento rápidamente. El propio Antonio así lo preveía: “la implementación de servicios gestionados va a ir en aumento los próximos años pues las empresas están dando cuenta de que gestionar toda la ciberseguridad de forma interna es un reto muy grande que requiere mucho presupuesto y además tener una plantilla muy especializada y tener la capacidad y el apoyo de la dirección para hacerlo”. No obstante, en ciberseguridad, no se puede externalizar todo. Tal y como apuntaban desde Aenor: “hay una parte que nunca, en general en IT y en ciberseguridad en concreto, nunca conviene externalizar, que es la toma de decisiones. Para decidir tienes que saber cuál es la cultura de la compañía, cuáles son los procesos core de la compañía”.

Del mismo punto de vista se mostró Arsenio, al afirmar: “hay decisiones técnicas que a lo mejor quedan más en manos de los técnicos,


**“Cada compañía es única, o sea, esto no es café para todos”**
José Bernal, director de Servicios, **CRAYON**

pero luego hay decisiones técnicas que afectan al negocio y ahí es obligatorio establecer este equilibrio entre las dos partes”.

## ¿QUÉ HAY QUE TENER EN CUENTA A LA HORA DE APOSTAR POR UN SERVICIO GESTIONADO?

A la hora de enfrentarse a esa decisión tan estratégica, es necesario tener claras las necesidades y el objetivo a cubrir. No obstante, muchos de los participantes en el debate mostraron que existe mucha subjetividad a la hora de apostar por un proveedor u otro, y la diferencia no siempre la marca la tecnología sino la confianza y las personas. Para el garante de la seguridad de IESE BUSINNES SCHOOL la clave está en “la empatía” y lo explicaba así: “cuando tienes 4 players encima de la mesa, lo que marca la diferencia es la confianza porque, al fin y al cabo, serán nuestras manos ejecutoras en muchas ta-

reas y hay que tener confianza ciega". Desde Aenor se mostraban de acuerdo y añadían: "cuando uno toma la decisión de contactar a un servicio gestionado, le tienes que inculcar tu empresa a esa empresa, o sea, tienes que hacerla partícipe de tus problemas, de tu visión de negocio" a lo que Borja Carroquino sumaba: "es muy importante el que se vaya mimetizando un poco con la cultura, tener esa confianza y sentir que te escuchan y entienden lo que les cuentas y son receptivos a cualquier cambio o cualquier comentario que pueda surgir", pero además de la confianza hay otros aspectos que cuentan para el directivo de Pernod Ricard: "otra cosa en la que me gusta fijarme cuando tienes la elección de un proveedor es que no sea lo que tú digas siempre. En definitiva, que te den otro punto de vista, pongan sobre la mesa el expertise".

## EL PUNTO DE VISTA DEL MERCADO

Para explicar algunas de las opciones que ofrece el mercado el mercado de la cibersgeuridad respecto a los servicios gestionados, tuvimos la oportunidad de escuchar la visión de Crayon de la mano de José Bernal, Director de Servicios de la compañía para España. En su intervención, José explicó que una de las claves de este tipo de servicios radica en la especialización: "cada compañía es única, o sea, esto no es café para todos" explicaba. Y nos ponía un ejemplo: "nosotros siempre que un cliente nos llama y hablamos de ciberseguridad, el primer paso que damos es hacer lo que nosotros llamamos BAC, Business Advisory Consulting, que básicamente es analizar, extraer datos de lo que se quiere proteger, analizarlos y sincronizarlos para, solo entonces plantear la solución".

Y es que, añadía el portavoz, "las soluciones de Crayon son múltiples y variadas, pero nos adaptamos al presupuesto del cliente". Eso sí, advertía: "Hay que cumplir unos mínimos. Si me dices que no tienes activadas las actualizaciones de Windows, por ejemplo, no te voy a poder proteger, por lo tanto, lo siento mucho, pero a un riesgo de perder unos ingresos para mi compañía importantes no te voy a dar el servicio". Además, José aprovechó para hacer entender a los presentes que la responsabilidad, a la hora de contratar un servicio gestionado es compartida: "yo voy a asumir una responsabilidad, pero si tu presupuesto te deja proteger el 25% de lo que tienes como activo, tienes que saberlo y te voy a escribir un disclaimer diciendo esto es cosa tuya". Al mismo tiempo, explicó que la industria sigue teniendo un gran problema: el enfoque de la ciberseguridad como un gasto "la palabra clave es inversión" exponía. "Todavía muchas empresas siguen pensando que es un gasto. ¿Qué es peor, que tener un ransomware o pagar 5.000 euros al mes? Evalúa" preguntaba.


**"En ciberseguridad hay mucha demanda y faltan profesionales, pero hay, sobre todo, muchas organizaciones que no saben que deben tener esa capacidad de detección de respuesta"**
Álvaro Fernández, Sales Manager, **SOPHOS**

Precisamente con el objetivo de no tener que llegar a eso Crayon entiende la ciberseguridad como un proceso de aprendizaje continuo "La ciberseguridad cambia continuamente por lo que nuestra relación es un proceso continuo de aprendizaje para nosotros y para vosotros, que también nos encargamos de formaros. O sea, no capturamos el conocimiento y generamos una dependencia malsana del cliente, sino que si yo aprendo te lo cuento y si necesitas más, seguimos hablando. Hay mucha gente que dice: "bueno, ya he contratado el servicio, ahora lo hace todo Crayon". No. Crayon puede

hacer el 80%, el 70%, pero el resto o trabajamos en equipo o no funciona" sentenciaba.

Llegado el turno el Sophos, Álvaro Fernández, Sales Manager de la compañía para Iberia no se escondía "Nosotros somos un fabricante de ciberseguridad, de productos, principalmente de ciberseguridad" pero, explicaba: "nos hemos subido al carro de los servicios con unos servicios muy específicos: servicios de detección y respuesta gestionados". Y es que, la situación que vive hoy en día el sector hace necesario que todos los actores remen en una misma dirección. Por eso Álvaro, en su intervención quiso dejar claro que su tecnología puede apoyarse en su propia inteligencia, en sus propios productos, pero también es capaz de apoyarse "en los productos que estén instalados dentro de la casa del cliente, aprovechando su stack de seguridad. Podemos beber de esa telemetría, procesar esa telemetría y en base a eso, detectar amenazas en fase temprana y responder en nombre del cliente, con la idea de eliminar o reducir el riesgo todo lo que se pueda".

Además, agregaba, "también ofrecemos un servicio de respuesta ante incidente para que esas compañías que han sufrido un incidente se apoyen en nuestros servicios con una guía de actuación muy clara". En ciberseguridad "hay mucha demanda y faltan profesionales, pero hay, sobre todo, muchas organizaciones que no saben que deben tener esa capacidad de detección de respuesta. O si lo saben, no hay dinero para ello". Y comentaba a los participantes del debate: "Si queréis montar un equipo de detección de respuesta, necesitáis que sea 24 x 7, que estén altamente formados y cualificados y que sigan unos procedimientos y se apoyen en una tecnología. Necesitas meter a 6 o 7 personas y eso, para el 90 y mucho por ciento del tejido español es imposible".

Y concluía: "Nosotros como fabricante de ciberseguridad creemos que podemos aportar mucho valor ahí por la cantidad de gente que tenemos. Ahora mismo somos el proveedor más grande que existe de MDR y yo creo que podemos ayudar a muchísimas organizaciones pues tener tantos clientes también nos ayuda a saber lo que está ocurriendo en otros lugares y lo que puede ocurrir. Al tener clientes de todos los sectores, conocemos qué tipo de ataques se ven más en cada tipo de actividad y, lo más importante, sabemos cómo responder, porque al final, ese servicio de monitorización y respuesta está continuamente enfrentándose a amenazas reales, a atacantes activos".

## CONCLUSIONES

Tal y como vimos en el debate, en ciberseguridad ya no vale adoptar una postura reactiva y actuar sólo en caso de ciberataque. Hoy en día, debemos ser proactivos, "prevenir antes que curar" como marca el refranero español y eso implica mejorar la inversión en ciberseguridad, no necesariamente invertir más, sino invertir mejor, conociendo nuestras necesidades y los diferentes modelos que existen en la industria para aumentar nuestras capacidades de protección de la forma más sencilla posible. Los servicios gestionados se han convertido sin duda en uno de los modelos predilectos y, parece, seguirá siéndolo en los próximos meses pues es la única forma, para muchas empresas, de alcanzar una ciberseguridad real. ■

## CONTENIDO RELACIONADO

La ciberseguridad impulsa el crecimiento del mercado de servicios gestionados

Mejorando la seguridad con servicios gestionados

RAWAN NAZMI-ISSA, GERENTE DE RISK-ADVISORY-CIBERSEGURIDAD DE DELOITTE

# "ES ESENCIAL QUE LAS EMPRESAS ESPAÑOLAS COMPRENDAN CÓMO NIS2 AFECTA SUS OPERACIONES Y QUÉ MEDIDAS DEBEN TOMAR PARA CUMPLIR CON SUS DISPOSICIONES"

La ciberseguridad es un sector en constante cambio y esta evolución tiene que ir acompañada de un avance en el terreno normativo capaz de velar por la protección de los activos de las empresas y los ciudadanos. En los últimos años hemos visto cómo surgían iniciativas legislativas europeas y cómo muchas de las normativas ya existentes se adaptaban a pasos agigantados al nuevo entorno, pero ahora son las empresas las que deben estar al tanto de las novedades para poder cumplir con la norma y evitar las temidas multas.

Por eso, una de las ponencias de la V edición del Foro IT Digital Security: Nuevos modelos de ciberseguridad para proteger a la empresa global se centró en la Directiva NIS 2 y los cambios que supone su entrada en vigor para el tejido empresarial español.


**NIS 2: Directiva sobre las medidas destinadas a garantizar la ciberseguridad en la UE. Rawan Nazmi-Issa, Deloitte.**

En esta ponencia, Rawan Nazmi-Issa, gerente de Risk-Advisory-Ciberseguridad de Deloitte nos comparte las claves de la Directiva NIS2 y los cambios que supone para las empresas.

La directiva de seguridad de redes y sistemas de información 2 (NIS2) de la Unión Europea, es un marco regulatorio fundamental diseñado para fortalecer la ciberseguridad en toda Europa. A partir de su entrada en vigor, la NIS2 introduce una serie de cambios significativos con el objetivo de extender su alcance y reforzar la protección digital en sectores críticos y servicios digitales. "En este contexto, es esencial que las empresas españolas comprendan cómo esta regulación afecta sus operaciones y qué medidas deben tomar para cumplir con sus disposiciones" señalaba Rawan para hacer hincapié en la importancia de que las empresas se adapten a la nueva norma.

Para comprender las novedades que vienen con la llegada de la nueva normativa, es vital conocer los principales hitos que ha sufrido esta directiva desde su primera entrada en vigor. "A lo largo de estos últimos años, hemos visto que esta directiva ha ido acompañada de distintas publicaciones tanto a nivel nacional como a nivel europeo. Entre los puntos más importantes a tener en cuenta destacan varias fechas: en julio de 2019 se empezó a trabajar a nivel nacional el proyecto del Real Decreto para ese desarrollo reglamentario que necesitábamos en España y que vio la luz en el BOE en enero de 2021. Poco después, el 27 de diciembre de 2022 la publicación de la NIS 2 vino acompañada del reglamento DORA, que también está dando bastante que hablar, y de la directiva CER, que está muy enfocada, igual que las otras dos, a esa resiliencia, a esa mejora, pero en infraestructuras críticas".

**"NIS2 INTRODUCE UNA SERIE DE CAMBIOS SIGNIFICATIVOS CON EL OBJETIVO DE EXTENDER SU ALCANCE Y REFORZAR LA PROTECCIÓN DIGITAL EN SECTORES CRÍTICOS Y SERVICIOS DIGITALES"**

## ¿QUÉ NOS TRAE LA NUEVA DIRECTIVA NIS 2?

Uno de los cambios clave en la NIS2 es su alcance ampliado. Ahora, la regulación no solo se aplica proveedores de servicios digitales (DSP) u operadores de servicios esenciales (OSE) sino que también incluye a sectores adicionales, como salud, finanzas y energía que, con este cambio, pasan a formar parte de esas entidades afectadas por la norma. "Lo que queremos es llegar a cubrir el máximo posible" apuntaba Rawan.

Además, como toda normativa, "trae impactos e incluye una serie de pilares sobre los que va a trabajar y desarrollar sus exigencias. Los principales pilares de NIS 2 son:

- **Gobernanza:** "la responsabilidad recae en el órgano de dirección de la empresa". En este sentido, la normativa hace hincapié en la necesidad de formación "necesitamos a gente formada" aseguraba Rawan.
- **Gestión:** "NIS2 detalla mucho más cómo tenemos que trabajar las medidas de seguridad que tenemos que llevar a cabo o tener implementadas en nuestras compañías". La NIS2 exige a las empresas realizar evaluaciones de riesgos digitales para identificar amenazas y vulnerabilidades en sus sistemas de información. Posteriormente, deben implementar medidas de seguridad adecuadas para proteger sus activos digitales contra posibles ataques. Esto incluye la necesidad de establecer políticas y procedimientos de seguridad robustos.
- **Intercambiar conocimiento, experiencia e información:** La NIS2 promueve la colaboración entre empresas y países de la UE que culmina con la creación de un grupo de cooperación, lo que implica que las empresas deben trabajar en estrecha colaboración y compartir información relevante sobre amenazas y ciberataques con las autoridades nacionales y otras empresas. "Cuando una persona ha su-


## "CON LA NIS 2 SE ESTABLECEN CON MÁS DETALLE LOS TIEMPOS PARA NOTIFICACIONES TEMPRANAS, NOTIFICACIONES INTERMEDIAS Y NOTIFICACIONES FINALES"

frido un ataque, ya tiene cierta experiencia, ya sabe qué no debe volver a hacer, ya sabe qué le ha llevado a tener éxito en esa mitigación, en esa resiliencia o en esa respuesta ante ese incidente. La nueva norma quiere que compartamos esa información para que la colaboración nos haga más fuertes".

❖ **Incidentes:** en este ámbito la directiva NIS 2 establece que, en caso de sufrir un incidente de seguridad, las empresas deben notificarlo para permitir una respuesta coordinada y efectiva ante ciberamenazas. "En la directiva NIS 1 había un apartado, un artículo, que ponía bastante foco en gestión de incidentes, sin marcar tiempos de cómo había que notificar. Con la NIS 2 ponemos mucho más foco, se establecen con más detalle los tiempos para notificaciones tempranas, notificaciones intermedias y notificaciones finales. Además, obliga a notificar a nuestros proveedores para que estén también al tanto de cómo estamos trabajando en esa respuesta ante el incidente". Así mismo, se establecen tiempos máximos para esa notificación: "24 horas para la notificación inicial, 72 horas si hablamos de una notificación intermedia o un mes para esa notificación final".

También incluye un nuevo papel, el papel del supervisor. "Y como toda supervisión, vendrá acompañada una sanción porque si no, nadie nos haría caso" aseguraba entre risas Rawan a los asistentes al evento. Estas sanciones pueden incluir multas significativas, lo que subraya la importancia de abordar seriamente la seguridad de la información, pero, además, se establecen las competencias de ese supervisor de forma que se ha de saber quién es el responsable a la hora de saber cómo poder desplegar o trabajar las estipulaciones marcadas por el reglamento. En relación con este cumplimiento, "habrá que tener en mente nuevas fechas, fechas en las que tendrá lugar esa transposición que será el año que viene, en octubre de 2024, y que incluirá una lista de entidades que deberán tener en cuenta su aplicación".

En definitiva, NIS2 llega con novedades y lo hace con el objetivo de modernizar el marco jurídico existente para adaptarse al aumento de la digitalización y un panorama de amenazas a la ciberseguridad en plena evolución. Al ampliar el ámbito de aplicación de las normas de ciberseguridad a nuevos sectores y entidades, se busca mejorar la resiliencia y las capacidades de respuesta a incidentes de las entidades públicas y privadas, por el bien común. ■

### CONTENIDO RELACIONADO

Directiva de seguridad de redes y sistemas de información 2 (NIS2) de la Unión Europea

ESET BUSINESS SOLUTIONS

# BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

## Gestiona toda la ciberseguridad de tu empresa estés donde estés.

| PREDICCIÓN | PREVENCIÓN |
|---|---|
| ESET Threat Intelligence<br>ESET Virus Radar<br>WeLive Security | Endpoint Protection Platform<br>ESET Mail Security<br>ESET Sharepoint Security<br>ESET Secure Authentication<br>ESET Endpoint Encryption<br>ESET PROTECT |
| **RESPUESTA** | **DETECCIÓN** |
| ESET Inspect<br>ESET LiveGuard Advanced<br>ESET PROTECT | Endpoint Protection Platform<br>ESET LiveGuard Advanced<br>ESET Inspect<br>ESET Mail Security<br>ESET Secure SharePoint Server<br>ESET Secure Authentication<br>ESET Endpoint Encryption<br>ESET PROTECT |

Progress. Protected.

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

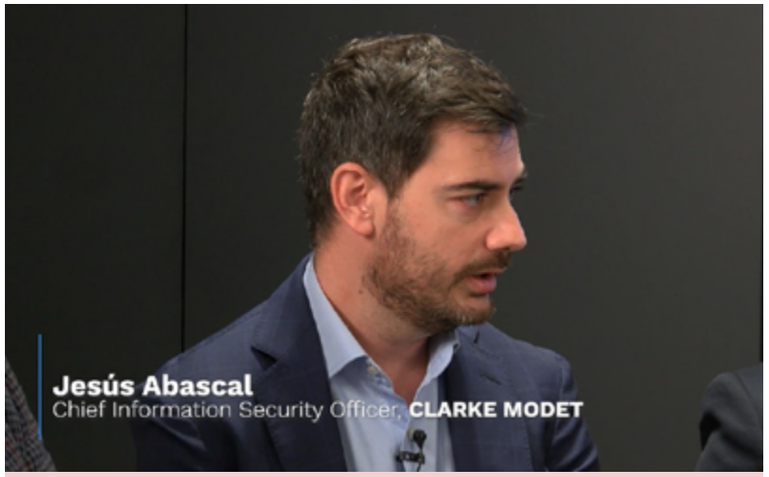
MADE IN EU

# CONFIANZA CERO: CONSTRUYENDO UN PERÍMETRO EMPRESARIAL SEGURO

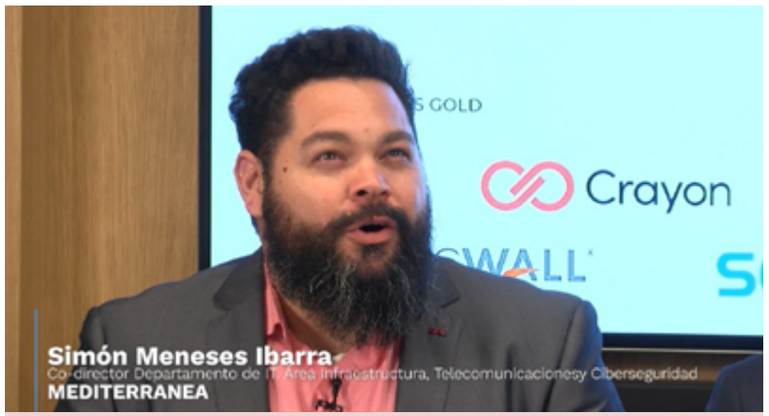
**EL SEGUIMIENTO DE INTRUSIONES Y LA ACTUALIDAD ES, SIN DUDA, UNA DE LAS CLAVES DE LA PROTECCIÓN REAL. LAS SOLUCIONES DE SEGURIDAD DEBEN SER CAPACES DE DETECTAR ACTIVAMENTE LAS AMENAZAS. PARA REALIZAR ESTA TAREA, SE REQUIERE UNA VISIBILIDAD COMPLETA DE LO QUE OCURRE EN NUESTRO ENTORNO Y ESO, EN LOS TIEMPOS QUE CORREN, NO ES TAREA FÁCIL. POR ELLO, ANTE LA FALTA DE VISIBILIDAD Y INCAPACIDAD DE GESTIÓN GLOBAL, SON MUCHAS LAS COMPAÑÍAS QUE HAN OPTADO POR ENFOQUE EN EL QUE DESCONFIAR SE HA CONVERTIDO EN LA CLAVE.**

Hasta hace poco, el perímetro de seguridad que teníamos que proteger estaba dentro de las cuatro paredes de nuestras empresas. Pero esto ha cambiado mucho en los últimos años. La incorporación de nuevas formas de trabajo híbridas y remotas, la utilización de la nube o de dispositivos móviles o conectados ha supuesto un cambio de paradigma en ciberseguridad. Los nuevos modelos de protección de la empresa global incluyen ahora la confianza cero en mayor o menor medida y es por eso que la primera mesa redonda de la V edición del Foro IT Digital Security: Nuevos modelos de ciberseguridad para proteger a la empresa global se centró, precisamente,


**Analizamos, de la mano mano de CLARKE MODET, MEDITERRÁNEA, ORANGE, RISKMEDIA GROUP, SOLARIA ENERGÍA, con la colaboración de B-FY, SAMSUNG y SONICWALL, el papel de la confianza cero en la estrategia de ciberseguridad de las organizaciones.**




**“Cada vez vienen más normativas que te imponen nuevos controles evitar que haya fugas de información”**
Jesús Abascal, CISO de **Clarke Modet**




**“El zero trust probablemente sea uno de los retos más importantes que podemos tener dentro de las organizaciones, ya que tienes que no confiar en tus propios usuarios”**
Simón Meneses, Co-Director Departamento IT, Área Infraestructura, Telecomunicaciones y Ciberseguridad de **Mediterránea**

en este enfoque en el que desconfiar es la máxima norma.

En este debate participaron responsables de ciberseguridad de **Clarke Modet, Mediterránea, Orange, RISKMEDIA Group** y **Solaria** para hablar de su preocupación por la visibilidad, el control y la proliferación de modelos como BYOD. **B-FY, Samsung** y **SonicWall** aportaron su visión tecnológica.

Precisamente de este riesgo nos habló Simón Meneses, Co-Director Departamento IT, Área Infraestructura, Telecomunicaciones y Ciberseguridad de Mediterránea para quien la pandemia supuso un antes y un después. “Ahora desde cualquier móvil, tablet, portátil se conecta a la infraestructura de la empresa desde cualquier wifi, la del autobús, la de otras empresas y tienen acceso a toda una infraestructura que ya dejó de ser una cajita cerrada, un perímetro cerrado”. Entonces para poder dar una garantía de que los datos están seguros, “tengo que desconfiar de todo y de ahí nace el famoso este zero trust”. “Esta filosofía probablemente sea uno de los retos más importantes que podemos tener dentro de las organizaciones, ya que tienes que no confiar en tus propios usuarios” señalaba Simón.

Para Alberto López, Global Head of IT and Cybersecurity de Solaria “el zero trust era un paso natural en la cultura de seguridad para mejorar los procesos” porque, sentencia: “el factor persona siempre es el que más riesgo se entraña”.

Y sin embargo,” nos encontramos con empresas medianas y grandes que siguen siendo muy reacios a aceptar que el uso de credenciales, usuarios y contraseñas es un tema desfasado, del pasado, y que hay que complementarlo con un doble factor de autenticación. Si a esto le añadimos que encima tenemos que vigilar la manera de trabajar de nuestros proveedores externos de servicios tecnológicos, ahí tenemos un mix con el que sin duda los ciberdelincuentes se están frotando las manos” señalaba José Ramón Monleón, Manager Seguridad Información Corporativa - Dirección de Seguridad de Orange.

Sin duda, el archifamoso “factor humano” es una de las grandes preocupaciones a día de hoy en ciberseguridad y el origen del surgimiento de posturas como la confianza cero en la que, se apuntó desde Solaria: “la confianza se tiene que ir ganando”.

El zero trust se base, entonces, en una “restricción por defecto” en la que el usuario tiene que probar que es quien dice ser, pero, para Jesús Abascal, CISO de Clarke Modet, va más allá pues nos permite saber realmente “si se está conectando desde un equipo, dispositivo corporativo, con el sistema actualizado,



**“Es imposible monitorizarlo todo”**
José Ramón Monleón, Manager Seguridad Información Corporativa - Dirección de Seguridad de **Orange**


**“Todos tengan el tamaño que tengan, tienen posibilidades de acceder a herramientas en cuanto a ciberseguridad se refiere”**
David Santana, Responsable de Ciberriesgo de RISKMEDIA Group

con antivirus corporativo, etcétera”. “El poder crear canales de comunicación, usuario, aplicación tipo VPN, para manejar toda la información y dar visibilidad y conectividad es vital”. No se trata de evitar el teletrabajo, sino de securizarlo. “Nosotros facilitamos el teletrabajo y lo que queremos es que cualquier usuario, en cualquier sitio, se pueda conectar y pueda teletrabajar de manera cómoda sin que suponga un esfuerzo adicional en su día a día pero que tampoco suponga un problema para la empresa” compartía Jesús.

Esa visibilidad se convirtió, sin duda, en uno de los ejes centrales del debate pues, como apuntaba David Santana, responsable de Ciberriesgo de RISKMEDIA Group: “que la seguridad de la información esté en nuestro sistema, esté en servicios eternos, no deja de ser responsabilidad de uno mismo”. “Todavía alguno piensa que teniendo todo en la nube o sacándolo todo de sus propios servidores o sistemas ya tienen solucionado todo el problema y que no se tienen que preocupar mucho más por la seguridad, cosa que lógicamente no tiene ningún sentido” sentenciaba. Y es que, como añadían desde Orange: “aunque se dice que no existe, el perímetro al final existe: es acceso a una aplicación, pero lo que hay que tener en cuenta es que el perímetro se va ampliando sin que tú te enteres. Las aplicaciones no son las mismas que teníamos hace diez años y ya no es que tú hayas contratado o tú tengas un servicio en la nube, sino que el propio usuario utiliza los servicios en la nube y te obliga, no solamente a tener un control de tus aplicaciones corporativas, sino de las aplicaciones que tus usuarios o tu empresa están utilizando”.

“Se trata de trasladar esa precaución que tenemos en el mundo físico al mundo digital. Es algo que en el mundo físico hacemos sistemáticamente, y sin ni siquiera te-


**“Aquello que no podemos ver, monitorizar, no podemos ejercer ningún control”**
Alberto López, Global Head of IT and Cybersecurity, **Solaria Energía**

ner que pensar en ello: cierras la puerta de tu casa, cierras el coche, pones una etiqueta en la maleta por si acaso…desconfiar” agregaba el directivo de Solaria.

## LA VISIBILIDAD: CLAVE PARA UNA PROTECCIÓN REAL

Tal y como afirmó Alberto de Solaria de forma rotunda: “No se puede ejercer ningún tipo de control sobre aquello que no puedes ver” y esta es precisamente una de la grandes precoupaciones de los CISO hoy en día. Por ello, para el responsable de Solaria “lo mejor es configurar un CASB, que te dé acceso a esas aplicaciones SAS y te de toda visibilidad que necesitas para definir las políticas y accesos, incluso configurar los roles de cada usuario”. Una vez establecido ese primer punto, hay que proteger “todo lo que es la red y endpoints: tanto móvil, dispositivo, laptop, cualquier dispositivo que use el usuario, lo tenemos monitoreado con un pequeño agente, que  junto al EDR, a través de inteligencia artificial, nos va indicando alertas de peligrosidad”.

Una apuesta similar tienen en Mediterránea: “tenemos que apoyaros sí o sí en proveedores de tecnología que, de una u otra manera, instalando un agente con una APN específica, u otro método, realmente recoja la información que pasa a través de un tráfico, como con un firewall virtual, un firewall en cloud, para tener una visibilidad de verdad útil”. Pero, ¿se puede monitorear y tener visibilidad sobre la infraestructura completa de la empresa? José Ramón Monleón no parece muy seguro: “el mercado que se está moviendo a tener muy controlado el dato pero es imposible monitorizarlo todo” sentenció, -a lo que agregó- “al final es un tema de análisis de riesgo y a veces para reducir el riesgo, tienes que limitar el uso. “Hay que hacer un compendio de las herramientas que debería utilizar un empleado por eficiencia, por necesidades del negocio, versus lo que te aporta, versus el problema


**“Las identidades llevan años en el centro de la ciberseguridad”**
Rodrigo Jiménez, Managing Director de **B-FY**

de seguridad que puede dar, y restringir y monitorizar en consecuencia”.

Además, apuntaba a una de las grandes problemáticas del sector: “en ciberseguridad cada vez tenemos muchas más herramientas, cada vez tenemos más dashboards, que monitorizan, regulan, lanzar alarmas, etcétera.; pero yo no tengo gente para monitorizar todo eso, para ver los dashboards. La monitorización, tener visibilidad de todo ello, es un reto impresionante”.

De la misma opinión es el responsable de Clarke Modet quien compartió su modelo de negocio a día de hoy: “nosotros estamos desregulando un poco todos los datos: vemos como viajan, como se almacenan, quién accede…

más que nada porque cada vez vienen más normativas que te imponen nuevos controles evitar que haya fugas de información. Y nosotros no es que tengamos demasiados datos, como ocurre en otras empresas, pero sí que tenemos algunos confidenciales, incluso algunos que son de secreto de alto nivel que tenemos que vigilar muy bien".

De hecho, apuntaba, Monleón: "todas esas normativas implican un informe de trazabilidad para mostrar que has tenido un incidente, qué es lo que ha ocurrido... las autoridades van a pedir ese informe y eso requiere tener la visibilidad suficiente como para poder tener un peritaje que te diga lo que ha ocurrido realmente y cómo has hecho frente a ese problema".

Y esto afecta a todas las empresas, independientemente de su tamaño. El responsable de RISKMEDIA Group manifestó que "los pequeños y medianos ya son conscientes de que la ciberseguridad es una cosa que le afecta a todos, da igual el tamaño, donde estés o a lo que te dediques, pero ellos siguen viendo la ciberseguridad como herramientas para presupuestos millonarios que no están hechas para ellos." Y lanzaba un mensaje directamente a estas pequeñas y medianas empresas: "Todos tengan el tamaño que tengan, tienen posibilidades de acceder a herramientas en cuanto a ciberseguridad se refiere".

En este contexto, afirmaba el directivo de Orange "la ciberseguridad debería ser el área de mayor crecimiento en cualquier empresa en tanto que todas las empresas cada vez tienen más datos, más información, más usuarios deslocalizados, más globalización y demás. La ciberseguridad, si estamos concienciados con ello, debería ir por delante de cualquier otra inversión".

## LA VISIÓN DEL PROVEEDOR

Los retos y problemas expuestos en el debate no son nuevos para la industria, porque, como reconocía Rodrigo Jiménez, Managing Director de B-FY, "las identidades llevan años en el centro de la ciberseguridad". Por eso, B-Fy ofrece su tecnología "en marca blanca para que seáis vosotros, los que le déis la oportunidad al usuario final o bien a un empleado de que evite el uso de contraseña. Nuestra tecnología os la cedemos a vosotros y sois vosotros los que dais un servicio final como oferta vuestra utilizando la biometría de los propios fabricantes de dispositivos. Es decir, ofrecemos un modelo colaborativo donde te evitas la contraseña con lo que, desde el lado de la gestión de IT no tienes que gestionar una base de datos centralizada de contraseñas y de punto de vista de identificación es un modelo no cloud, que lleva la identidad al dispositivo sin necesidad de almacenarlo en cloud".


**"Aparte de trabajar en dispositivos que desde el diseño estamos securizando, vamos a implementar soluciones cloud para identificar al empleado, para aplicar esta política de privilegio mínimo"**

Isabel López Peral,
Sales Engineer Manager de **Samsung**


**"Para reducir la superficie de exposición al riesgo en ciberseguridad es necesario implementar una serie de sistemas de gestión, planes de ciberseguridad al mismo tiempo que desplegamos las mejores herramientas de detección y protección"**

Eduardo Brenes, Territory Manager de **SonicWall**

Por su parte, Isabel López Peral, Sales Engineer Manager de Samsung España quien quiso destacar cómo en Samsung dentro del diseño "de nuestros dispositivos móviles, la seguridad es uno de los pilares". Desde el diseño del terminal, desde hace más de 10 años, Samsung cuenta con un proyecto, llamado Knox donde se fabrican terminales con el sistema operativo Android pero a este sistema operativo Android "al que vamos a añadir una serie de capas de seguridad que nos va a ofrecer un terminal más seguro y más gestionable. Esta plataforma de seguridad que viene embebida en el sistema operativo, Samsung va más allá en la línea de proteger esos datos biométricos, esa información súper sensible que está en el terminal y que nunca debe salir fuera. Se trata de una Smart Card donde se va a almacenar información sensible de forma que la comunicación con esa información es con un procesador seguro".

"Aparte de trabajar en dispositivos que desde el diseño estamos securizando, vamos a implementar soluciones cloud para identificar al empleado, para aplicar esta política de privilegio mínimo, donde se permite definir cuáles son tus accesos, hasta dónde puedes llegar, independientemente de dónde te estés conectando, gracias al contexto. Un terminal móvil, un teléfono móvil aporta mucha información del contexto, vamos a saber dónde estás ubicado, qué cuenta, tanto de Google como de la Samsung account se ha registrado, cuando se creó esa cuenta a la qué tienes acceso... todo ese contexto que se está generando con el terminal nos va a servir para identificarte y saber si confiamos o si vamos a evitar el acceso" añadía. La unión entre Knox y estas soluciones nos permite "tener controlado un parque de dispositivos, no sólo móviles sino cualquier dispositivo de la empresa, y tener conocimiento de cómo se está comportando".

Para concluir el debate tuvimos la oportunidad de conocer la propuesta de valor de SonicWall que, de la mano de Eduardo Brenes, su Territory Manager para Iberia quien bromeaba diciendo que "el siglo XXI comenzó con dos décadas de retraso, comenzó en marzo 2020". Y es que la pandemia hizo que la transformación digital y digitalización de las compañías se llevase a cabo a un ritmo vertiginoso. "Estamos en un mundo hiperconectado y descentralizado, en el cual hay gente conectada desde cualquier sitio, accediendo desde cualquier dispositivo, recursos on-premise y en la nube, sensores IoT por todos lados... El perímetro, como decíamos, se ha desdibujado". En ese sentido, decía Eduardo, "yo creo que todos estamos de acuerdo en que para reducir la superficie de exposición al riesgo en ciberseguridad es necesario implementar una serie de sistemas de gestión, planes de ciberseguridad al mismo tiempo que desplegamos las mejores herramientas de detección y protección".

Como compañía americana, "que llevamos 32 años de historia en el mercado", decía Eduardo, "ofrecemos soluciones de todo tipo, tenemos soluciones basadas en el contexto, ese tipo de soluciones de acceso seguro, de soluciones de protección de correo electrónico, de CASB, tipo Cloud Access Security Blocker, soluciones tipo SASE, ZTNA, wireless, Wifi 6 y los accesos cableados con switches. Tenemos de todo pero lo más importante es que tenemos experiencia y que sabemos que incluso nosotros podemos ser atacados y, como vosotros, tenemos que estar preparados para ello". ■

## CONTENIDO RELACIONADO

Caminando hacia Zero Trust

SAMSUNG

# Galaxy Z Fold5

## Protegido por Knox

Mantenga su negocio
protegido de forma íntegra


Imagen simulada con fines ilustrativos. UX/UI (experiencia de usuario/interfaz de usuario) puede variar y está sujeta a cambios. S Pen se vende por separado y sólo es compatible con Z Fold5, Z Fold4 y Z Fold3. El modo Flex es compatible con ángulos entre 75° y 115°.

LORENZO MARTÍNEZ, CONSULTOR DE SEGURIDAD, PERITO INFORMÁTICO FORENSE Y DIRECTOR TÉCNICO EN SECURÍZAME

# "CON "R" DE RANSOMWARE"

El ransomware es sin duda una de las técnicas de ataque más conocidas (por ser una de las más utilizadas por los cibercriminales). De hecho, los ataques ransomware ya no son simplemente una amenaza; ha evolucionado para convertirse en una herramienta tan poderosa como las temidas Amenazas Persistentes Avanzadas (APT). Además, se ha utilizado como un arma geopolítica en un intento de desestabilizar las economías rivales.

En esta ponencia, de la mano de Lorenzo Martínez, Consultor de seguridad, perito informático forense y director técnico en Securízame, conocemos qué ha motivado su evolución, los tipos que existen e incidentes destacados, pero también abordamos las diferentes estrategias, técnicas y tácticas generales empleadas por los grupos de ransomware; y se ofrece una visión del estado actual en materia de protección frente a este malware, con recomendaciones de cara a mejorar la situación de las empresas.


**Con R de ransomware. Lorenzo Martínez, Securízame.**

En la V edición del Foro IT Digital Security no podía faltar un espacio dedicado al rey del cibercrimen que, en la primera mitad de 2023, ya superó el equivalente al 90% del pago en rescates de todo el 2022. Para Lorenzo Martínez, el ransomware es un antiguo conocido, "he gestionado más de 100 casos de ransomware en empresas, he visto gente llorar por tener que cerrar la empresa" confesaba. Y es que, como perito informático su tarea empieza una vez el atacante ha conseguido su objetivo: entrar en la empresa. Una vez dentro y con los ordenado-

## “MUCHOS CREEN QUE SOY EL GENIO DE LA LÁMPARA Y PONEN TODA SU FE EN MÍ Y NO ENTIENDEN QUE HAY CIERTAS COSAS QUE A TORO PASADO NO PUEDO SOLUCIONAR”


res bloqueados, sucede la llamada. “¿Qué es lo que me encuentro cuando llego a una empresa?” lanzaba Lorenzo al público compuesto por CISO y expertos del sector – su siguiente diapositiva no dejó a nadie indiferente pues mostraba un escenario apocalíptico similar al de series como The walking dead o The Last of Us.

“Lo que generalmente pide la gente son dos tipos de cosas. Una: quiero que me recuperes todos los ficheros y, otra, muy distinta: dime cómo ha pasado esto para que no me vuelva a pasar”. Ambas situaciones ocurren de forma recurrente pero una petición es posible y la otra no. “Muchos creen que soy el genio de la lámpara y ponen toda su fe en mí y no entienden que hay ciertas cosas que a toro pasado no puedo solucionar” explicaba Lorenzo, -a lo que añadía-, “se pasa mal, sobre todo en el momento en el cual no queda más remedio que pagar porque no hay forma de recuperar los archivos”.

Lo que sí es posible llegados a este punto post-incidente, es intentar descubrir qué ha ocurrido llevando a cabo labores de DEFIR, labores de Digital Forensics Inseam Response. Este tipo de análisis trata de identificar qué ha sucedido y ver si podría haber sido evitado ese acceso ilegítimo que ha posibilitado el cifrado completo de los datos de la empresa de forma que, aunque no soluciona la situación actual, sí muestra las debilidades y necesidades de protección de la compañía para no tener mayores problemas en el futuro.

### LA EVOLUCIÓN DEL RANSOMWARE

Durante su presentación Lorenzo mostró varias pantallas típicas de un ataque de ransomware “fijaos aquí tenéis 2015, ya tenía este aspecto” puntualizaba para mostrar que por mucho que se hable de evolución del ransomware, esta técnica lleva años siendo el dolor de cabeza de millones de expertos. “La forma en la cual se pagaba era a través de una dirección de bitcoins, antiguamente, Si nos vamos más atrás incluso se solicitaba un código ucash, tenías que ir a comprar un código ucash, dar el código y con eso alguien en otro país sacaba y le daban ese dinero”. Con las criptomonedas solo se hizo posible que el pago y el cobro fuese más sencillo y universal.

“Lo que sí ha cambiado mucho es la forma del acceso al usuario, es decir, el usuario ha ido pudiendo tener incluso diferente grado de interacción con los malos, no solo a través de un correo, sino a través de paneles dentro del corrector en los cuales puedes probar a descifrar uno o dos ficheros, llevar a cabo el pago y darle al F5 y que te aparezca el Decryptor”.

Sin embargo, los canales de entrada siguen siendo los mismos. Han aumentado pues “desde el momento en el cual la empresa abre su exposición o hace uso de servicios en diferentes plataformas la exposición es mayor y

el control, muchas veces menor". Mensajería instantánea, correo electrónico con enlaces, archivos ofimáticos que contienen macros...las opciones son múltiples pero lo importante es tener claro cómo funciona el ransomware porque, tal y como apuntaba Lorenzo en su intervención, lo que sí ha cambiado es que ahora existen "ataques dirigidos y ataques "al peso"".

## ATAQUES "AL PESO"

Ataques que son al peso son aquellos en los cuales se descubre una vulnerabilidad en un sistema en concreto, en un dispositivo que habitualmente está expuesto a Internet. Una vez encontrada la vulnerabilidad, el cibercriminal busca cuántas IPs españolas tienen este servicio expuesto y va probando para ver "cuáles caen". "En ese conjunto puede haber desde una empresa de 50.000 empleados como una mercería o una panadería, todos entran" de ahí que la típica frase "yo no tengo nada importante, para qué me van a atacar" no tenga validez.

"Lo que hacen en muchos casos (los cibercriminales) es identificar sistemas vulnerables o comprar credenciales en foros, markets de la deep web en los cuales, pagando módicos precios, como 10.000 dólares, compran un pack de 200 credenciales robadas que va probando hasta dar con alguna que le permite entrar en una empresa". Llegados a este punto la pregunta es, "¿el usuario con el que estoy dentro de la organización es administrador? En caso positivo podrán acceder a máquinas y recursos compartidos y exfiltrar toda la información. En caso negativo tendrán que intentar dumpear el proceso e intentar sacar credenciales almacenadas de diferentes usuarios en esos sistemas...Buscan los backups y se llevan puestas las copias de seguridad".

## MÁS VALE PREVENIR

Analizada la realidad ligada al ransomware que a día de hoy viven muchas empresas parece necesario prevenir, pero ¿cómo hacerlo? ¿cuál es la mejor prevención frente al ransomware? Para Lorenzo la clave está en varios puntos:

- Concienciación de empleados: "fortalecer la concienciación de los empleados puede hacer que cada uno de ellos contribuya a mejorar la seguridad. Hay que concienciar porque muchos ataques empiezan con un click. Para que no hagan, no descarguen, no bajen software pirata".
- Contar con una solución antimalware: "por si al empleado le da por no estar activo ese día y consciente de lo que tiene que pasar que haya un programita que, por lo menos, bloquee algunas de las acciones que pueda llevar a cabo y pongan en peligro a la empresa".
- Auditoría continua: "si tengo servicios expuestos una auditoría me lo dirá y me permitirá proteger todo aquello que sea un potencial punto de entrada".
- Cambios frecuentes de contraseñas: "Si hemos dicho que un atacante compra un pack de contraseñas que tiene 6 meses, si tú las cambias cada tres, las tuyas de ese pack no van a funcionar".
- Sistemas de autenticación fuerte: "para que, aunque la contraseña funcione, se base todo el acceso en algo en un usuario y contraseña únicamente".
- Copias de seguridad, pero no cualquier copia: "Por favor, un sistema de copias de seguridad que sea a prueba de ransomware".
- Después de un tren puede venir otro: "cuidado con sentirse seguro después de haber "sobrevivido" a un ataque de ransomware porque puede venir otro detrás". ■

## CONTENIDO RELACIONADO

Las empresas españolas sufren más ataques de ransomware, pero pagan menos rescates

# El 93% de las organizaciones admiten que les resulta difícil llevar a cabo tareas esenciales de seguridad

## Actúe contra las amenazas con un servicio gestionado de expertos


## Sophos Managed Detection and Response

Sophos MDR es un servicio de seguridad gestionada que se adapta a sus necesidades y le permite alcanzar sus objetivos de seguridad y empresariales, compatible con las herramientas de ciberseguridad que ya tiene.
**Más información en: es.sophos.com/mdr**



SOPHOS

230606 ES [PC]

# GESTIÓN DE LA EXPOSICIÓN A AMENAZAS: EVOLUCIONANDO LOS PLANES DE PROTECCIÓN

A DÍA DE HOY, LAS ORGANIZACIONES PASAN POR ALTO MÁS DEL 60% DE LAS AMENAZAS DE SEGURIDAD SIN SIQUIERA SABERLO. CONTAR CON TECNOLOGÍAS COMO EDR, GESTIÓN AUTOMÁTICA DE INSTALACIÓN DE PARCHES O MFA ES VITAL PARA MINIMIZAR LA SUPERFICIE DE ATAQUE DEPENDIENDO DE LA EMPRESA, PERO NO VALE SOLO CON INVERTIR EN TECNOLOGÍA. GESTIONAR LA EXPOSICIÓN A AMENAZAS ES HOY UNA MISIÓN COMPLEJA Y QUE HA DE TOMARSE EN SERIO SI QUIERE CONSEGUIRSE UNA CIBERSEGURIDAD REAL.

Analizamos, de la mano mano de ISEMAREN, PRISA MEDIA, ALLFUNDS, BROSETA ABOGADOS, IBERDROLA ESPAÑA, SP GROUP, con la colaboración de ESET y TREND MICRO, el papel de las amenazas en la estrategia de ciberseguridad de las organizaciones.


**“El trabajo que estamos haciendo todos los CISOS de un tiempo a esta parte está mejorando mucho y se nos está reconociendo”**
Javier Torres Alonso, CISO de **Allfunds**


**“La clave en los próximos años va a ser la resiliencia colectiva”**
Manuel Asenjo, Director de Tecnologías de la Información, **Broseta Abogados**

Los ciberdelincuentes están en constante cambio y, si queremos seguirles el ritmo, los planes de protección han de evolucionar rápidamente. Los nuevos modelos de protección de la empresa global incluyen ahora la gestión de la exposición a amenazas y es por eso que el segundo panel de expertos de la V edición del Foro IT Digital Security: Nuevos modelos de ciberseguridad para proteger a la empresa global se centró, precisamente, en este punto. Para hablar sobre esta problemática contamos con la participación de responsables de seguridad de **Allfunds, Broseta Abogados, Iberdrola, Isemaren, SP Group** y **Prisa Media** quienes tuvieron la oportunidad de conocer la propuesta de valor de **ESET** y **Trend Micro** para hacer frente a sus problemas.

Y es que, hablar de gestión de amenazas es hablar de negocio, de formación y riesgos. La mejor forma de protegerse es, para Javier Luque Díaz, CISO de SP Group, conocer tu negocio “es fundamental saber qué tienes para poder protegerte”. De la misma opinión se mostró Rafa Tenorio Fuentes, CISO de Iberdrola España, para el que “conocer en qué escenario te encuentras, qué amenazas se pueden plantear en ese escenario, qué actores y qué intereses tienen es la única manera de poder hacerles frente”.

Javier Torres Alonso, CISO de Allfunds, fue más allá al afirmar que no vale con conocerse a sí mismo, también es necesario “llevar a cabo un buen análisis de nuestros proveedores porque podemos llegar a tener amenazas ocultas”.

Por su parte, Manuel Asenjo, director de Tecnologías de la Información de Broseta abogados reconoció que “no podemos hacer frente en casa a todas las herramientas, a todas las amenazas” por lo que para él, la mejor solución es “confiar en una empresa de ciberseguridad, con un servicio 24x7x365, y que ellos se encarguen con personal muy especializado de proteger y, sobre todo, de informarnos y decirnos dónde estamos flaqueando”.

Para Jesús Valverde Romero, IT Manager & CISO de Isemaren el principal problema es que “los riesgos son infinitos y el presupuesto es finito” por eso hay que ser consciente de que “las amenazas cambian cada día, evidentemente vas a tener mayor o menor exposición por lo que lo importante es conocerlo y gestionarlo, que no caiga en el olvido. Restringir los accesos que no son necesarios, restringir a los permisos a los mínimos que se necesitan para hacer una actividad... En definitiva, saber lo que tienes, dónde lo tienes y que está protegido”.

Jorge Tomé Hernando, director de Ciberseguridad y Continuidad de Negocio de Prisa Media, quiso mostrarse positivo al afirmar

**“Los riesgos son infinitos y el presupuesto es finito”**
Jesús Valverde Romero,
IT Manager & CISO de **Isemaren**


**“La seguridad no es solo papel del CISO o del CIO, es algo de todos”**
Javier Luque Díaz, CISO de **SP Group**

que, obviamente, “las amenazas, requieren una gestión. Esa gestión, como toda la gestión, requiere paciencia, requiere buen humor, requiere alegría, requiere equipo y requiere proceso”. A lo que añadió: “La gestión de la ciberseguridad no es un proceso complejo, de hecho, es un proceso, intrínsecamente, bastante simple, con tres pasos muy básicos, que es defensa, vigilancia y respuesta”.

De la misma opinión se mostraba el responsable de ciberseguridad de SP Group quien reconocía que la industria necesita “pasar de un enfoque meramente reactivo a uno proactivo”. Y esa proactividad empieza por que “todos los usuarios tienen que estar formados… La seguridad no es solo papel del CISO o del CIO, es algo de todos”. Para Javier de SP Group “Sí, al final la clave es intentar hacer del eslabón más débil, el eslabón más fuerte.”

## EL PERÍMETRO, ¿DIFUMINADO, DISPERSO, INEXISTENTE?

Hablar de amenazas es sin duda hablar de perímetro ¿o ya no? Precisamente de esta realidad cambiante hablamos con los responsables presentes en el panel y es que, para muchos, el perímetro “ha muerto” pero ésta no es una opinión homogénea pues son igual de numerosos los expertos que a apuntan a que el perímetro sigue existiendo solo que se ha difuminado, se encuentra disperso y abarca mucho más allá de la sede de la empresa. Ésta es justamente la opinión del responsable de la seguridad de Prisa Media quien cree que “El perímetro de amenazas es similar a lo que ocurre con los topógrafos cuando hacen mapas. En un mapa la línea de costa está muy clara pero cuando vas a la playa no parece tan fácil porque las cosas se mueven” explicaba. Para Jorge, “El perímetro es muy fácil. Está donde están tus datos y tus dispositivos. Por eso, antes tus datos y tus dispositivos estaban cerquita y agrupados, ahora los tienes distribuidos. Pero el perímetro no ha cambiado, el perímetro son mis equipos, mis usuarios y mis datos”.

Manuel de Broseta abogados recogía este símil para explicar que “la marea sube y baja por eso tenemos que adaptarnos a las nuevas amenazas, tenemos que adaptarnos a las nuevas capacidades que tienen los equipos y no tirar la toalla”.

## EL ATAQUE VA A LLEGAR

Si en algo coincidieron todos los participantes del debate fue en que el ataque, antes o después, llegará. “Los incidentes van a ocurrir, te va a pasar, tienes que estar preparado porque por mucho que tengas todos los mecanismos: un buen análisis de riesgo,


**“El perímetro es muy fácil. Está donde están tus datos y tus dispositivos”**
Jorge Tomé Hernando, Director de Ciberseguridad y Continuidad de Negocio de **Prisa Media**

una buena normativa, una buena cultura… al final te va a ocurrir y te vas a tener que remangar, ponerte operativo y responder” apuntaban desde Iberdrola. Por eso, para el responsable de Isemaren hay que tener planes de respuesta y, sobre todo “probarlos” porque “cuando pase algo va a sonar tu teléfono y tienes que saber por dónde tirar. Cada segundo que pierdes puede ser más complejo recuperar la actividad de tu empresa”. “Esa resiliencia es lo que te va a permitir levantarte al día siguiente” añadían desde Prisa. A lo que desde Broseta abogados agregaba: “resiliencia colectiva, creo que va a ser clave en los próximos años. Entre todos vamos a tener que juntar fuerzas y ser capaces de responder y poder recuperaros ante un ataque y ayudar al resto”. Lo mismo exponían desde Isemaren al admitir que: “la colaboración que hay entre nosotros, entre los diferentes responsables de seguridad, en los foros en los que al final todos estamos, nos ayuda mucho a aprender de aquello que todavía no nos ha ocurrido”. Un argumentario que Jorge de Prisa Media concluía con un consejo: “hay que estar con los ojos abiertos. Es muy importante que los que estamos en el lado del dolor lo llevemos con resignación y hablemos y colaboremos, porque al final somos un frente común frente a los malos”.

Para terminar con un punto positivo, desde Allfunds apuntaban a que “el trabajo que estamos haciendo todos los CISOS de un tiempo a esta parte está mejorando mucho, se nos está reconociendo también bastante y creo que los fabricantes están dándonos también esas mejoras tecnológicas que necesitamos para proteger nuestra información”.

## LA RESPUESTA DE LA INDUSTRIA

Precisamente para conocer la oferta de los proveedores del sector, aquellos que, con su tecnología, ayudan a mejorar la seguridad de las empresas y su protección frente a las cambiantes y temidas amenazas. Por eso, para finalizar el debate quisimos conocer cómo dos fabricantes de la industria pueden ayudar en esta gestión de las amenazas.


**“Las dos patas de la ciberseguridad a día de hoy son la tecnología y el talento. Hay que basarse en herramientas y especialistas para mejorar la protección”**
Carlos Tortosa,
Director de Grandes Cuentas España de **ESET**

Carlos Tortosa, Director de Grandes Cuentas para España de ESET fue el encargado de mostrar las capacidades de ESET para paliar estos problemas y resumió su potencial en 2 patas: “tecnología y talento, eso que tanto nos está costando a todos conseguir. Y es que, para Carlos hay que contar con tecnologías XDR, EDR, MDR, etcétera para que la amenaza en un principio no nos lle-


**“Desde Trend Micro, ofrecemos plataformas que se alimentan de cualquier solución, que te permiten medir y reducir tu ventana de exposición y tu nivel de riesgo en el tiempo”**
Raúl Guillén, Cibersecurity Strategy Director de **Trend Micro**

gue, es decir, no llegue a amenazarnos de verdad”. A lo que añadía: “nosotros, como proveedor de la Unión Europea, intentamos facilitar que estas herramientas sean de calidad, que sean certificadas a nivel europeo, para que puedan ayudar realmente en esta protección. Y después con las mismas herramientas intentar analizar qué es lo que nos ha pasado, sobre todo para que no nos vuelva a pasar, en caso de accidente”. Pues, como expuso el portavoz de ESET: “siempre pueden encontrar un hueco por el que entrar”. Por eso, terminaba: “tenemos que basarnos en herramientas y especialistas, en empresas, proveedores capaces de ofrecer estos servicios de monitorización, de recuperación de negocio… para estar preparados y saber responder en caso de ciberataque”.

Por su parte, Raúl Guillén, Cibersecurity Strategy Director de TREND MICRO para España resumió que la principal tarea de Trend Micro es “ayudar a los clientes a medir su nivel de riesgo durante el tiempo, no en un momento puntual”. Al final, añadía, “hemos hablado de múltiples vectores, de Cloud híbrida, de convergencia IT-OT, del perímetro y la identidad del usuario…todo esto evidentemente son múltiples puntos de entrada. Por eso nuestro esfuerzo está enfocado en medir ese nivel de riesgo y analizarlo durante el tiempo para que, en base a orquestación, plataformas y automatización se puedan llevar a cabo respuestas”. “Los fabricantes tenemos una obligación y es hablar entre nosotros” exponía, para después explicar que “estaría encantado de que compréis todos los productos de Trend Mi-

cro, pero eso no va a ocurrir, o raramente va a ocurrir. Entonces debemos tener mecanismos para colaborar entre los fabricantes, escuchando a los clientes, para alimentar de la mejor manera las soluciones y hacer un playbook dinámico para modificar la configuración en tiempo real. Y eso es lo que hacemos desde Trend Micro, ofrecemos plataformas que se alimentan de cualquier solución, que te permiten medir y reducir tu ventana de exposición y tu nivel de riesgo en el tiempo".

Si algo quedó claro durante el debate es que se necesita colaboración y Raúl no quiso dejar pasar este mensaje por alto, al que quiso poner la guinda: "Como fabricantes creo que tenemos la obligación de intentar simplificar los procesos para hacer más cosas y siempre desde un punto de vista colaborativo. Es fundamental colaborar con fuerzas y corporaciones de Estado, instituciones, con el CNI, con INCIBE, con el esquema nacional de seguridad porque hay que adaptar las soluciones globales a las problemáticas locales".

Simplicidad y colaboración son dos de las grandes necesidades del sector. Está claro que los cibercriminales aprovechan de forma habitual cualquier tipo de vulnerabilidad o fallo por lo que es cada vez más necesario realizar un mantenimiento regular de la infraestructura, parcheado y pruebas de penetración para comprobar que todo sigue funcionando correctamente a pesar de la cantidad de ataques que surgen cada día y las diferentes vulnerabilidades que se van encontrando paulatinamente.

A medida que el ciberespacio, la infraestructura de red y la cadena de suministro se han convertido en objetivos principales para los cibercriminales, tener en cuenta estos pasos puede ayudar a las empresas y organizaciones a garantizar, no una seguridad 100%, pero sí, que se ha hecho todo lo posible para proteger los activos, tangibles o intangibles, de la empresa, lo que a su vez puede evitar sanciones por parte de los organismos reguladores. ■

## CONTENIDO RELACIONADO

Informe sobre la cibercriminalidad en España 2022 (interior.gob.es)

ENISA Threat Landscape 2023 — ENISA

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

DESCÁRGUELO AHORA EN:
SONICWALL.COM/THREATREPORT

# 2023

# INFORME DE CIBERAMENAZAS DE SONICWALL

EL CAMBIANTE PANORAMA DEL CIBERCRIMEN

SONICWALL®

sonicwall.com | @SonicwallSpain

## PEDRO JORGE VIANA, HEAD OF PRESALES IBERIA DE KASPERSKY

# OPTIMUM SECURITY: COMBATIR AMENAZAS EVASIVAS

Existen en el sector multitud de tecnologías que pueden ayudar a mejorar la protección frente a amenazas de las empresas. Durante la celebración de la la V edición del Foro IT Digital Security: Nuevos modelos de ciberseguridad para proteger a la empresa global pudimos conocer la apuesta de Kaspersky para combatir amenazas evasivas de la mano de Pedro Jorge Viana, Head of Presales Iberia para la compañía.

En su ponencia, el directivo se centró en Optimum Security pero, para empezar su ponencia quiso exponer, primeramente, lo que puede llegar a costar llevar a cabo un ataque. Y es que, tal y como explicó: "unas credenciales de RDP, por ejemplo, pueden costar desde 0 euros hasta 5000 euros o 5000 dólares. Algún tipo de malware, lo podemos comprar por 10 dólares, más 3 o 5 dólares la guía de uso de ese malware" con lo que está claro que perpetrar un ataque es cada vez más sencillo, pero también más barato.


**Optimum Security: combatir amenazas evasivas. Pedro Jorge Viana, Kaspersky.**

Una vez conocida parte de la dinámica que se da para desde el lado del atacante, tocaba conocer las consecuencias que pueden darse para la víctima. Pedro Jorge compartío algunos datos como que "el 64% de las mayores amenazas de las víctimas han sido afectadas por ransomware, y les piden 2, 5, 10, 15 millones por el rescate". Si tenemos en cuenta que el coste de un ataque no se calcula exclusivamente para la parada de negocio, "sino teniendo en cuenta todo lo que se deriva de la parada de negocio y de este ataque, como puede ser, por ejemplo, la

contratación de profesionales externos para la respuesta a incidentes, la mejora de la infraestructura, cambio de cualquier tipo de arquitectura necesaria para mejorar la ciberseguridad de la empresa e incluso penalizaciones o multas por quiebra de contrato, subida de prima de seguro o incumplimiento de normativas, veremos que hay muchas empresas en nuestro mercado que tendrían un grave problema para la continuidad de su negocio en caso de sufrir un ataque de esas características".

¿Cuáles son las maneras de combatir este tipo de ataques? Para Kaspersky lo primero es "reducir la superficie de ataque con diferentes tipos de tecnología" lo que incluye: "adaptative anomalies control, control de aplicaciones, control de dispositivos, control de la navegación web, protección del correo electrónico..." para después centrarnos en "la prevención automática, que conseguiríamos utilizando diferentes métodos para mejorar, con detección automática, Machine Learning o análisis de comportamiento, la protección frente a esas amenazas en su estado más latente". Posteriormente, el portavoz de Kaspersky recomienda "la utilización de una solución de R&R, en caso de que queramos, el servicio más avanzado de gestión 24x7". Y, por último, "la formación de nuestros empleados pues la concienciación en ciberseguridad es clave para aumentar nuestro nivel de ciberseguridad de una forma global. Y no porque el último eslabón sea el más débil, como mucha gente indica hoy en día, sino porque es el eslabón más importante de toda la cadena".

El caso de uso con Kaspersky Optimum Security abarca tres procesos: una fase de intrusión "donde el usuario recibe un phishing por correo electrónico y ejecuta el fichero", una segunda que englobaría "el proceso de instalación, ejecución y comunicación en el que se comunicaría con servidores de common control" y posteriormente "la persistencia en la que el atacante consigue mantener el acceso a la infraestructura de la víctima" explicaba Pedro Jorge. Para, inmediatamente después, desarrollar el funcionamiento de la solución del gigante ruso basada en SaaS que proporciona detección avanzada, búsqueda de amenazas automatizada y administrada con el respaldo de los expertos de Kaspersky, y capacidades de respuesta guiada.

En palabras de Viana: "Kaspersky Optimum Security va desde la concienciación sobre la ciberseguridad para empleados a la reducción de la superficie de ataque pasando por la prevención automática de amenazas con mecanismos de detección avanzados para que trabajen el proceso de instalación y persistencia. Además, incluye la búsqueda con indicadores de ataque, con indicadores de compromiso por si tenemos la amenaza latente en la infraestructura del cliente y el escenario de respuesta automatizada guiada y remota 24 por 7, lo que viene a ser un MDR en todo su conjunto". Así mismo, "a nivel de producto, "Kaspersky Security Awareness, nuestro EDR óptimo trabajaría en toda la parte de protección, incluyendo los mecanismos de detección con tecnologías avanzadas, las búsquedas de IOA y la monitorización continua de la carga y detección de IOCs y causa raíz. Por último, ofrecemos un escenario de respuesta consolidada, unificada y guiada se haría mediante la combinación del EDR óptimo con el MDR óptimo". Con lo que, resumiendo, Kaspersky Optimum Security ofrece la posibilidad de, con una única solución, englobar la "concienciación, protección del endpoint y gestión centralizada de toda la arquitectura de ciberseguridad". ■

## CONTENIDO RELACIONADO

Kaspersky Optimum Security

TREND MICRO™ | Global Leader in Cybersecurity

# DETECTA CON PRECISIÓN, RESPONDE CON RAPIDEZ

## Experimenta la plataforma **Trend Vision One™**

Detén más rápido a los adversarios y toma el control del riesgo cibernético con una sola plataforma.

**trendmicro.com**

MARIO VELARDE, EX-DIRECTIVO DEL MERCADO DE LA CIBERSEGURIDAD

# "LA PROLIFERACIÓN DE PLAYERS NO ES ALGO NUEVO, LA INDUSTRIA DE LA CIBERSEGURIDAD VIENE MANTENIENDO E INCLUSO INCREMENTANDO EL DINAMISMO DESDE SUS INICIOS"

La industria de la ciberseguridad no ha parado su evolución desde que surgiera a mediados de los años 90 del siglo pasado. En un entorno en que hemos pasado de una ciberdelincuencia prácticamente anecdótica, donde los sistemas de información carecían de seguridad más allá de una rudimentaria protección de los equipos físicos en los que se sustentaba a infraestructuras dispersas y dinámicas que necesitan de una protección robusta para hacer frente a los cada vez más numerosos y sofisticados ataques, no es de extrañar que la evolución del sector haya sido exponencial.

Para conocer cómo han cambiado las cosas en estos últimos años y qué podemos esperar a futuro en la V edición del Foro IT Digital Security quisimos hablar con Mario Velarde, exdirectivo del sector y cuya larga experiencia


**Entrevista con Mario Velarde, ex-directivo de empresas de ciberseguridad TIC, durante la cual analizamos la marcha del mercado y sus propios desafíos.**

## “LA INDUSTRIA DE LA CIBERSEGURIDAD VIENE MANTENIENDO E INCLUSO INCREMENTANDO EL DINAMISMO DESDE SUS INICIOS”


profesional en diferentes organizaciones del sector de las nuevas tecnologías, en las cuales ha venido desempeñando diversos cargos de distinta índole hace de él un importante testigo de la evolución de la industria.

Durante la entrevista celebrada durante el evento, tuvimos la ocasión de hablar de una de las grandes características del sector: “el dinamismo”. Y es que, para Velarde, “no es algo nuevo, la industria de la ciberseguridad viene manteniendo e incluso incrementando el dinamismo desde sus inicios con la aparición de startups que han ido abordando los nuevos problemas que aparecían cuando surgían nuevas vulnerabilidades y amenazas”. Esta agilidad es algo intrínseco a nuestro sector, pero también algo “necesario” pues hace posible que las nuevas amenazas “puedan ser neutralizadas de manera más ágil y rápida”. Pero tiene consecuencias: “Esto ha dado lugar a un crecimiento exponencial del número empresas con tecnologías nuevas e innovadoras creando a lo largo de estas dos décadas del siglo XXI un ecosistema cada vez más grande” asegura el experto.

La proliferación de proveedores de ciberseguridad es un fenómeno en pleno auge. Llevamos años viendo como surgen nuevos jugadores que se unen al ya de por sí inmenso ecosistema existente. Sin embargo, lejos de pensar que este crecimiento desmesurado de players sería una rémora para su desarrollo futuro lo cierto es que aseguran el dinamismo necesario en el sector. Para Mario: “Una reducción drástica de players en este mercado seguramente llevaría a efectos indeseados de incremento de precios por falta de competencia y finalmente a modelos monopolísticos o pseudo-monopolisticos, lo que no sería la peor de las consecuencias ya que el sector perdería el dinamismo necesario para contrarrestar las nuevas amenazas

## “EL DINAMISMO ES NECESARIO PARA CONTRARRESTAR LAS NUEVAS AMENAZAS DE LA CIBERDELINCUENCIA”

de la ciberdelincuencia en tiempo y forma poniendo en mayor riesgo a las empresas usuarias de estas tecnologías y servicios”.

Y es que, el surgimiento de nuevos jugadores se explica, muchas veces, por el aumento de la inversión en ciberseguridad que ofrece una puerta de entrada para empresas muy especializadas. “Que muchas veces acaban en manos de los grandes gigantes tecnológicos” recuerda Mario -a lo que añade- “la adquisición de startups por parte de empresas más grandes supone la mejora de sus productos y servicios añadiendo estas tecnologías desa-

rrolladas fuera de sus propios departamentos de I+D. Las nuevas técnicas de ataque provocan el surgimiento de nuevos jugadores y su alto grado de tecnificación conllevan procesos de compra y consolidación que terminan por reducir efectivamente el número de players con lo que se asegura el dinamismo pero se mantiene el status quo dando lugar a un círculo virtuoso donde las nuevas ideas o iniciativas, en forma de respuestas a amenazas y vulnerabilidades producidas por cambios tecnológicos, como el almacenamiento y proceso en la nube o la Inteligencia Artificial, ayudan a mantener o mejorar el nivel de la Industria de la ciberseguridad".

Este dinamismo intrínseco que vive el sector desde su nacimiento es para muchos la única forma de mejorar el nivel de protección de forma constante, más si cabe en un sector en el que la falta de talento sigue siendo un hándicap insalvable. Sin embargo, si miramos desde fuera el panorama de la ciberseguridad, el gran número de soluciones disponibles en el mercado podría considerarse abrumador.

## ¿ES LA FRAGMENTACIÓN DEL SECTOR UN PROBLEMA PARA ALCANZAR LA SEGURIDAD REAL?

La fragmentación, excesiva para muchos, del mercado de la ciberseguridad supone

**"UNA REDUCCIÓN DRÁSTICA DE PLAYERS EN ESTE MERCADO SEGURAMENTE LLEVARÍA A EFECTOS INDESEADOS DE INCREMENTO DE PRECIOS POR FALTA DE COMPETENCIA"**

para Mario "una intensificación de la competencia" pero esto lejos de ser un problema "es un indicador del dinamismo que hay en esta industria y tiene la virtud de ofrecer muchos más matices a cada tipo de solución que permite que las empresas puedan encontrar el producto o servicio más adecuado a sus necesidades tanto desde el punto de vista tecnológico como del punto de vista económico". "La intensificación de la competencia hace que los actores en este mercado estén en un continuo proceso de mejora de la calidad de sus productos, así como de los precios que pueden ofrecer a sus clientes" sentencia el experto.

Definitivamente la de la ciberseguridad es una industria única, cambiante y apasionante para los que forman parte de ella. Está en pleno cambio y "seguirá así por mucho tiempo" vaticina Velarde, "es parte de su naturaleza". ■


## CONTENIDO RELACIONADO

Ciberseguridad: oportunidad en alza para emprendedores e inversores

Las partidas de ciberseguridad deberían aumentar un 40% para garantizar la protección empresarial

kaspersky 25 years

# Búsqueda proactiva de amenazas. Detección continua. Respuesta superior.

Protección óptima proporcionada por un partner de ciberseguridad.
Administrada para que usted no deba hacerlo.

Kaspersky Optimum Security

go.kaspersky.com/es_optimum

MARÍA RIESCO, JEFA DE GRUPO DE INVESTIGACIÓN CIBERAMENAZAS DEL MINISTERIO DEL INTERIOR Y DOCENTE DE CIBERSEGURIDAD

# "LAS ORGANIZACIONES CRIMINALES YA ESTÁN ESTRUCTURADAS COMO UNA INDUSTRIA ENTERA"

Toda protección empieza por una buena información, por una actualización constante. Por ello, conocer el estado de la ciberseguridad y cuáles son los ataques y técnicas más utilizadas por los cibercriminales es una de las mejores formas de protegerse frente a las amenazas. Precisamente con el objetivo de ahondar en el escenario actual de la ciberseguridad la última ponencia de la V edición del Foro IT Digital Security: Nuevos modelos de ciberseguridad para proteger a la empresa global se centró en este tema. En ella, de la mano de María Riesco, jefa de Grupo de investigación Ciberamenazas del Ministerio del Interior y docente de ciberseguridad conocemos el estado presente y futuro de la ciberseguridad.

Hablar de ciberseguridad es, a día de hoy, abarcar numerosos puntos de vista. "Por un lado, a nivel económico y geopolítico, nos encontramos con una situación de guerra híbrida, desde la agresión de Rusia a Ucra-


**Ciberseguridad, escenario presente y futuro. María Riesco, experta en ciberseguridad.**

nia, y cómo nos afecta ello como países de la OTAN".

Al mismo tiempo, "el cibercrimen sigue creciendo, porque sigue siendo muy rentable, y además estamos en un escenario de inestabilidad económica, con inflación, con una ralentización económica que hace que la gente busque dinero de forma fácil o de forma menos lícita" exponía María. A lo que le sumaba un elemento más: "Nos encontramos en un escenario de innovación tecnológica. Seguimos inmersos en esa transformación digital, en la era de la social information, pero este año ha habido un boom con la inteligencia artificial y está por venir el boom del quantum computing también o el 5G y el Internet de las Cosas que ya están aquí cada vez son más reales. Aunque, es verdad que el metaverso se ha abandonado un poquito, y que seguimos avanzando en la web 3 y en la descentralización de Internet". Todas estas novedades, continuaba explicando María "hacen que, al final, tengamos una superficie de exposición mucho mayor y que seamos más vulnerables".

## ¿QUÉ ESTÁN HACIENDO LAS AUTORIDADES?

Visto el panorama y su complejización parece vital que también avancemos en la protección. Por ello María quiso, aprovechando su labor como jefa de Grupo de investigación Ciberamenazas del Ministerio del Interior y su trabajo en la Policía Nacional, mostrar los avances que están llevando a cabo las autoridades. "Por un lado, avanzan en la regulación: este año ha sido publicada la NIS 2 junto con la directiva de resiliencia de entidades críticas y con Dora para el sector financiero. Y además se está trabajando ya en el reglamento de la ciberresiliencia que va a obligar a todos esos dispositivos que tengan conexión a internet a tener una certificación en ciberseguridad y unas prácticas mínimas de ciber higiene, que hagan que un producto sea mínimamente seguro". En definitiva, las autoridades siguen intentando "imponer obligaciones de ciberseguridad a las empresas y a sus productos para que todos estemos conectados de una manera mucho más segura". Y es que, "no vale con que solo las entidades más importantes tengan esa ciberseguridad, al final todos estamos interconectados y si atacan a una entidad que no esté protegida nos puede llegar a las demás". En Estados Unidos también "se está avanzando en la normativa CIRCIA, una normativa de reporte de incidentes que afecta a las entidades cotizadas".

> **"EL ESCENARIO DE CONFRONTACIÓN QUE TENEMOS A DÍA DE HOY HA HECHO QUE LOS PROPIOS GRUPOS CRIMINALES SE ATAQUEN ENTRE SÍ"**

## EL MERCADO SIGUE CRECIENDO

Por otro lado, "el mercado de la ciberseguridad todavía no llega su pleno potencial, podría crecer incluso a un ritmo del 13%, pero no hay capacidad de absorción tal en la industria porque seguimos contando con una gran falta de talento y de personal capacitado".

Si nos centramos en los ataques que más utilizan los cibercriminales hoy en día destacan: "el fraude económico o los ciberataques de tipo ransomware, que es la estrella de los ciberdelitos. El ransomware ha ido evolucionando, de ese cifrado y ese pago de rescate a una exfiltración y extorsión, no solamente por el descifrado, sino por la no publicación de datos o por la no publicación de esa brecha de seguridad". Esta triple o incluso cuádruple extorsión es cada vez más habitual y supone un riesgo aún mayor para las empresas.

Este escenario de confrontación que tenemos a día de hoy ha hecho que los propios grupos criminales, "se ataquen entre sí, revelando información de sus contrincantes".

Es algo que se está viendo sobre todo ligado a los conflictos bélicos: "gente que ha sido pro-Ucrania ha ayudado a destapar mucha información de organizaciones criminales prorrusas y gente pro-rusa ha ayudado a revelar información de organizaciones criminales pro-Ucrania. Esto nos ha permitido conocer cómo trabajan más en detalle". De hecho, estamos viendo que el cibercrimen va "hacia la comoditización, pero no solo de cibercrimen, en concreto del ransomware. Vemos mucho más ese cibercrimen como servicio o ese ransomware as a service, y cómo estas organizaciones criminales están estructuradas como una industria entera. Europol ha sacado recientemente un report completo de cómo trabajan estos grupos de cibercriminales en el que se ve cómo están organizados como si fueran una industria. Ellos prestan un servicio a sus clientes, grupos de criminales que contratan los servicios que necesitan" relataba María. Y explicaba: "Están organizados en capas, como cualquier industria. Tienen su grupo core, su grupo central, que está compuesto por senior managers y desarrolladores de backend; luego tienen la segunda capa, que ofrece los servicios dependiendo de dónde esté orientado el ataque; tienen pentesters, tienen developers, gente especializada en desencriptado, ingenieros de reversing, administradores de sistemas... incluso su propio departamento de recursos humanos, su propio equipo legal y negociadores de ransomware. Además, cuentan con su propio equipo de infraestructuras, todo aquello que sea necesario para llevar a cabo estas campañas de ransom y monetizarlas y para ello cuentan incluso con servicios de traducción. Están súper especializados, pero también el mismo problema que la industria de ciberseguridad: tienen necesidad de recursos y falta de talento; y por tanto ofrecen, por supuesto, muchísimo dinero si trabajas para ellos".

Precisamente con la intención de poder desenmascarar estas infraestructuras y detener a estos cibercriminales se están tomando medidas a nivel internacional "de forma muy estratégica" sentenciaba María y nos compartía algunos ejemplos: "se han hecho un montón de operaciones de éxito este año, a través de Europol, pero con colaboración internacional, con FBI, pero también con todo tipo de agencias. Y vemos que, muchas veces, estas organizaciones criminales están directamente financiados muchas veces por agencias de inteligencia, que también los utilizan para cometer ciberespionaje y para que estos bloques de confrontación geopolítica puedan avanzar en sus intereses haciendo ese uso de información confidencial. Todo se hace de manera coordinada y muy pensada, hay una estrategia muy sólida detrás".

Escuchando a María queda claro que el cibercrimen actualmente es una industria en sí misma, y muy rentable a nivel económico. Por eso hay que avanzar hacia "una colaboración público-privada a nivel nacional e internacional. Aquí solo hay dos ejes, los buenos y los malos, y debemos tener claro en qué ejes estamos, y trabajar y coordinar y cooperar mucho entre nosotros para poder desmantelar todas estas infraestructuras a nivel legal, a nivel tecnológico y poner también esas medidas legislativas y tecnológicas para intentar mantener nuestro ecosistema ciberseguro". ■

## CONTENIDO RELACIONADO

Serious and Organised Crime Threat Assessment (SOCTA)

SECURIZAME

# Black FRIDAY 23

# 25% DE DESCUENTO EN CURSOS ONLINE++

## HTTPS://CURSOS.SECURIZAME.COM

Válido del 24 al 27 de noviembre de 2023.
Consulta las bases de la promoción en https://www.securizame.com/blackfriday2023.
No aplicable con otras promociones y/o descuentos, ni en caso de bonificación FUNDAE.


# NUEVOS MODELOS DE CIBERSEGURIDAD

## PARA PROTEGER A LA EMPRESA GLOBAL


¡Ver todos los contenidos!

PATROCINADORES GOLD

PATROCINADOR SILVER