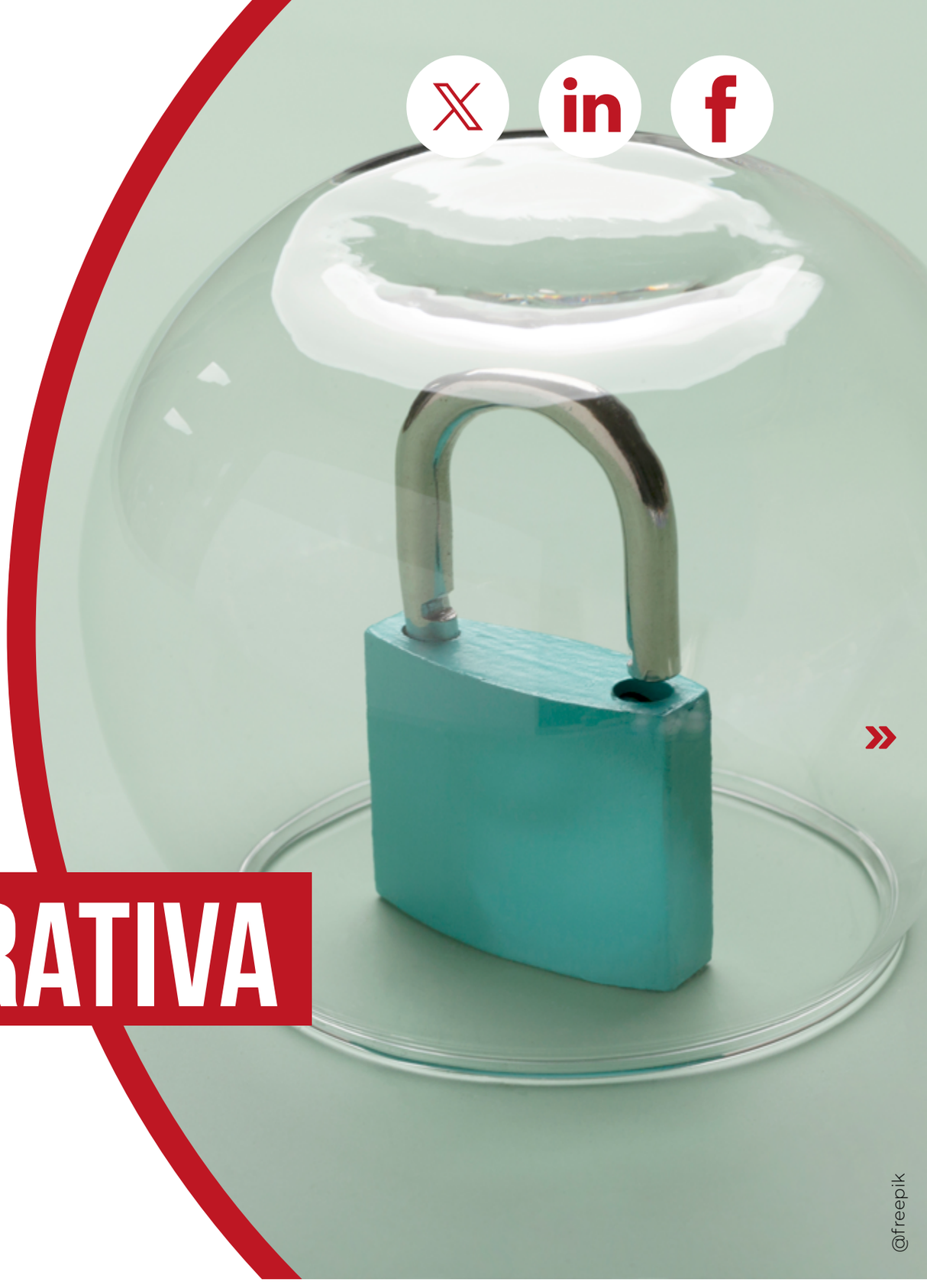
FORO it Digital Security

CONSOLIDANDO LA RESILIENCIA OPERATIVA



@freepik

ORGANIZA

it Digital MEDIA GROUP

PATROCINADORES GOLD

hp kaspersky motorola veeam

PATROCINADORES SILVER

Barracuda. SONICWALL Synology

COLABORA

CYBER MADRID laSalle UNIVERSIDAD RAMON LLULL

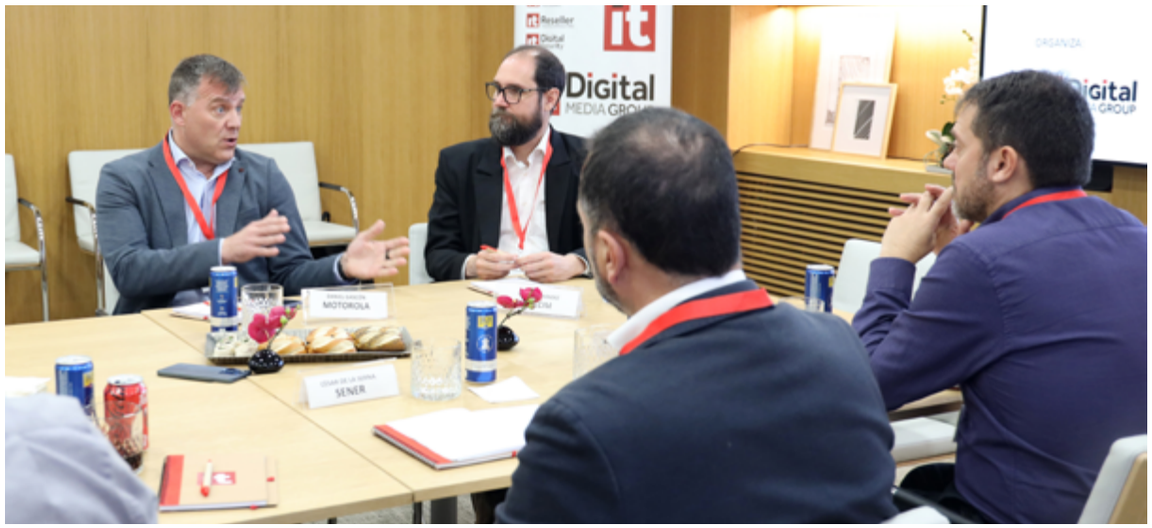
UNA TORMENTA PERFECTA PARA LA CIBERSEGURIDAD

EN LA X EDICIÓN DEL FORO DE IT DIGITAL SECURITY HEMOS VISTO CÓMO ORGANIZACIONES DE PERFILES MUY DIFERENTES AFRONTAN RETOS MUY SIMILARES, EN UN MOMENTO EN QUE LA PROTECCIÓN DEL ENDPOINT Y EL NUEVO PERÍMETRO DILUIDO Y LA CAPACIDAD DE RECUPERARSE TRAS UN CIBERATAQUE EXITOSO SE HAN CONVERTIDO EN ELEMENTOS FUNDAMENTALES DE LA SEGURIDAD CORPORATIVA.

Una digitalización acelerada que no ha dado tiempo al personal a interiorizar nuevos procesos laborales; la implantación de nuevos modelos de trabajo que incluyen constantes conexiones remotas; la multiplicación de los dispositivos conectados a las redes corporativas; el despliegue de la IA, en muchos casos con riesgos añadidos para la seguridad de los datos; la mayor sofisticación de las ciberamenazas y su constante aumento; una situación geopolítica que no para de tensarse...

Un combinado muy explosivo, una tormenta perfecta para la ciberseguridad.

En la X edición del Foro IT Digital Security, bajo el eslogan “Consolidando la resiliencia operativa”, hemos querido abordar la compleja situación de la ciberseguridad desde dos perspectivas. Por un lado, cómo se trabaja en la protección del endpoint con esa superficie ampliada y de perímetro diluido, en el observatorio “El endpoint y la



movilidad segura como piezas fundamentales de la resistencia digital". Por otro, cómo se aborda el elemento fundamental de las estrategias de seguridad corporativas, la ciberresiliencia, con el observatorio "Desde Zero Trust hasta los planes de recuperación: las claves de la ciberresiliencia".

LA CAPACIDAD PARA RECUPERARSE TRAS UN ATAQUE, FUNDAMENTAL PARA EL FUTURO

La ciberresiliencia es fundamental en una estrategia de ciberseguridad corporativa que parte de minimizar la posibilidad de que el ataque se produzca... Pero tiene un principio básico: esperar que, antes o después, un ciberataque tenga éxito. La adopción de la resiliencia cibernética depende de factores como el tamaño de la empresa, su sector o sus características propias, como el número de proveedores externos, la presencia de tecnología operativa o la cantidad de colaboradores que acceden a sus sistemas. Pero, en todos los casos, la ciberseguridad y la resiliencia han pasado a formar parte de los imprescindibles que permiten el crecimiento corporativo.

El cambio en las dinámicas de trabajo combina elementos como la IA, la digitalización y el trabajo a distancia, entrelazados entre sí y combinados con los desafíos propios de cada organización. La transformación de la superficie de ataque ha llevado a modelos de ciberseguridad corporativa en constante evolución, en paralelo a la transformación a largo plazo que está suponiendo la digitalización. El puesto de trabajo vive un proceso que no tiene vuelta atrás, en el que se intenta sacar el mayor partido a su propia evolución.

Además de los dos observatorios centrales de la jornada, el X Foro de IT Digital Security ha contado con entrevistas destacadas a Marc Rivero, coordinador del Máster de Ciberseguridad en La Salle; Viktor Kijaško, IT Resiliency director de DHL IT Services; César de la Serna, Cybersecurity lead de Dcode, área digital del grupo Sener; Modesto Álvarez, CISO en el Grupo TSK; y Virginia Vicente, manager de CyberMadrid.

Las presentaciones individuales del foro corrieron a cargo de Javier Sanz, presales manager de Kaspersky; Víctor Pérez de Mingo, presales manager de Veeam; Melchor Sanz, CTO de HP; Daniel Gascón, head of B2B en Motorola Iberia; Miguel López, regional sales director para el sur de Europa en Barracuda; Sergio Martínez, country manager para Iberia de SonicWall; y Tomás Saiz, business project manager para Iberia de Synology. ■

MÁS INFO +

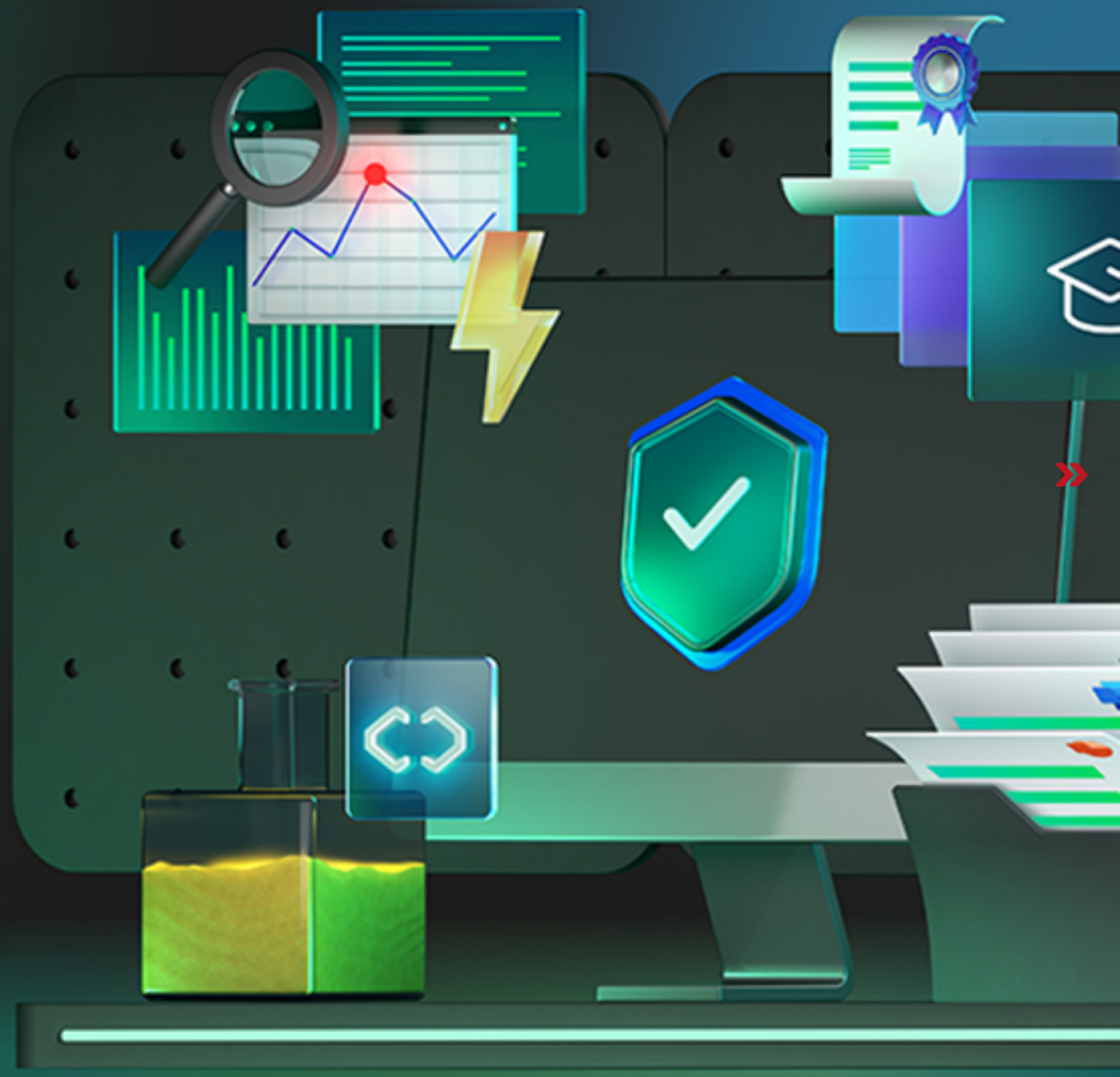
» X Foro de IT Digital Security: Consolidando la resiliencia operativa

Kaspersky Next
XDR Optimum

Amplía las capacidades, no los «presupuestos»

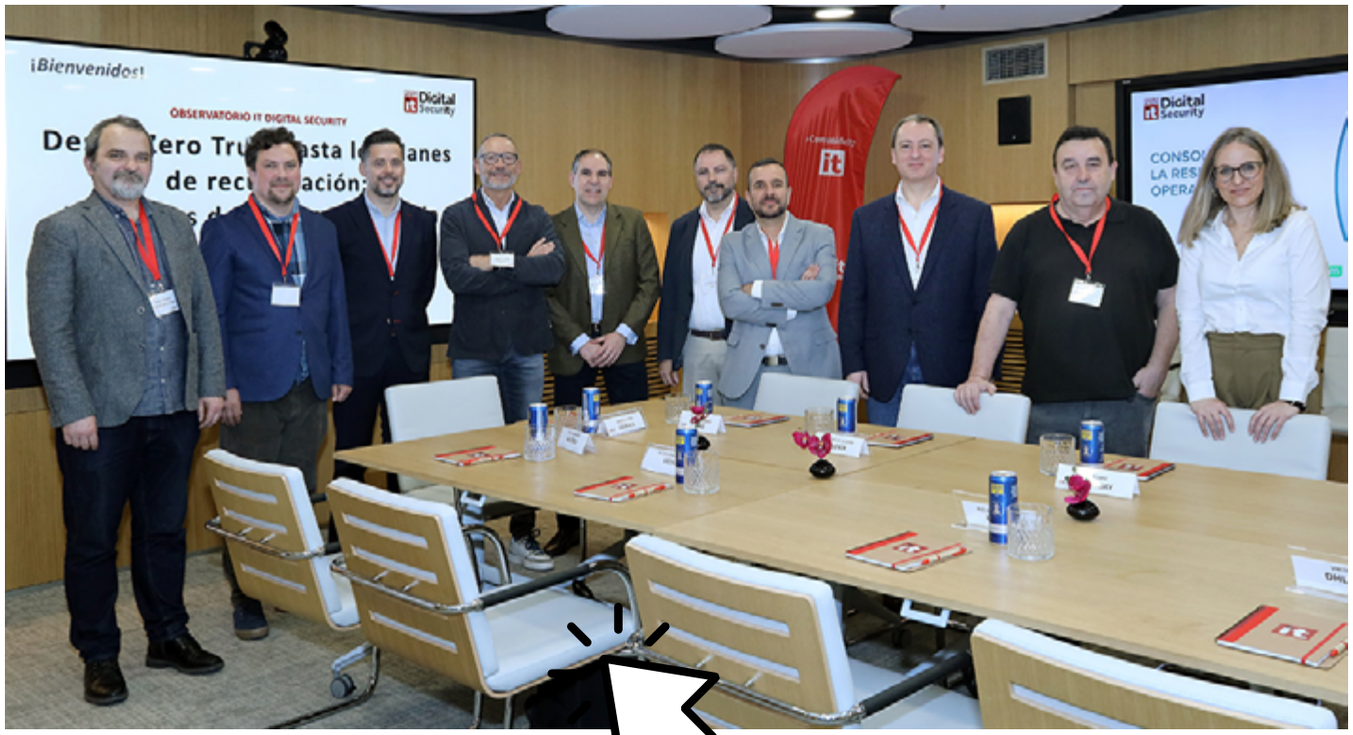
Mejora tu ciberseguridad con
Kaspersky Next XDR Optimum

kaspersky



Observatorio IT Digital Security

DESDE ZERO TRUST HASTA LOS PLANES DE RECUPERACIÓN: LAS CLAVES DE LA CIBERRESILIENCIA



Hablamos de cómo reforzar la capacidad de ciberresiliencia de las organizaciones, un elemento básico para su supervivencia en el contexto actual, con líderes de tecnología y ciberseguridad de **Ávoris, DHL IT Services, EADA Business School, Embou, Grupo TSK, MPO** y **Sener**, en un observatorio que ha contado también con la perspectiva de representantes de **Kaspersky** y **Veeam**.

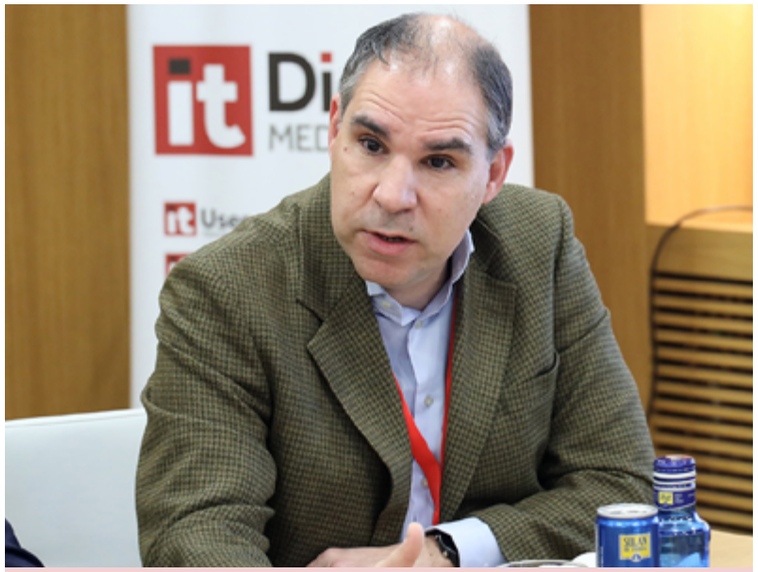
#FOROITDS

DESDE ZERO TRUST HASTA LOS PLANES DE RECUPERACIÓN: LAS CLAVES DE LA CIBERRESILIENCIA

CON CONSTANTES INCREMENTOS EN EL VOLUMEN DE LAS AMENAZAS, CON TIPOS DE ATAQUE CADA VEZ MÁS SOFISTICADOS Y TENSIONES GEOPOLÍTICAS QUE NO PARECE QUE VAYA A AMAINAR, LOS PLANES DE CIBERRESILIENCIA SE HAN EMPEZADO A INCORPORAR EN LAS POLÍTICAS CORPORATIVAS COMO UN ELEMENTO BÁSICO PARA LA ESTRATEGIA DE SUPERVIVENCIA Y DE CRECIMIENTO DE LAS EMPRESAS.

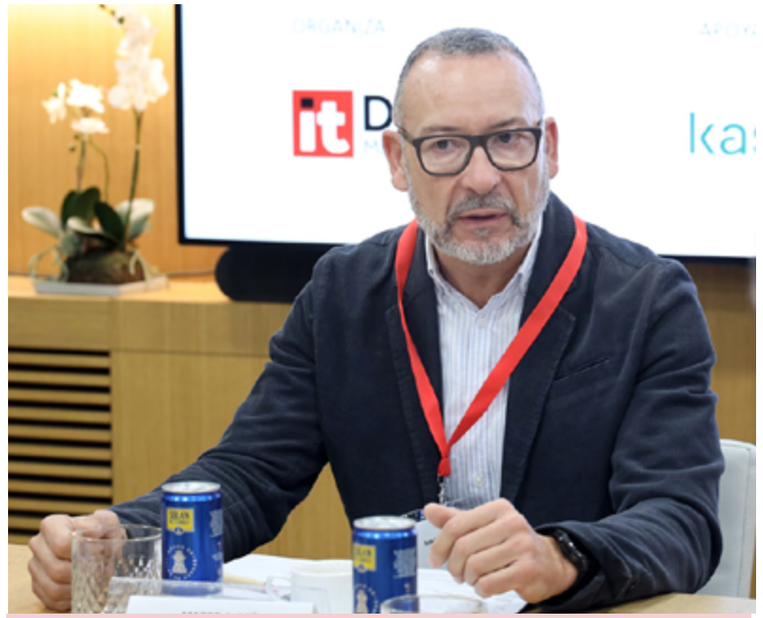
La capacidad de recuperarse tras un incidente de seguridad marca no solo la postura de seguridad de las empresas, sino su futuro. Según los datos del Instituto Nacional de Ciberseguridad (INCIBE), un 60% de las empresas de tamaño pequeño o mediano que sufre un incidente de seguridad grave se ve obligada a echar el cierre en los seis meses siguientes al ciberataque. Para una gran empresa, verse obligada a detener sus operaciones unos días o semana puede ser un golpe duro, pero para la mayor parte de las pymes es definitivo.

La ciberresiliencia es un concepto relativamente nuevo. Hay que tener en cuenta que la propia práctica de la ciberseguridad se ha transformado en la última década, en línea con la transformación de las empresas y los modelos de trabajo hacia entornos más fluidos y menos rígidos. Con muchas empresas digitalizadas, la resiliencia no tiene sentido



“La resiliencia y la continuidad de las operaciones no son una cuestión técnica sino estratégica, y deben estar lideradas desde negocio, conjuntamente con ciberseguridad”
Jesús Dorado, CISO, **Ávoris**

“En ciberresiliencia no todas las soluciones deben ser caras: hay que pensar cómo podemos ayudar con los recursos que hay”
Viktor Kijasko, IT Resiliency director, **DHL IT Services**



“Hay que trabajar mucho en la cultura de la ciberresiliencia para que sea una idea que se asimile y pueda nacer desde dentro”
Marco Peña, CIO, **EADA Business School**

sin la parte ciber y cada vez más compañías están avanzando hacia estrategias de resiliencia que contemplan la parte física y la lógica como un todo.

Como es habitual, el modo en que las compañías se van adaptando a estas nuevas realidades depende de los factores concretos en los que se desarrolla su actividad. En el primero de los observatorios del X Foro de IT Digital Security hemos podido hablar sobre los usos y las claves de la ciberresiliencia con representantes de **Ávoris**, **DHL IT Services**, **EADA Business School**, **Embou**, **Grupo TSK**, **MPO**, **Sener**, en una mesa redonda que ha contado con el apoyo de **Kaspersky** y **Veeam**.

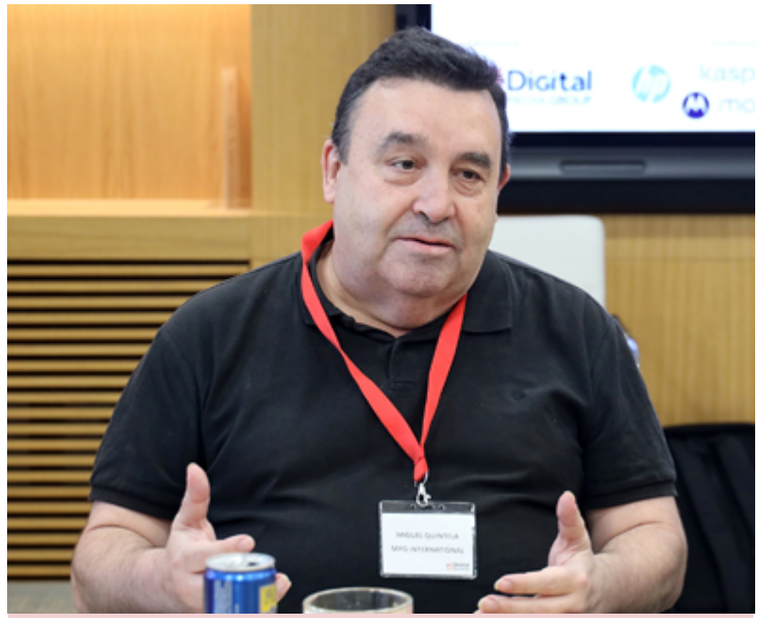
¡SIMULACROS, SIMULACROS, SIMULACROS!

Uno de los grandes consensos de la ciberseguridad es el de la formación. Una formación que tiene más sentido cuanto más práctica es. En el caso de la ciberresiliencia, los planes se tienen que poner a prueba con cierta frecuencia para asegurarse no solo de que funcionan los elementos técnicos, sino los procesos y el reparto de responsabilidades en caso de incidente. Por más claros que estén los conceptos sobre el papel, la realización de simulacros es un elemento básico que no puede faltar en la planificación de la resiliencia.

Javier Sanz, presales manager de Kaspersky, explica que “ya no hablamos de perímetro como hace algunos años, sino que hemos pasado a hablar de identidades. Creo que es fundamental involucrar al comité de dirección en toda la parte de seguridad para que sean conscientes del peligro que supone. No siempre somos capaces de aprender

“Los planes de recuperación y resiliencia son maravillosos sobre el papel, pero hay que probarlos recurrentemente para asegurarse de que no son papel mojado”
Alejandro Velilla, CTO, **Embou**

“Es mucho más difícil conseguir que se cambien procesos de negocio o la cultura de trabajo, que lograr mayores inversiones tecnológicas”
Modesto Álvarez, CISO, **Grupo TSK**



“Lo más importante para la ciberresiliencia es que el consejo de dirección se implique al 100%, tanto personal como económicamente”
Miguel Quintela, CIO/CISO, **MPO**

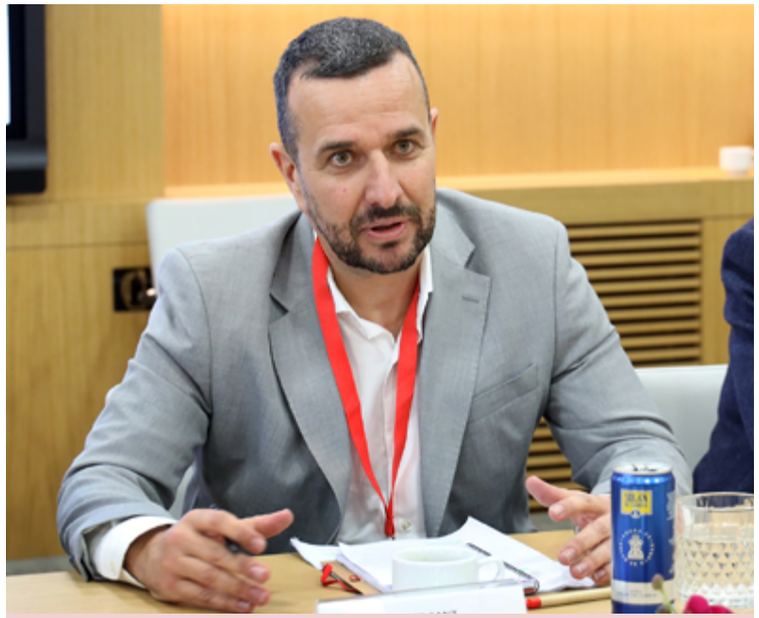
de situaciones que nos hemos encontrado. Nosotros realizamos simulacros en los que utilizamos casos reales que nos hemos encontrado en Kaspersky. Explicamos, entre otras cosas, cómo tienen que reaccionar. Llevamos los simulacros un poco al límite, apretando a nivel de tiempo y de todo lo que supone, involucrando a todos los equipos, desde el de marketing al de recursos humanos, obviamente a la parte de IT y seguridad. Pero no solo es cosa de tecnología: tu eslabón más débil es el usuario por falta de conocimiento. La concienciación es clave en temas como proteger el dato, las redes sociales, la detección de phishing o las passwords”.

Esos simulacros recurrentes permiten ver los puntos débiles que tienen los planes de ciberresiliencia. También permiten que los consejos de dirección entiendan los riesgos que pueden entrañar los ciberataques que tienen éxito y comprendan que una parte muy importante de la postura de seguridad es la capacidad de recuperarse que tenga la empresa. Una capacidad medible en elementos como el tiempo que puede estar con las operaciones detenidas o sin acceso a determinados datos o servicios. Pero lo que definitivamente contribuye a sensibilizar a una empresa es pasar por la mala experiencia de un ciberataque real.

LA CAPACIDAD DE SOBREVIVIR COMO CASO DE ÉXITO

Miguel Quintela, CIO y CISO de MPO, explicó el impacto que tuvo un ciberataque sobre su compañía en 2019: “Nosotros cambiamos nuestra mentalidad, como empresa, cuando sufrimos un ataque de

“En español, safety and security son lo mismo: un concepto muy bueno, porque la seguridad física y la lógica en estos momentos van de la mano”
César De la Serna Sánchez, Cybersecurity lead, **Dcode (Sener)**



“La seguridad perfecta no existe y seguramente no existirá nunca: lo que tienes al alcance es reducir la superficie de ataque a la que estás expuesto”
Javier Sanz, presales manager, **Kaspersky**

“Solos no podemos resolver nada, somos cada vez más conscientes de que todos necesitamos ayuda y es necesario hablar de ciberseguridad”
Víctor Pérez de Mingo, presales manager, **Veeam**

ransomware. Nos encriptaron todos los sistemas y nos pidieron rescate. Desde entonces hemos tomado conciencia y se ha trabajado mucho porque descubrimos que el plan de continuidad de negocio no funcionó correctamente. El ataque se inició por una factura que ni siquiera era de una empresa con la que trabajábamos. Un usuario abrió el fichero Excel por simple curiosidad. Llevaba una macro que se ejecutó y lo primero que hacía era preguntar si el teclado estaba en cirílico, porque los rusos no pueden atacar a empresas rusas. El ataque nos obligó a montar una empresa nueva, desde cero, en paralelo. Fue un mes y medio muy duro, pero logramos recuperar el 97% de toda la información y sistemas. Es de agradecer la colaboración y apoyo de todos los clientes durante el periodo de la reconstrucción de MPO”.Se trata, sin duda, de un caso de éxito. La compañía fue capaz de sobrevivir a un ataque muy duro gracias a su creatividad y desde entonces ha adquirido un nivel de madurez en ciberseguridad y resiliencia mucho mayor. El ransomware sigue siendo una de las principales amenazas para las empresas. Se va transformando, como todas las ciberamenazas, y va cambiando sus comportamientos, pero un tipo de ataque que no va a desaparecer.

La ciberresiliencia es fundamental en una estrategia de ciberseguridad que parte de minimizar la posibilidad de que el ataque se produzca. Marco Peña, CIO de EADA Business School, señala que, “aparte de proteger toda la parte de cloud, tenemos también mucha infraestructura on-premise. Estamos trabajando, por supuesto, en aportar todas las medidas técnicas posibles: protección

del endpoint, protección del correo electrónico, el firewall o el backup. Pero, sobre todo, estamos trabajando en la detección, en ganar visibilidad, en saber en un momento dado qué está pasando. Cuando pasa algo, cada segundo cuenta. Cuanto antes te des cuenta de que está pasando algo, mucho mejor. Entonces ese es el foco en el que estamos ahora. Pero, obviamente, eso es para luego generar el siguiente paso, que es cómo respondemos lo más rápidamente posible a cualquier eventualidad".

Víctor Pérez de Mingo, presales manager de Veeam, recuerda que "más del 30% de las compañías creen tener un nivel de ciberresiliencia mayor del que tienen. El desconocimiento es algo muy peligroso. La ciberseguridad efectivamente es un proceso de maduración. También se habla de detección temprana y de inmutabilidad. De hecho, una de las primeras cosas que suelen atacarnos es el backup, en el que además en muchos casos todavía no se encripta la información. Otra cosa en la que incidimos mucho es el entrenamiento. Los bomberos no se lanzan a apagar fuego sin haber tenido un entrenamiento previo: ellos entrenan con fuego real. Debemos intentar simular las condiciones de un ataque lo máximo posible. El mayor problema que hay, en todo caso, no es tecnológico, sino de personas, de organización. Y además la IA ha generado una superficie de exposición distinta y requiere una protección distinta. Necesitamos algo que sea capaz de ponerse en medio y revisar lo que hace la IA".

PRESENTACIÓN >> Javier Sanz, presales manager de Kaspersky, explica las capacidades de su solución de detección y respuesta gestionada y extendida. La propuesta de la compañía abarca desde la protección del endpoint hasta la concienciación y la formación de los equipos, reforzando la reducción de la superficie de ataque con el soporte del SOC de Kaspersky y sus motores de IA.

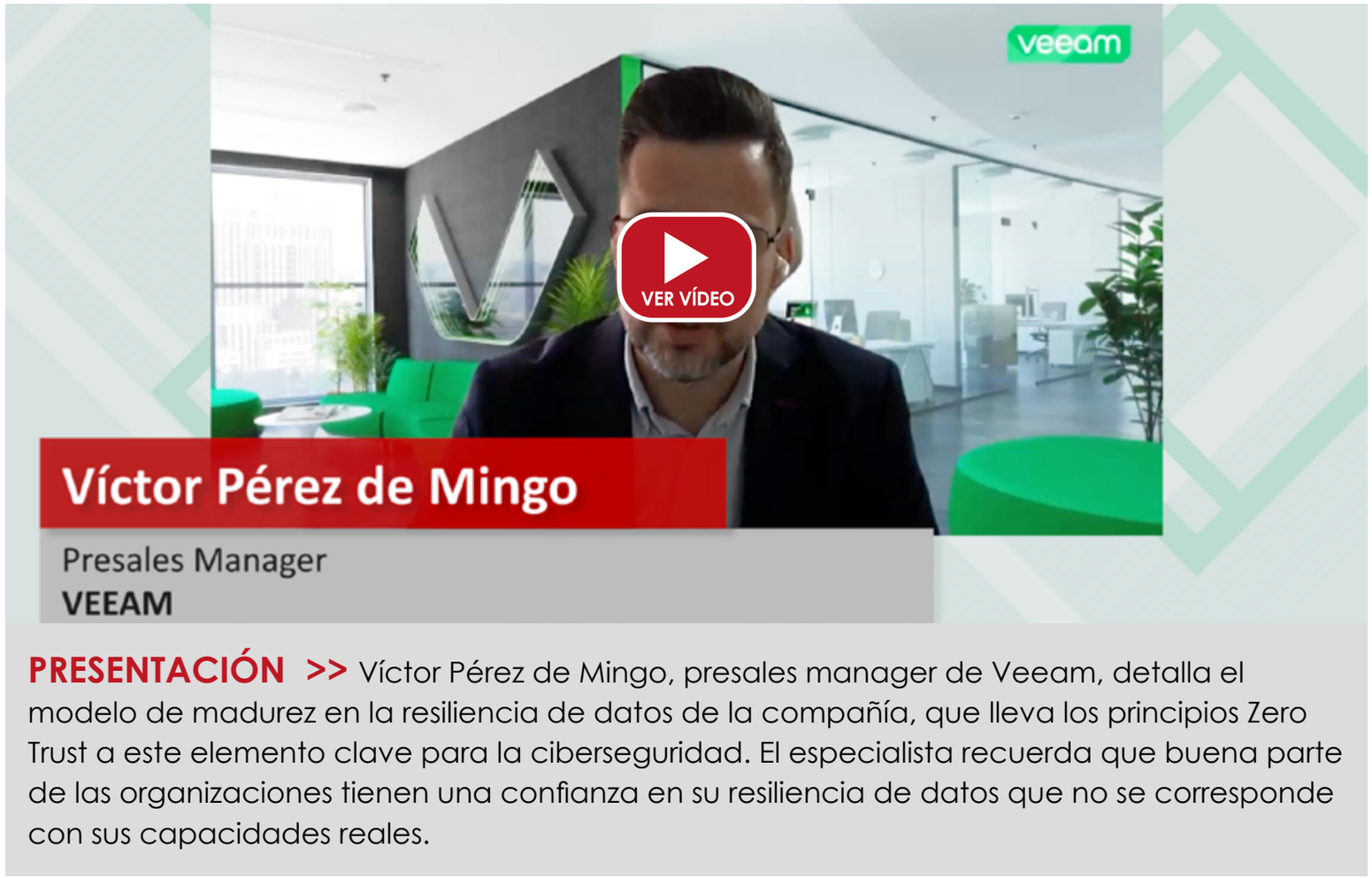
PREPARÁNDOSE PARA LA RESILIENCIA

Viktor Kijasko, IT Resiliency director en DHL IT Services, pone un ejemplo muy práctico del desarrollo de la resiliencia: "Tenemos un equipo dedicado a IT Resiliency y a la gestión de la continuidad de negocio. Con los servicios críticos de todo el grupo. Hemos empezado por identificar qué servicios son los más críticos que tenemos, 13 en total. Después, los equipos de operaciones hacen su Business Impact Analysis y definen qué necesitan para recuperar sus operaciones críticas. Tenemos miles de operaciones, pero no todas son críticas. ¿Qué necesitas recuperar? ¿En qué tiempo? ¿Cuál es el período máximo de caída? Si dicen que es necesario que una operación funcione, ¿qué sistemas críticos la soportan? Y, después, ¿cuáles son las dependen-

cias que tiene? Es difícil gestionar las instancias de automatización. Tienes algo pequeñito que, si no funciona y no se soporta, va a provocar que todo falle. Por eso hay que identificar las dependencias y las consecuencias de un fallo".

El modo en que se afronta la ciberresiliencia depende de factores como el tamaño de la empresa, el sector en el que trabaja y elementos que forman parte de su propia idiosincrasia, como el número de proveedores externos con el que trabaja, la presencia de tecnología operativa o la cantidad de colaboradores que acceden a sus sistemas. Pero, en todos los casos, la ciberseguridad y la resiliencia han pasado a formar parte de los imprescindibles que permiten el crecimiento corporativo.

Alejandro Velilla, CTO de Embou, explica que han vivido "una fase de crecimiento exponencial en la que hemos tenido que ir adaptándonos reactivamente a cómo ha ido el negocio. La parte de IT y de ciberseguridad son elementos muy importantes en el crecimiento, sobre todo cuando está basado tanto en el crecimiento orgánico de tus empresas como en la adquisición de otras que ya tienen un punto de madurez. Cada uno de los terrenos en los que nos metemos es una brecha potencial de seguridad, un nuevo desafío con un tercero. Con la fusión con Orange hemos pasado a una posición de ciberseguridad sólida, con un SOC muy potente. Algo muy importante para controlar y proteger la nueva barrera digital y la IA. No solo con las telecomunicaciones, sino con todas las verticales que tenemos en diferentes entornos, somos de las empresas que más clientes tienen en España. Y eso son datos que, al fin y al cabo, hay que proteger, pero que también se explotan".



PRESENTACIÓN >> Víctor Pérez de Mingo, presales manager de Veeam, detalla el modelo de madurez en la resiliencia de datos de la compañía, que lleva los principios Zero Trust a este elemento clave para la ciberseguridad. El especialista recuerda que buena parte de las organizaciones tienen una confianza en su resiliencia de datos que no se corresponde con sus capacidades reales.

Por su parte, Modesto Álvarez, CISO en Grupo TSK, señala que realizan "instalaciones industriales para los clientes, yendo desde el diseño hasta la puesta en marcha y entrega; y, a veces, seguimos con operación y mantenimiento. Tenemos la ventaja de que cada una es independiente respecto a las demás. Pero tenemos dos desafíos de cara a la ciberresiliencia: la visibilidad y la gestión del cambio. Trabajamos en diferentes países y hay diferentes legislaciones, diferentes aproximaciones normativas, diferentes culturas. Esto entra dentro de lo previsible, pero te encuentras también, en algunas ocasiones, con una visibilidad muy limitada de una sola parte. Y los problemas pueden venir de todas. Respecto a la gestión del cambio, creo que al final tiene que ver con per-

sonas y procesos, elementos más complicados que la propia tecnología".

César De la Serna Sanchez, Cybersecurity lead en Dcode, área digital del grupo Sener, explica que en su caso trabajan "principalmente en un mundo muy físico, donde nuestra mayor preocupación son tres elementos: primero las personas, luego los procesos y luego las tecnologías. Protegiendo las tres cosas estamos llegando a un ecosistema amplio, en el que la ciberseguridad parte desde el diseño, desde la concepción. Como ingeniería, nos gusta mucho el dato, nos gusta mucho recoger información para tratarla y buscar puntos de mejora. En el mundo de la ingeniería, antes se decía que, si funciona, no lo toques. Eso ya acabó. Ahora hay que preguntarse: ¿y es seguro? Tenemos unos programas de formación bastante potentes, también para el tema de la resiliencia. No solo los procesos de comunicación internos, sino también ejercicios de simulación de ataques por sector. Otra cosa que nos preocupa es la gestión de la cadena de suministro, porque no todo el mundo tiene la misma conciencia de la ciberseguridad".

UN BÁSICO PARA LA SUPERVIVENCIA

Sea cual sea el sector en el que se mueven las empresas, las interconexiones entre unas y otras son cada vez mayores. No es casualidad que una buena parte de los ciberataques exitosos de los últimos años se hayan generado en las cadenas de suministro. No es casualidad tampoco que las últimas normativas de ciberseguridad se hayan basado en una mejora de la postura de ciberresiliencia. Es el caso de DORA en el sector financiero y de NIS2 en muchos otros entornos.

Pero, por si fuera poco, además de estos marcos normativos en la Unión Europea tenemos la Ley de Ciberresiliencia. Entró en vigor a finales de 2024 y será obligatoria de forma general a finales de 2027, pero ya este año afectará a las obligaciones de información de los fabricantes y a los organismos de evaluación de conformidad, estableciendo unos requisitos de ciberseguridad obligatorios para todos los productos que tengan elementos digitales en su ciclo de vida. Estos marcos normativos en ocasiones se ven como punitivos, pero contribuyen a mejorar la postura de seguridad de todo el tejido productivo.

Jesús Dorado, CISO de Ávoris, recuerda que trabajan "en un amplio ámbito regulatorio, desde NIS2 o el Esquema Nacional de Seguridad hasta las directivas europeas en el ámbito de la seguridad operacional. Lo que intentamos es enfocar la ciberresiliencia y la confianza cero desde la perspectiva de la garantía de funcionamiento facilitando usabilidad y operativa. Para nosotros son muy importantes tanto ZTNA como la resiliencia activa que en conjunto permiten ofrecer al viajero una experiencia ágil, eficiencia y segura. Optamos por un enfoque integral de garantía de funcionamiento asumiendo que vamos en algún momento tendremos que asumir una disrupción para la que estaremos mejor preparados. En definitiva, lo enfocamos desde un punto de vista de negocio, de importancia de las operaciones para cada unidad, intentando homogeneizar las principales acciones de la continuidad de negocio. Y, dentro de esa continuidad, llevamos a cabo acciones tanto de concienciación como de sensibilización".

En 2025, INCIBE gestionó un 26% más de incidentes que el año anterior. Con la mejora de la IA y las tensiones geopolíticas no parece que el volumen de ciberamenazas vaya a disminuir. Solo queda adaptarse. Ya se sabe: no se trata de si te van a atacar sino de cuándo. O incluso de si ya lo han hecho y no te has dado cuenta. La ciberresiliencia es, simplemente, imprescindible para sobrevivir. ■

MÁS INFO +

» Cuándo actualizar de EDR a XDR

» Consolidar la resiliencia operativa: de Zero Trust a la recuperación cibernética

» Cómo anticipar los ciberataques del mañana con Inteligencia Contextual de Amenazas

» Modelo de Madurez de Resiliencia de Datos de Veeam (DRMM)

» Desarrollo de una estrategia de recuperación de datos ciberresiliente

¿No sabes qué hacer ante los desafíos de la protección de datos?

veeam

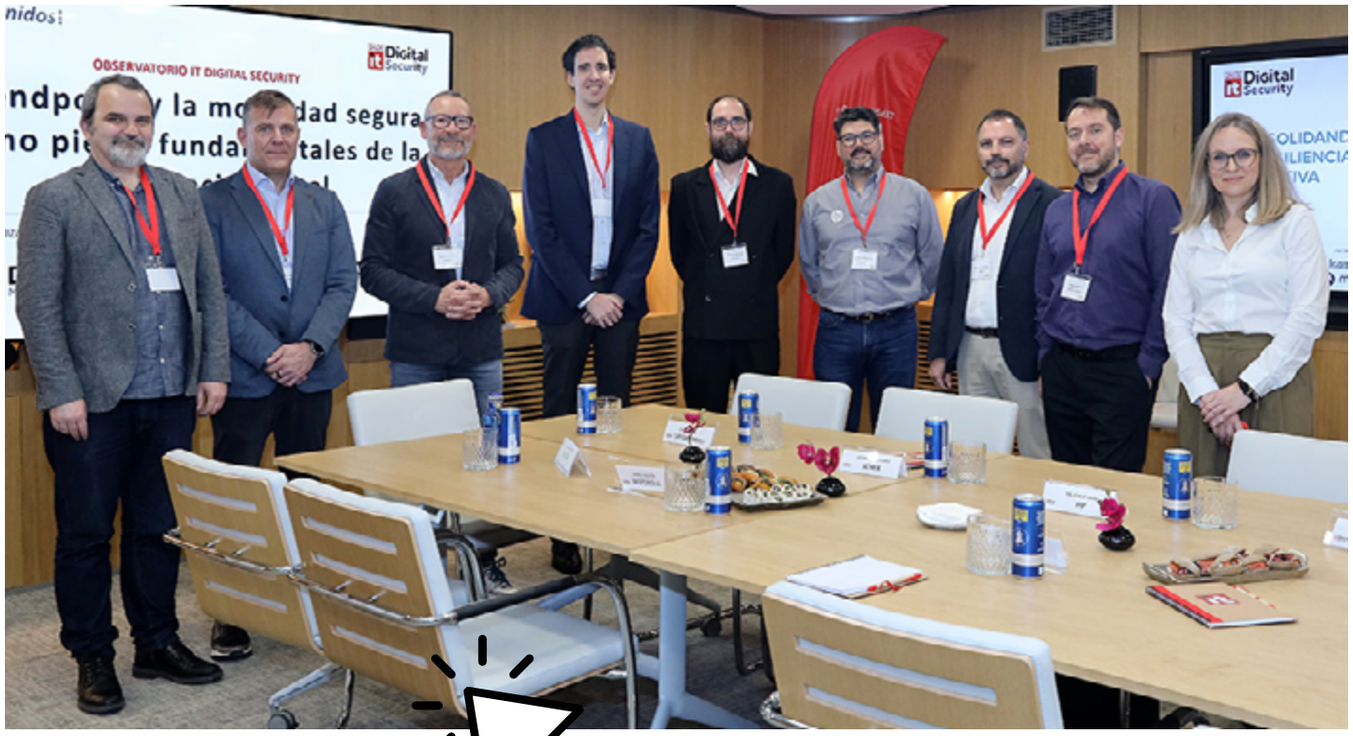
Descubre lo nuevo de Veeam Data Platform

Descargando la versión de prueba gratuita

Descarga Aquí

Observatorio IT Digital Security

EL ENDPOINT Y LA MOVILIDAD SEGURA COMO PIEZAS FUNDAMENTALES DE LA RESISTENCIA DIGITAL



Hemos querido conocer de primera mano cómo diferentes empresas afrontan el cambio en su perímetro de seguridad. Para ello hemos tenido ocasión de hablar sobre la transformación de la ciberseguridad corporativa con responsables de tecnología y ciberseguridad de **Capital Energy, EADA Business School, Embou, Holcim** y **Sener**, en un observatorio que ha contado con el apoyo de **HP** y **Motorola**.

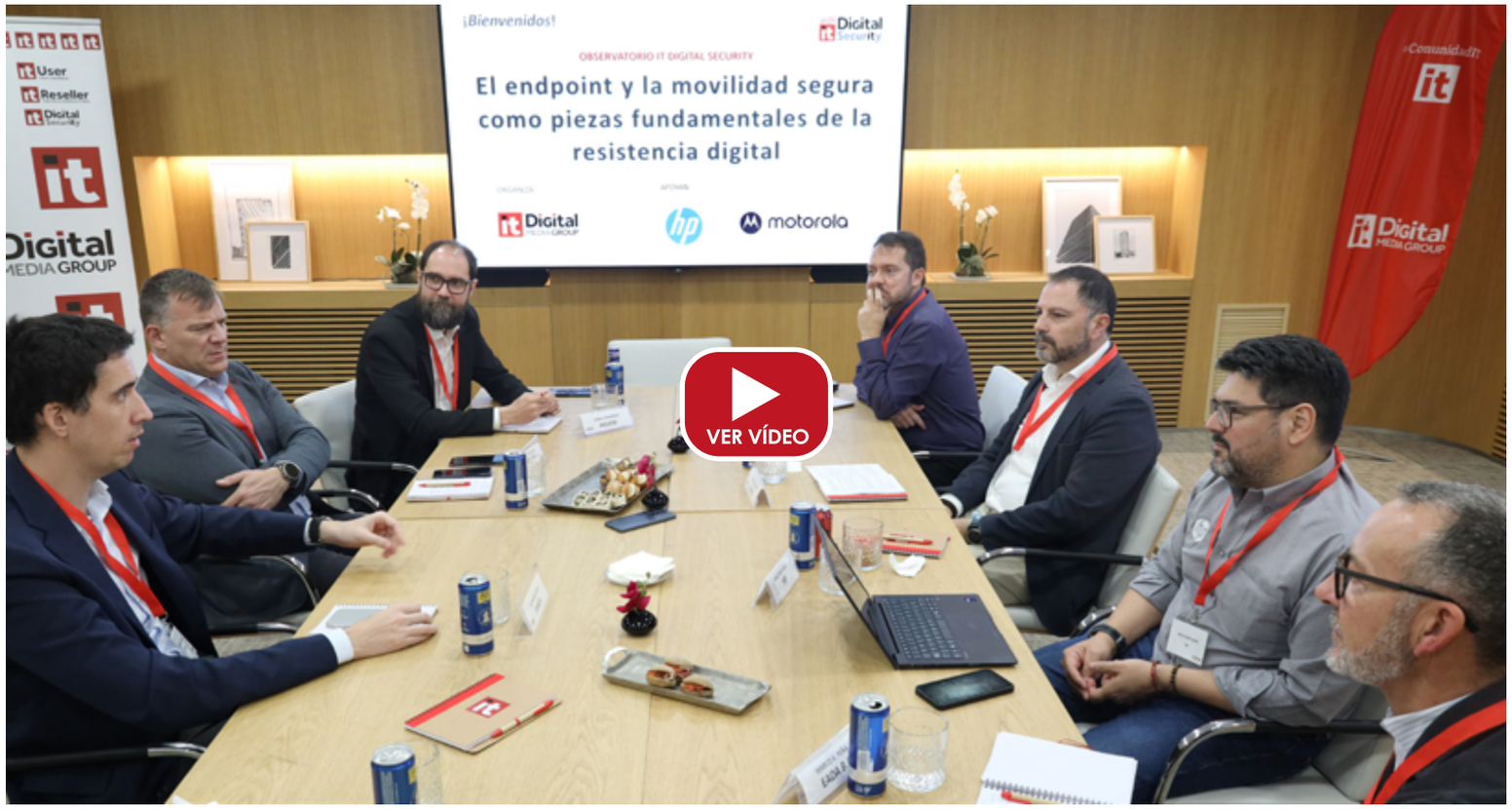
#FOROITDS

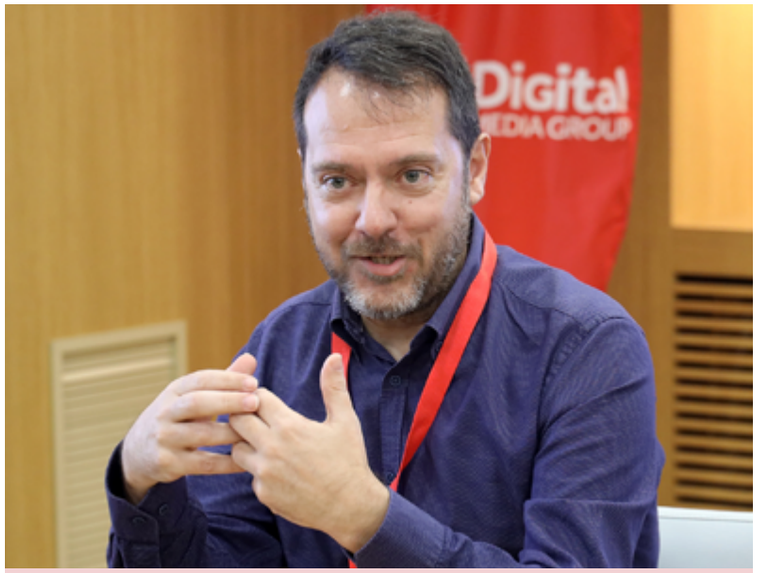
EL ENDPOINT Y LA MOVILIDAD SEGURA COMO PIEZAS FUNDAMENTALES DE LA RESISTENCIA DIGITAL

CON MODELOS HÍBRIDOS DE TRABAJO BIEN ASENTADOS Y UNA DIGITALIZACIÓN CORPORATIVA EXTENDIDA EN TODO TIPO DE SECTORES, LA PROTECCIÓN DEL PUESTO DE TRABAJO SE HA TRANSFORMADO, OBLIGANDO A LAS ORGANIZACIONES A REFORZAR SUS ESTRATEGIAS DE PROTECCIÓN DEL ENDPOINT.

No hace mucho tiempo, el modelo de la ciberseguridad corporativa se basaba en el llamado bastión: una fortaleza protegida por altos muros, dentro de la cual todo se consideraba protegido. Un perímetro seguro y más o menos fácil de defender. Sin embargo, en la última década, especialmente a partir del 2020, diferentes elementos han contribuido a transformar el paradigma de la seguridad corporativa, hasta el punto de que la palabra perímetro ha empezado a perder su sentido.

El último de esos elementos diferentes es la inteligencia artificial, en sus variantes generativa y agéntica. Dejando de lado la utilización que se hace de ella en la creación de diferentes tipos de ciberataques, el uso interno que hacen las organizaciones de esta tecnología ha ampliado el tipo de riesgos a los que se enfrentan, como el aumento





“Hacemos sesiones de formación departamentales y también píldoras de información más personales, lo que ha mejorado el porcentaje de éxito”
Jorge Crespo, responsable de Operaciones IT, **Capital Energy**

“Las herramientas del endpoint de algún modo son sondas, distribuidas en muchos entornos, con información sobre el comportamiento de los usuarios”
Marco Peña, CIO, **EADA Business School**

“Utilizamos una herramienta de formación interactiva, es una especie de escape room con el que nos aseguramos un mínimo de seguimiento”
Alejandro Velilla, CTO, **Embou**

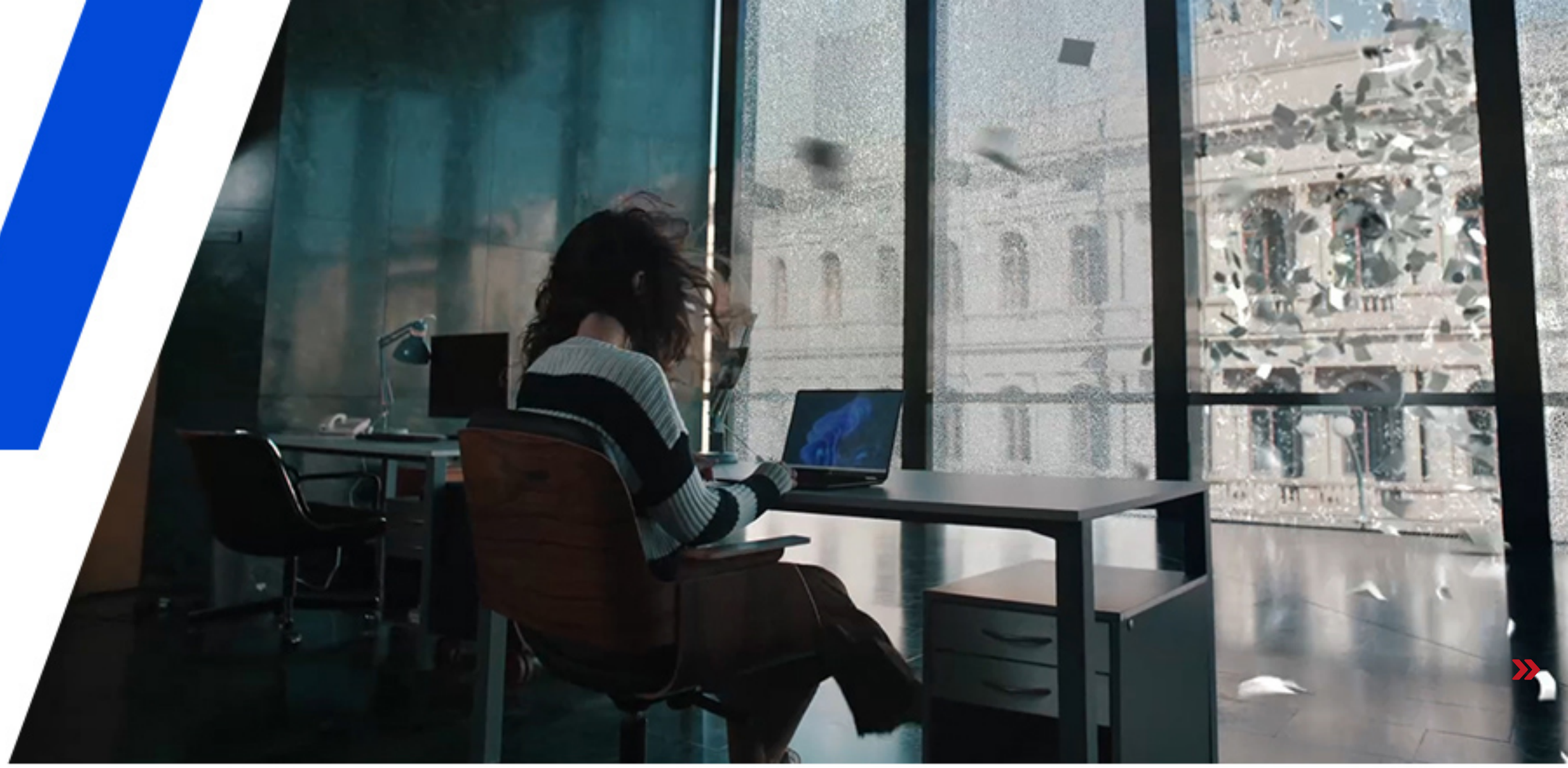
de las identidades de máquina o las herramientas de IA en la sombra. Pero estos nuevos tipos de IA han llegado en un momento en que el perímetro ya había sufrido una enorme transformación.

La digitalización de numerosos sectores y la expansión de los modelos de trabajo remotos e híbridos ya había hecho su trabajo para transformar la forma en que se gestiona la ciberseguridad en las empresas. Entre otras cosas, cambió el volumen y la tipología de los endpoints que se tienen que gestionar. Hemos hablado sobre la transformación de la ciberseguridad corporativa con responsables de tecnología y ciberseguridad de **Capital Energy, EADA Business School, Embou, Holcim** y **Sener**, en un observatorio que ha contado con el apoyo de **HP** y **Motorola**.

LA TRANSFORMACIÓN DE LA SEGURIDAD DEL ENDPOINT

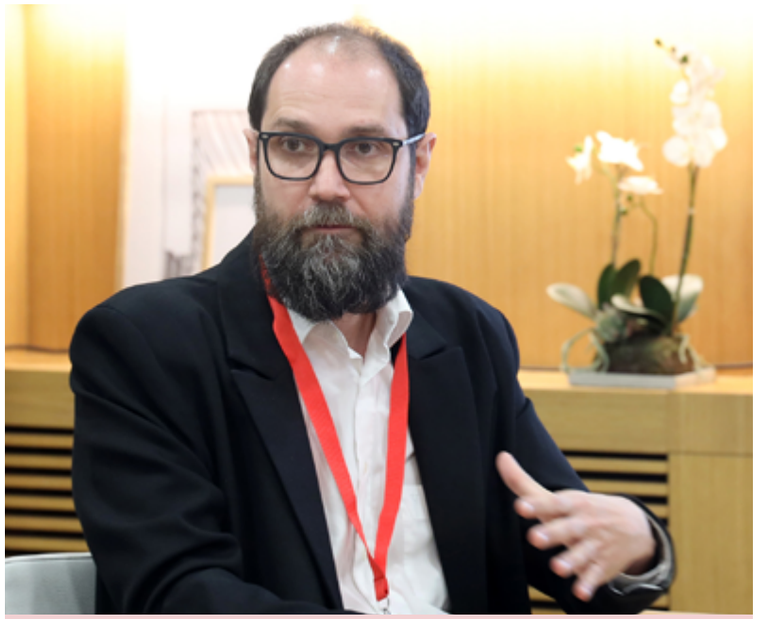
El cambio en las dinámicas de trabajo combina esos tres elementos: la IA, la digitalización y el trabajo a distancia, elementos entrelazados entre sí. Y, de igual manera que cada organización ha adoptado su modelo de trabajo o las estrategias de IA y digitalización que convenían a su negocio, la adaptación al nuevo escenario de la seguridad ha sido diferente en cada caso. Un buen ejemplo lo pone Jorge Crespo, responsable de Operaciones IT en Capital Energy:

“Hace 7 años, nuestro principal interés era el portátil de la empresa, que tuviera el antivirus o que esté en el directorio activo, entre otras cosas. Y ahora estamos viviendo un cambio. Las



Con las herramientas adecuadas, el trabajo no tiene por qué parecer trabajo

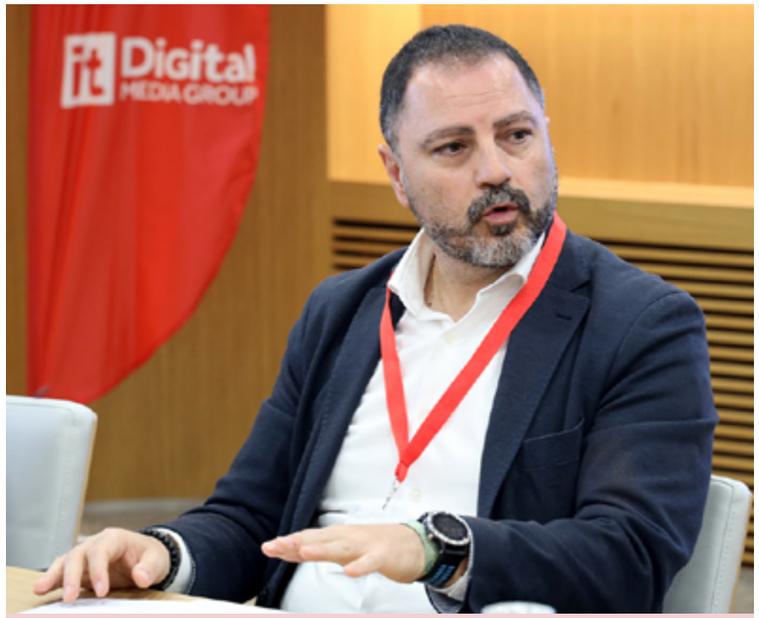
Redefine el futuro del trabajo



“Los ERP antiguos en red son los futuros legacy: en unos 20 años quizá no existirán las redes internas en muchas organizaciones medianas”

Daniel Fernández, global IT security officer, **Holcim**

oficinas se están convirtiendo en espacios de coworking privados; los usuarios pueden trabajar en ellos o donde quieran, con los ordenadores de la compañía. Nosotros nos apoyamos mucho en el acceso condicional. También estamos viviendo los cambios en la convergencia de IT y OT. Antes teníamos un castillo que protegíamos; veías que los aldeanos empezaban a salir cada vez más fuera del castillo. Se llevaban cosas y, al final, se quedaban a vivir ahí”.



“Le estamos quitando el peso de la seguridad al usuario y lo pasamos a la infraestructura, protegiendo toda la superficie de trabajo”

César De la Serna Sánchez, Cybersecurity lead, **Dcode (Sener)**

En mayor o menor medida, todos los expertos en ciberseguridad han vivido este cambio. Esa transformación de la superficie de ataque no es un hecho anecdótico. Siguiendo el ejemplo de la digitalización, el nuevo modelo de la ciberseguridad corporativa no es algo estático, sino que está vivo, sujeto a un proceso de constante evolución. Y, más que otra cosa, las circunstancias propias de cada compañía son las que marcan esa evolución.

PROTECCIÓN DEL PUESTO DE TRABAJO ADAPTADA A LA REALIDAD CORPORATIVA

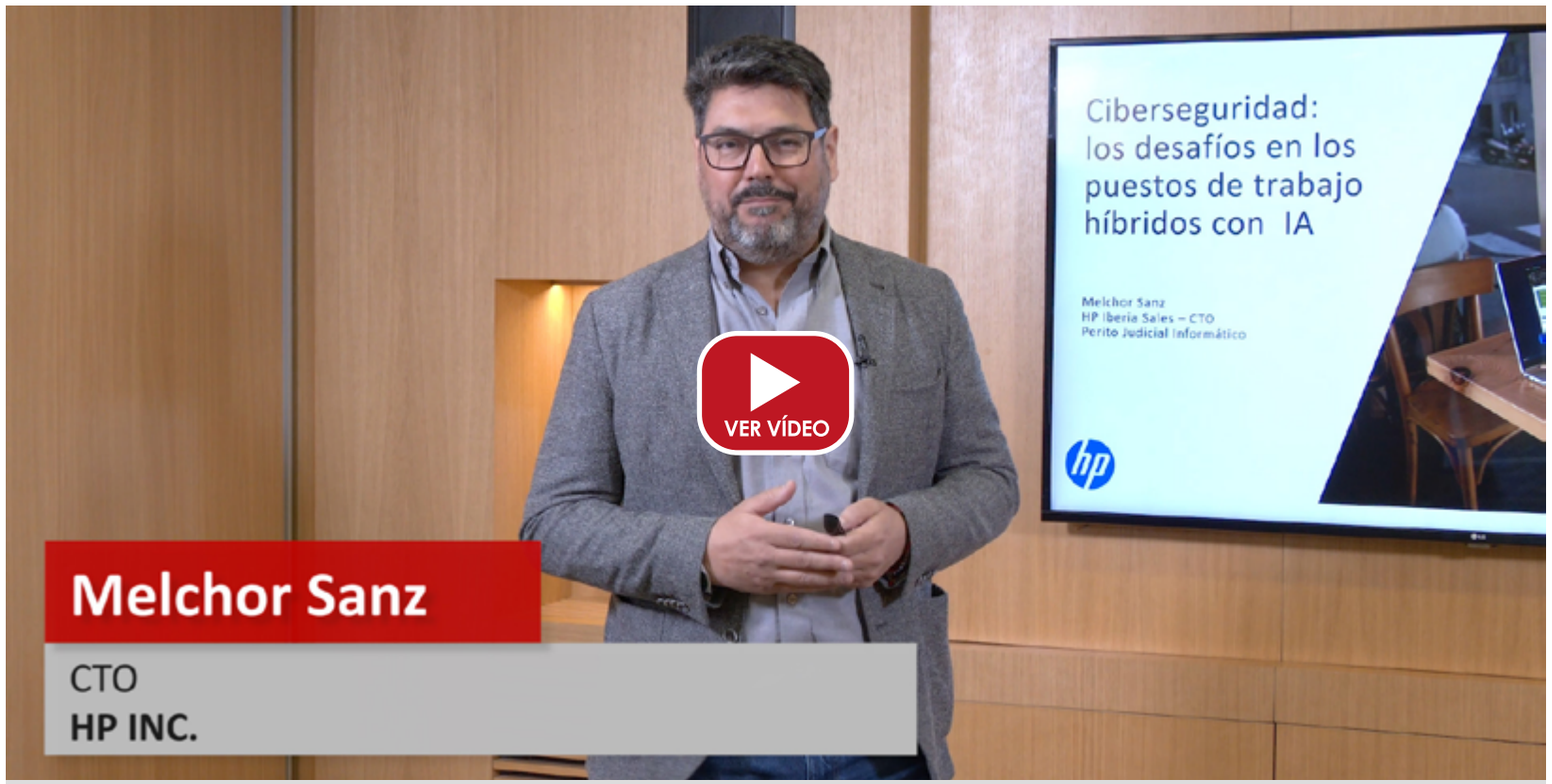
Marco Peña, CIO de EADA Business School, explica que “traer dispositivos a nuestro entorno está a la orden del día, aunque tenemos una problemática un poco mixta. En la parte corporativa, tienes un cierto nivel de control, con tus herramientas, tu supervisión, tu visibilidad, etc. La otra parte es diferente, es una especie de BYOD un poco más asilvestrado. Para nosotros es capital la supervisión de todos esos dispositivos constantemente en nuestras redes. Son redes de servicio, separadas de la red corporativa, con todos los niveles de segmentación y la supervisión. Y tenemos en marcha políticas de aislamiento de dispositivos: si detectamos un comportamiento sospechoso, podemos aislarlo”.

Por su parte, Alejandro Velilla, CTO de Embou, incide en que “uno de los grandes desafíos que tenemos es que la superficie de ataque incluye a mucha gente que no es de la organización. Nosotros tenemos un gran número de tiendas, con vendedores y comerciales que no son de la casa. Un reto constante porque hemos seguido creciendo. El otro reto es el de IoT, que también se ha ampliado con el despliegue de medio millón de antenas que hay por el mundo, sensores, etcétera, con nuestras SIM. Se calcula que más de un 60% de las incidencias entran por equipos de IoT no gestionados, que no están en una red corporativa. Securizar esos dispositivos es otro de los grandes retos”.

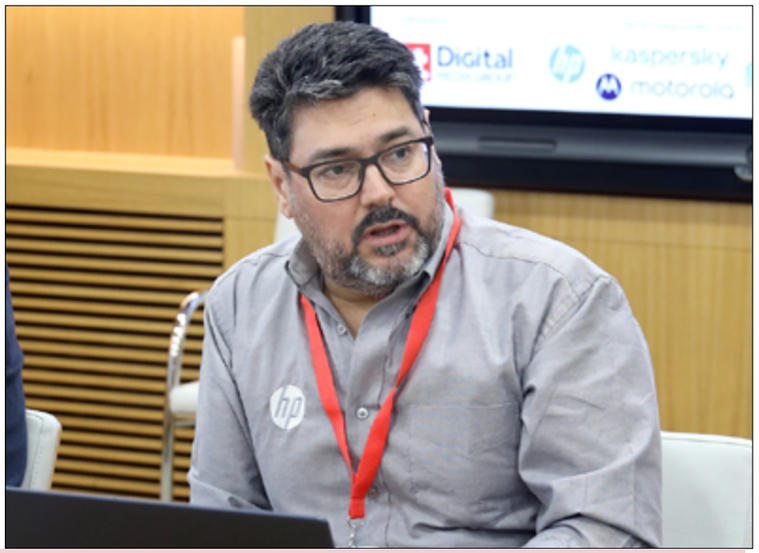
César De la Serna, Cybersecurity lead de Dcode, área digital del grupo Sener, señala que, “al crear, fabricar y desarrollar infraestructuras críticas, requerimos que nuestros empleados tengan un importante grado de movilidad. Por ello estamos cambiando para proteger no solo el dispositivo, sino todo lo que es la superficie del puesto de trabajo. Esto es, entender al usuario en su contexto, con su rol y el riesgo asociado a esa persona. En muchos de los casos, hay que adaptar las reglas a ese empleado que lo necesita. Hay departamentos que sí tendrán reglas comunes, pero eso también requiere por nosotros una agilidad para entender ese escenario. Por ejemplo, cuál es la interacción de entornos industriales y entornos IT, cuál es la gestión de la cadena de suministro. No es lo mismo el equipamiento que se le da a uno de marketing que el que está allí o el que esté probando en campo tecnologías de defensa avanzadas. Proteger la superficie de trabajo con la gestión de la identidad es una de las cosas que más nos importa”.

PROTECCIÓN END TO END

Todos estos cambios en los planteamientos de la ciberseguridad también han afectado a los proveedores tecnológicos, y no solo a los que se dedican específicamente a la ciberseguridad. El trabajo que realizan tiene dos ámbitos: por un lado, el trabajo



PRESENTACIÓN >> Melchor Sanz, CTO de HP, muestra la visión de la seguridad de la compañía en la presentación “Ciberseguridad: los desafíos en los puestos de trabajo híbridos con IA”. Entre otras cosas, detalla la importancia de incorporar una capa de ciberseguridad en el hardware, concibiendo la seguridad no solo desde el diseño sino desde el propio proceso de fabricación”.



“Los ordenadores profesionales tienen características de securización que protegen la cadena de suministro hasta su puesta en marcha: diseño, fabricación y distribución”

Melchor Sanz, CTO, **HP**

interno de su propia seguridad; y, por otro, la protección inherente que deben ofrecer en los dispositivos que fabrican, especialmente los dirigidos al trabajo en los entornos corporativos.

Melchor Sanz, CTO de HP, explica que tienen "una consola que ubica el equipo desde el momento en que se fabrica, aunque no tenga el sistema operativo, haya cambiado o esté guardado en un sótano sin encender... Incluso estando apagado puedes localizar el equipo, borrarlo o bloquearlo. Y es algo que se hace desde el hardware, no con el sistema operativo o el MDM. No se puede ceder el control de la seguridad a una de las capas. Si se cede el control de la gestión de la seguridad al software, pero la capa del hardware está comprometida entonces, ¿para qué sirve? Por eso, llevamos muchos años haciendo securizaciones desde el hardware. Ahora hemos incorporado la herramienta Workforce Experience Platform, que hace muchas cosas más, como medir la experiencia del usuario. No es intrusiva, pero permite controlar el equipo y también ver cómo se está usando. Facilita la seguridad del equipo y la gestión de la información, dando al departamento de IT ese poder sobre el hardware como base sobre la cual se sustentan

PRESENTACIÓN >> Daniel Gascón, Head of B2B en Motorola Iberia, detalla la propuesta de ThinkShield y Motorola for Business para lograr el endpoint ultra seguro. La compañía ha llevado a los móviles corporativos una completa propuesta de seguridad integral, a nivel de hardware y de software, así como una versátil capacidad de gestión y control remoto de la flota de dispositivos corporativos.

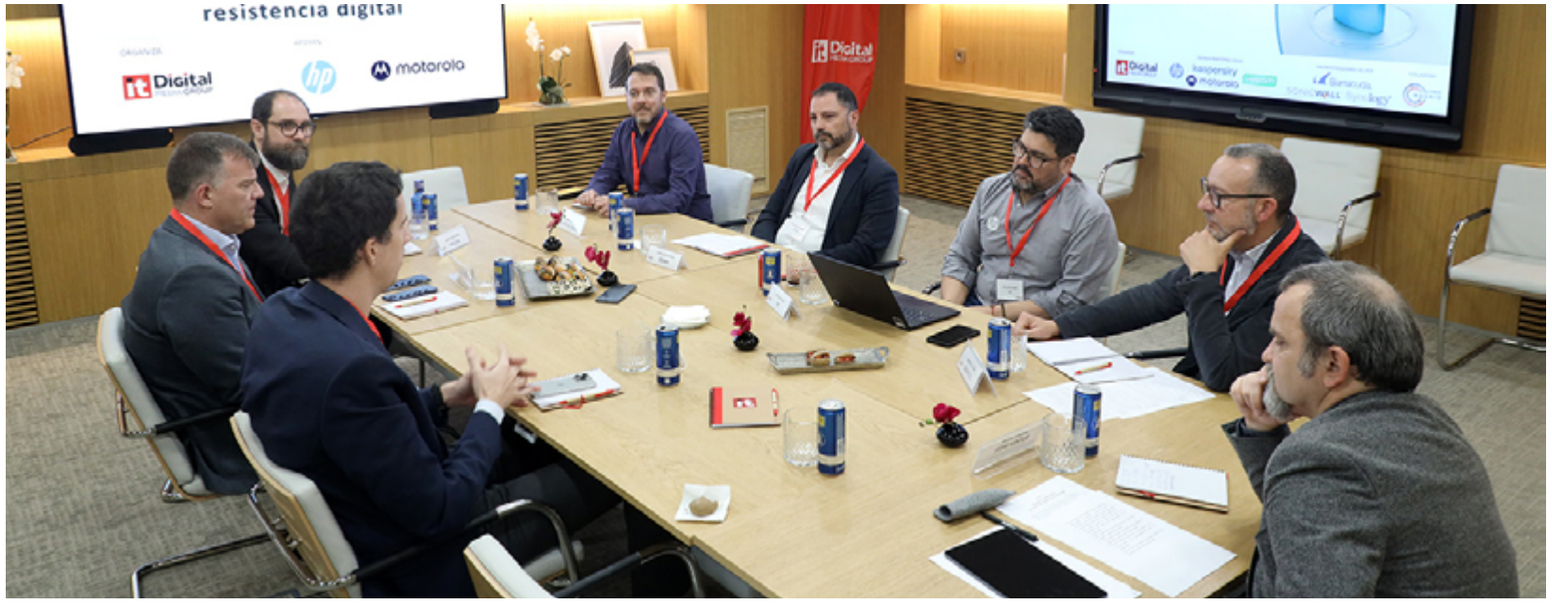
"Estamos democratizando el uso de herramientas de productividad y seguridad como MotoSecure, que añaden una capa de seguridad extra"
Daniel Gascón, head of B2B, **Motorola**

el resto de capas, que son el sistema operativo, el antivirus y las aplicaciones".

Por su parte, Daniel Gascón, head of B2B en Motorola, comenta que "ha habido una preocupación alta en el entorno B2B por todo lo relacionado con la seguridad de los dispositivos. Nosotros tenemos un equipo de desarrollo deslocalizado, que hace que evolucionen todas estas soluciones que luego están por encima del sistema operativo. Llevamos cuatro años y medio desarrollando ThinkShield, un nivel de seguridad por encima del que proporciona Android. También creamos nuestro propio MDM, por supuesto, además de una herramienta para controlar actualizaciones de software; la herramienta predictiva Motoanalytics para que, según la salud de los dispositivos, se decidan las actuaciones a futuro que se deben tomar; o Antena Performance, que muestra cómo se comportan los dispositivos, cómo está la batería, el consumo de las aplicaciones, etc".

De cara al futuro, es difícil evaluar los cambios en la ciberseguridad, aunque hay conceptos que parecen claros. Daniel Fernández, global IT security officer de Holcim, destaca "la identidad es un elemento clave para identificar todos los dispositivos y con eso orquestar la defensa de lo que está gestionando el usuario. Independientemente del dispositivo, sea de empresa o no, habrá que incorporar la mayoría de la seguridad de manera transparente. Pero también con prohibiciones serias, dependiendo del dispositivo. En general, o empezamos a controlar todo inventariándolo o va a ser un descontrol. El futuro pasa por prohibir dispositivos personales no securizados. Si quieren utilizar, por ejemplo, el correo corporativo, viene con una serie de implicaciones de seguridad. Y, si no, no podrían utilizarlo".

En todo caso, el puesto de trabajo ha experimentado una transformación que, sea como sea el camino que vaya a tomar, no tiene vuelta atrás. Nadie se plantea, en ningún caso, volver a un escenario anterior. Lo que está sobre la mesa, más bien, es aprovechar el escenario actual, utilizando incluso el endpoint como un sensor capaz de recabar todo tipo de información contextual útil para la organización. ■



MÁS INFO +

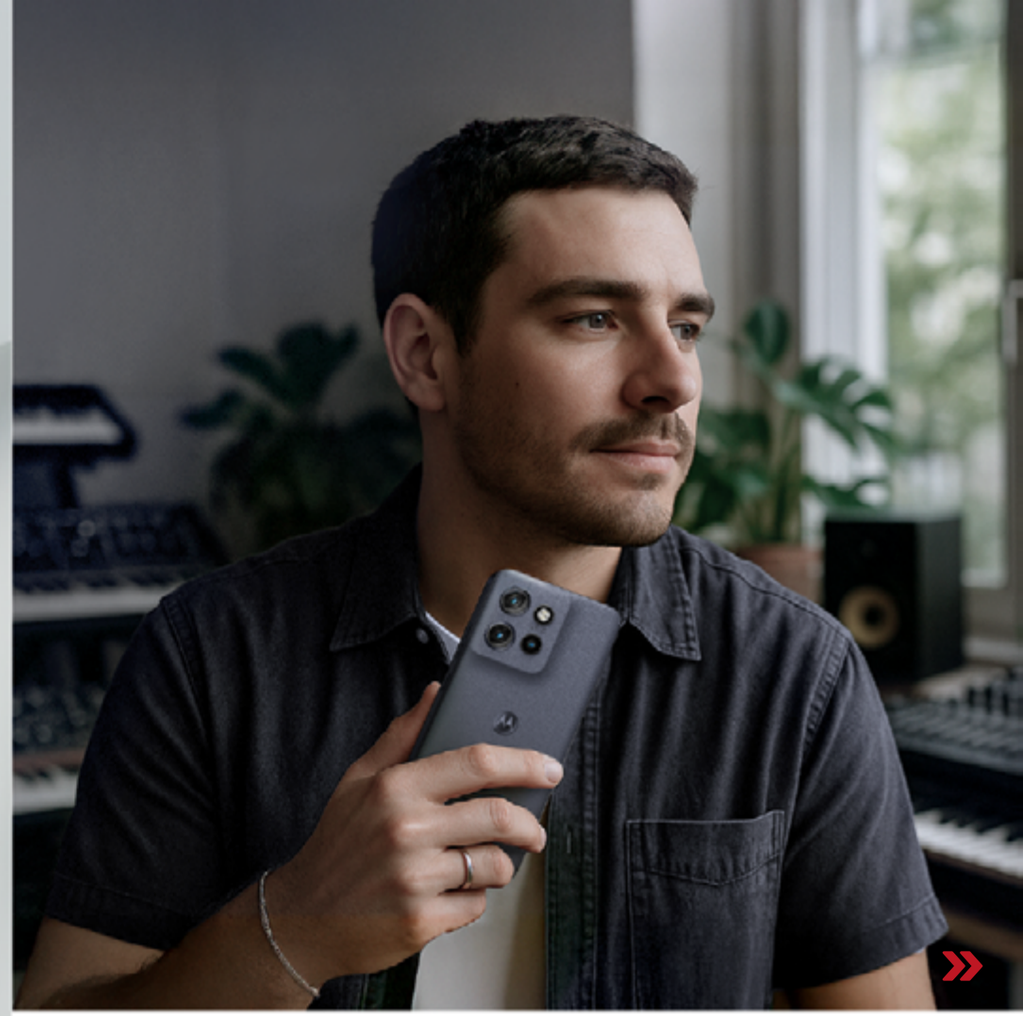
- X Foro de IT Digital Security: Consolidando la resiliencia operativa
- HP for Business
- Motorola Business
- Construyendo un endpoint ultra seguro
- Entrevista César De la Serna Sanchez, Cybersecurity Lead de Sener

COMPARTIR EN REDES SOCIALES

motorola

FOR BUSINESS

edge 60 NEO



DISEÑO PREMIUM. DURABILIDAD COMPROBADA.

Diseño compacto pero resistente con protección IP68/69, Gorilla® Glass 7i y certificación militar MIL-STD 810H

50 MP

Cámara principal de de 50MP Sony LYTIA™ y moto ai

Batería de 5000 mAh y carga rápida de 68W

A

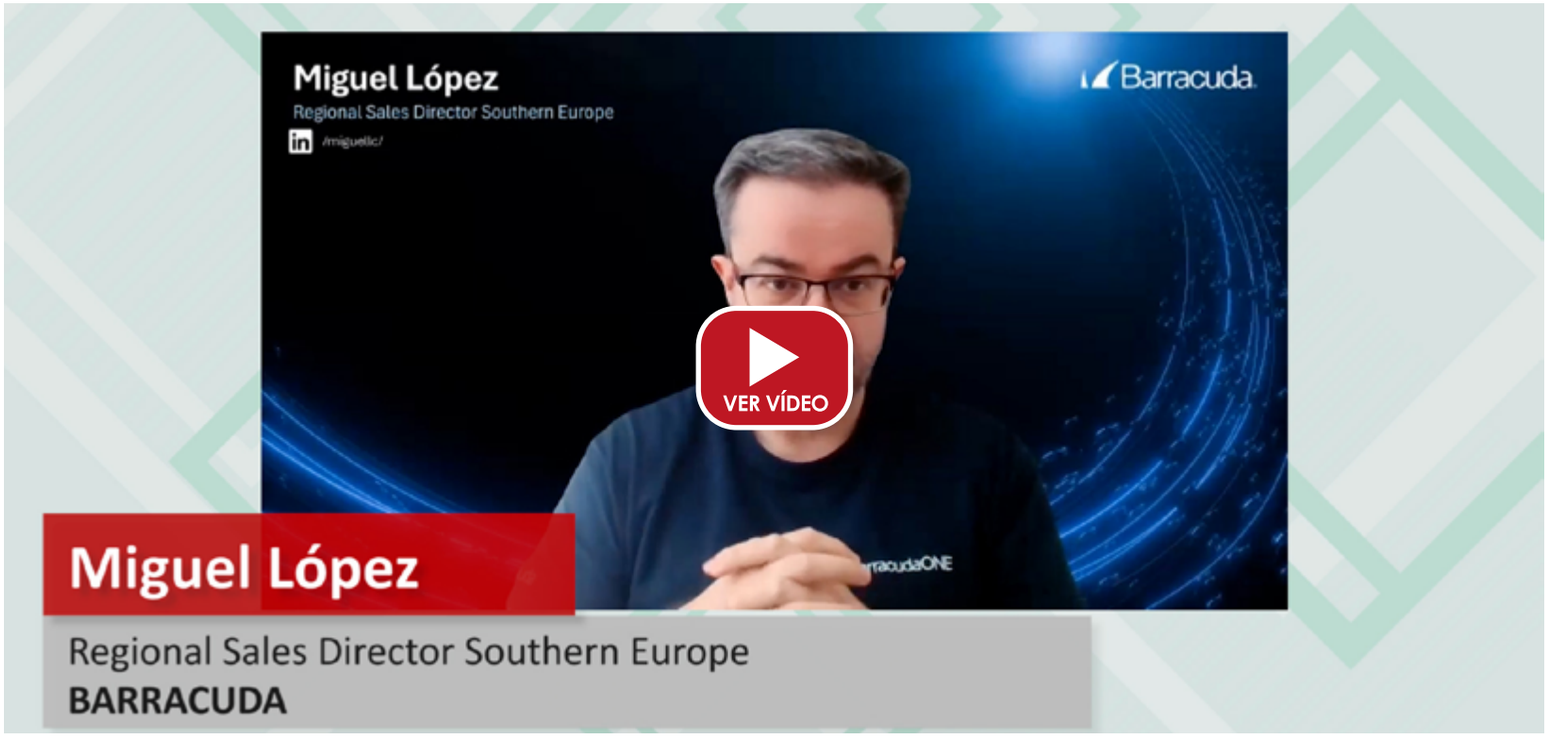
MIGUEL LÓPEZ, REGIONAL SALES DIRECTOR PARA EL SUR DE EUROPA DE BARRACUDA

ESCALANDO ZERO TRUST: IDENTIDAD Y CADENA DE SUMINISTRO COMO NUEVO PERÍMETRO

MIGUEL LÓPEZ, REGIONAL SALES DIRECTOR PARA EL SUR DE EUROPA DE BARRACUDA, EXPLICA LA EVOLUCIÓN DE LAS POLÍTICAS ZERO TRUST EN TORNO A LA IDENTIDAD, LOS DISPOSITIVOS, LOS ENTORNOS DE RED, LAS APLICACIONES Y LOS DATOS, DESTACANDO EL RETO OPERATIVO DE ESCALAR ZERO TRUST DE FORMA CONSISTENTE Y COHERENTE EN ENTORNOS HÍBRIDOS.

En la actualidad, la ciberseguridad ha dejado de centrarse en el perímetro tradicional, los límites físicos de la oficina, para enfocarse en los ecosistemas híbridos y distribuidos. Así lo explica Miguel López, regional sales director para el Sur de Europa de Barracuda, quien señala que muchas organizaciones cometen el error de pensar que Zero Trust es simplemente una cuestión de sustituir VPN o reforzar la autenticación. Para el directivo, “el verdadero reto es escalar Zero Trust de una forma coherente en un entorno híbrido” en el que deben convivir infraestructuras on-premise, nubes, usuarios remotos y terceros.

El concepto de seguridad basado en muros, en un modelo de bastión, ha quedado obsoleto.



Como señala el experto, “el perímetro tradicional ya no existe” y se ha desplazado de forma definitiva hacia la identidad digital. Esta identidad no se limita únicamente a las personas; hoy abarca dispositivos, cargas de trabajo y, de forma creciente, las API. En este nuevo escenario, cada acceso debe ser evaluado bajo una verificación que debe ser “continua, no puntual”, analizando quién accede, desde qué dispositivo y en qué contexto.

GRANDES AMENAZAS A LA CIBERSEGURIDAD MODERNA

López destaca como uno de los peligros más críticos detectados en entornos híbridos es la creación de “islas de seguridad”, debidas habitualmente a implantaciones parciales. Por ejemplo, proteger la identidad en la nube pero no en entornos locales genera brechas que los atacantes pueden explotar con facilidad. “Probablemente, una de las mayores amenazas que puede haber a la ciberseguridad es precisamente esta falsa sensación de seguridad”, pues deja múltiples huecos abiertos mientras la organización cree estar protegida.

Otro de los grandes desafíos lo representa la cadena de suministro. La superficie de ataque se ha expandido exponencialmente a través de terceros. En un modelo interconectado, “los ataques a la cadena de suministro ya no requieren vulnerar directamente a la víctima; basta con comprometer un proveedor, un software o una API de tercero”. Si estas identidades externas no se gobiernan bajo los principios de mínimo privilegio y verificación continua, se convierten irremediablemente en el eslabón más débil de la defensa.

Miguel López concluye que “Zero Trust no es un producto, es una estrategia operativa”, concebida en torno a la seguridad de cinco elementos: la identidad, los dispositivos, los entornos de red, las aplicaciones y los datos. Para escalar esta estrategia de manera sostenible, las empresas deben centrarse en tres aspectos clave: tratar la identidad, humana y no humana, como el nuevo perímetro; aplicar el modelo Zero Trust de forma coherente en entornos híbridos, eliminando los silos entre cloud y on-premise; e integrar la gestión del riesgo de la cadena de suministro dentro de todas las políticas de acceso. Al consolidar estas capacidades en una plataforma unificada, las organizaciones no solo reducen su superficie de ataque, sino que mejoran su resiliencia frente a un ecosistema cada vez más complejo e interconectado. ■

MIGUEL LÓPEZ, DE BARRACUDA, CONSIDERA QUE UNA DE LAS MAYORES AMENAZAS QUE HAY PARA LA CIBERSEGURIDAD ES PRECISAMENTE UNA FALSA SENSACIÓN DE SEGURIDAD

MÁS INFO +

- Guía para construir una estrategia de ciberresiliencia
- Por qué una plataforma integral de ciberseguridad supera a las soluciones puntuales
- Zero Trust en entornos híbridos: cuando la identidad y la cadena de suministro se convierten en el nuevo perímetro
- X Foro de IT Digital Security: Consolidando la resiliencia operativa

Barracuda

PROTECCIÓN COMPLETA FRENTE A LOS « CIBERATAQUES »

Managed XDR, protección de email, datos, aplicaciones y redes.

SERGIO MARTÍNEZ, COUNTRY MANAGER DE SONICWALL

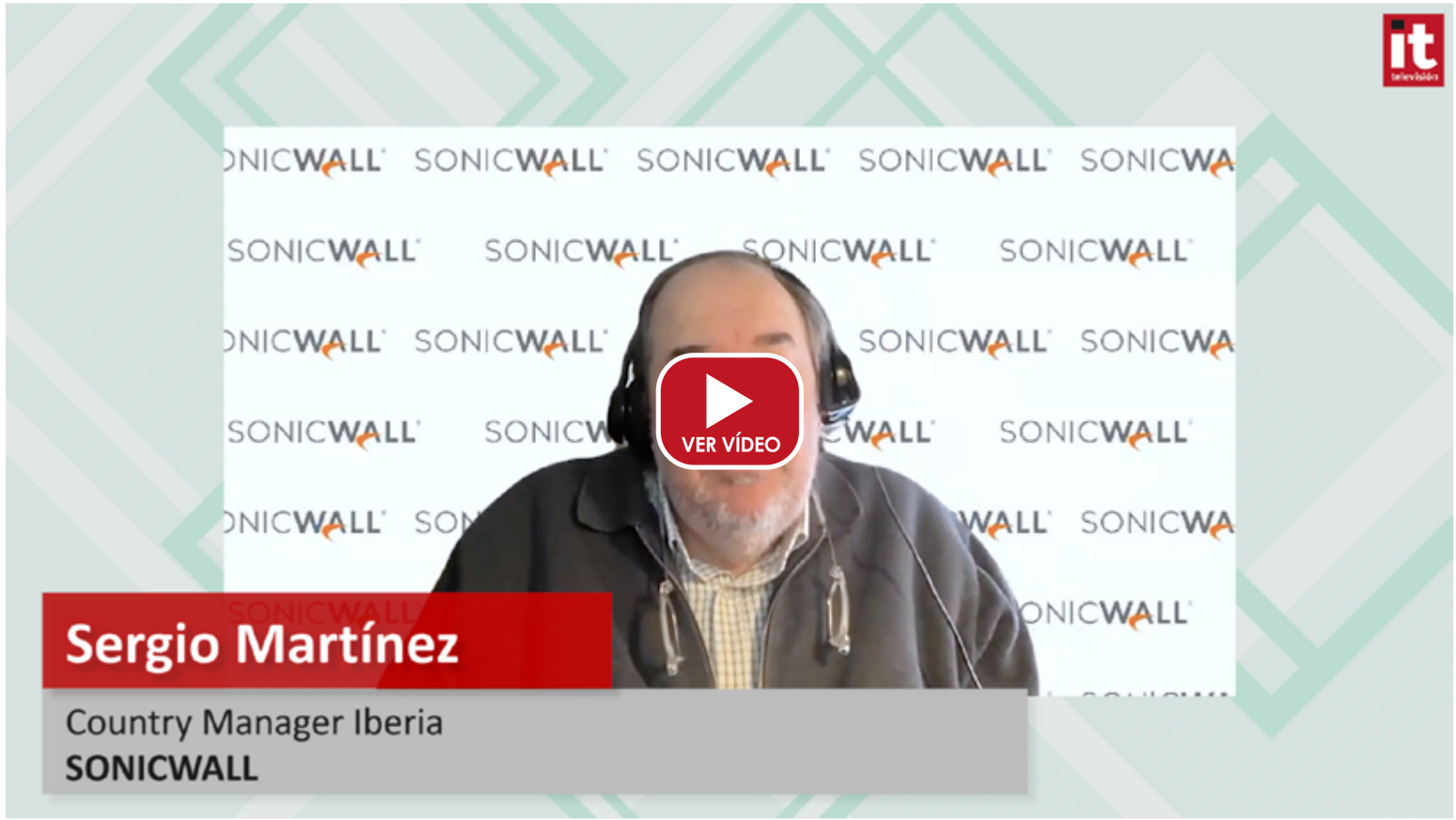
CÓMO SABER QUÉ SUCEDE EN TU RED Y SISTEMAS

SERGIO MARTÍNEZ, COUNTRY MANAGER DE SONICWALL, OFRECE UN DETALLADO ANÁLISIS DEL PANORAMA DE AMENAZAS ACTUAL Y LAS NECESIDADES DE PROTECCIÓN DE LAS EMPRESAS, FRENTE A LAS QUE LA COMPAÑÍA OFRECE UNA AMPLIA PROPUESTA DE DETECCIÓN Y RESPUESTA AMPLIADA Y GESTIONADA.

Uno de los mayores retos actuales es gestionar la ingente cantidad de información que generan los sistemas. Sergio Martínez, country manager de SonicWall, utiliza una analogía clara: una casa llena de sensores (cámaras, humo, ventanas) donde, de repente, “el perro ladra y no sabes por qué”. Las organizaciones se enfrentan a una fatiga de alertas donde no siempre es fácil distinguir qué eventos son críticos.

Además, los atacantes aprovechan los momentos de menor vigilancia, como recuerda Martínez: “Casi ocho de cada 10 ciberataques se producen fuera del horario laboral y los fines de semana, típicamente la madrugada del viernes al sábado, porque tienen así 48 horas para explotar”. Una complejidad a la que se suma la inteligencia artificial, utilizada para revitalizar viejos ataques.

En efecto, la IA generativa y agéntica permiten crear phishing extremadamente convincen-



te, localizar sistemas no parcheados (legacy) y automatizar el encadenamiento de exploits. Lo más preocupante es su capacidad para evadir la detección mediante técnicas de ofuscación, esperando el momento oportuno para actuar. Estos elementos crean un escenario con unos niveles de exigencia muy altos, habitualmente fuera del alcance de las pymes.

UN SERVICIO A LAS PYMES A TRAVÉS DEL CANAL

El desarrollo de SonicWall está, de hecho, muy ligado a las pymes, trabajando siempre a través de una red de decenas de miles de socios de canal. Para este segmento la compañía ofrece los servicios de seguridad gestionada soportada desde su SOC europeo situado en Frankfurt. Desde este centro de operaciones de seguridad proporcionan, entre otros, servicios de detección y respuesta gestionados y servicios NOC.

Sergio Martínez recalca la necesidad urgente de modernizar las VPN tradicionales basadas en SSL, que son un vector de ataque frecuente debido a fallos de diseño. La propuesta de la compañía para por evolucionar hacia arquitecturas de Zero Trust (ZTNA) y el uso de Cloud Secure Edge, integrando múltiples factores de autenticación para garantizar un acceso remoto seguro y moderno.

En cuanto a la inteligencia artificial utilizada en tareas defensivas, no se trata de una moda pasajera sino de algo que lleva mucho tiempo nutriendo a las empresas de ciberseguridad. Martínez explica que “hace más de 25 años que utilizamos la IA con nuestros sandboxes avanzados para detectar comportamientos, atípicos dentro de la infraestructura”.

El mensaje final de SonicWall es la democratización de la ciberseguridad avanzada. Su estrategia de “defensa por capas” busca que la capacidad de detectar lo desconocido y responder ante amenazas complejas sea algo asequible, “que todo esto lo pueda pagar una pyme”, permitiendo que cualquier organización, sin importar su tamaño, sea resiliente en el entorno hostil actual. ■

MÁS INFO +

- Informe SonicWall Cyber Protect 2026
- Cómo saber qué sucede en tu red y sistemas
- X Foro de IT Digital Security: Consolidando la resiliencia operativa

COMPARTIR EN REDES SOCIALES

SONICWALL®

Nunca solo. Seguridad inquebrantable.

Soluciones de ciberseguridad para

- Red
- Nube
- Endpoint
- Servicios XDR gestionados

Descubra cómo impulsar sus ingresos: visite SonicWall.com o escríbanos a spain@sonicwall.com.

TOMÁS SAIZ, BUSINESS PROJECT MANAGER EN SYNOLOGY

BACK-UP & GESTIÓN DEL DATO: NUEVOS RETOS EN LA CONTINUIDAD DE NEGOCIO

TOMÁS SAIZ, BUSINESS PROJECT MANAGER EN SYNOLOGY, DETALLA LOS DESAFÍOS Y LOS RIESGOS DE UN ELEMENTO CLAVE PARA LA CAPACIDAD DE CIBERRESILIENCIA DE LAS ORGANIZACIONES: EL BACKUP. DESDE LA COMPAÑÍA REFUERZAN LA PROTECCIÓN DE LAS COPIAS DE SEGURIDAD CON INMUTABILIDAD, SEPARACIÓN GRANULAR DE PERMISOS Y CREDENCIALES O UNA CAPACIDAD DE RESTAURACIÓN VERSÁTIL, ENTRE OTROS ELEMENTOS.

En un entorno empresarial marcado por la incertidumbre digital, la gestión del dato se ha consolidado como el pilar fundamental de la resiliencia corporativa. Tomás Saiz, business project manager en Synology, detalla en esta presentación la visión integral de la compañía sobre cómo las organizaciones deben afrontar los retos actuales, subrayando que la continuidad de negocio no se limita a responder ante desastres físicos, sino que exige una estrategia proactiva y coordinada.

Uno de los puntos clave que desgrana la ponencia es la necesidad de entender la interrelación entre tres pilares: el backup, la gestión del dato y la continuidad de negocio. El éxito de estos sistemas no reside únicamente en la infraestructura técnica, sino en un concepto humano y organizativo. Saiz destaca que "backup, gestión del dato y continuidad de negocio, son tres conceptos que van muy muy ligados. Y uno de los más relevantes es la orquestación, que no tiene nada que ver con la tecnología, sino que es la inclusión de toda la compañía en esta gestión".

EL ALTO RIESGO DE NO RECUPERARSE TRAS UN CIBERATAQUE

La realidad actual presenta amenazas sofisticadas como la inteligencia artificial en la sombra o los ataques de phishing altamente dirigidos que comprometen la integridad de los datos.

Las consecuencias son severas: se estima que, además del propio incremento en el volumen de los ciberataques el 60% de las pymes españolas no logran recuperarse totalmente tras un ataque, y aquellas que lo hacen tardan una media de 100 días en restablecer su actividad. A esto se suman los riesgos legales, ya que el 32% de estos incidentes terminan en multas y sanciones administrativas.

Frente a este escenario, Synology aboga por una restauración versátil y granular, huyendo de la idea de duplicar infraestructuras completas de forma ineficiente. La clave reside en identificar qué unidades de negocio son críticas y qué datos necesitan realmente para seguir operando. Tal como explica Tomás Saiz, "no se trata de restaurar todo el ecosistema, sino que tenemos que ir a cada una de esas unidades y darles las herramientas que sean necesarias para continuar con su trabajo".

La estrategia de protección del backup se completa con la adopción de la inmutabilidad del dato y la realización de pruebas constantes. La preparación es la única garantía de éxito ante un incidente real, lo que obliga a las empresas a pasar de la teoría a la práctica. En palabras de Saiz: "hay que ensayar de manera que cuando ocurra un incidente todos sepamos lo que tengamos que hacer y quién tiene que intervenir para poder restaurar en tiempo y forma". Esta capacidad de respuesta, sumada a una visibilidad clara del estado de los sistemas, es lo que permite reducir los tiempos de recuperación al mínimo posible, asegurando que el negocio no se detenga ante los riesgos del ecosistema digital actual. ■

MÁS INFO +

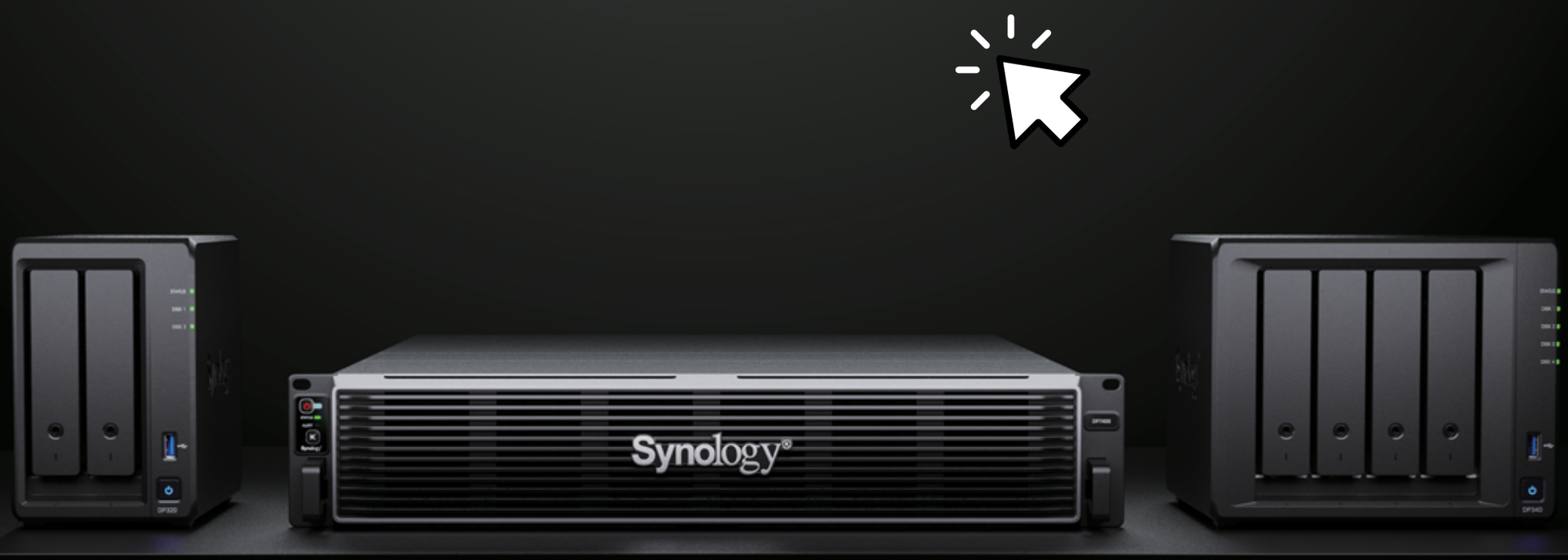
- X Foro de IT Digital Security: Consolidando la resiliencia operativa
- Soluciones ActiveProtect
- Contacta con Synology
- De la copia de seguridad a la ciberresiliencia real
- Seguridad en el Dato: Custodia, Confianza y Compliance

COMPARTIR EN REDES SOCIALES

Synology® | DP SERIES

Dispositivos con ActiveProtect 1.2

Impulse la protección de los datos de su empresa al más alto nivel, mientras simplifica su gestión y reduce la carga del equipo.



Fácil de usar

Interfaz intuitiva para empezar en minuntos.

Escalable

Facilita la evolución del sistema y reduce costes.

Seguridad avanzada

Inmutabilidad, WORM y protección completa.

Gestión centralizada

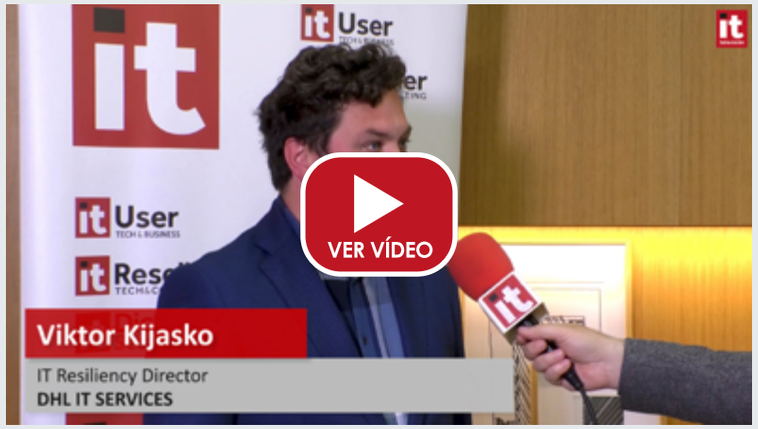
Supervise todas sus cargas desde una única consola.

*Hable con un experto de Synology:

MÁS CONTENIDO

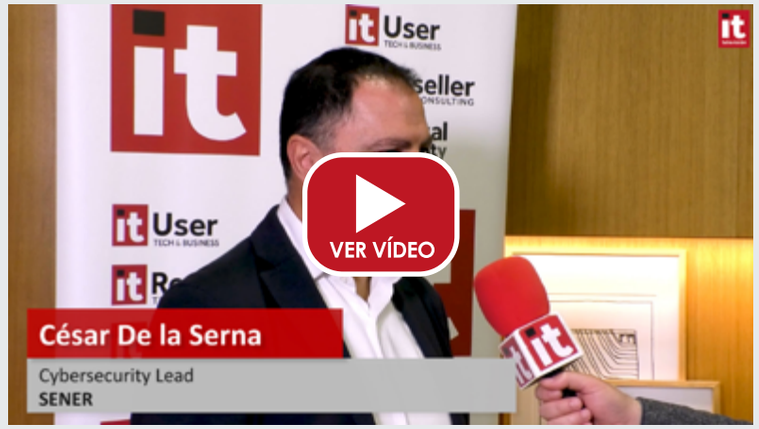
“La protección de la identidad y la higiene digital son básicos para pyme y gran empresa”

Marc Rivero, La Salle



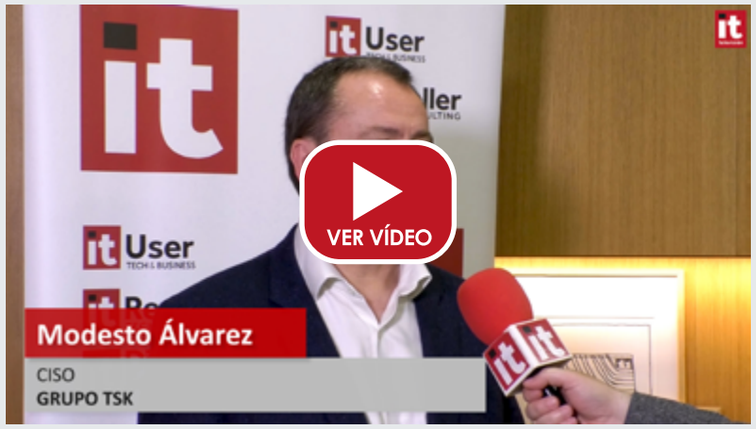
“Necesitamos asegurar que nuestras operaciones siempre están funcionando”

Viktor Kijaško, DHL IT Services



“La ciberseguridad será cada vez más transversal y estará más unida al negocio”

César de la Serna, Dcode (Sener)



“Tenemos que prepararnos para responder, pero tiene que hacerlo toda la empresa”

Modesto Álvarez, Grupo TSK

“Las mujeres no se pueden quedar atrás en un sector que es estratégico para la economía”

Virginia Vicente, CyberMadrid

Consolidando la resiliencia operativa

En la X edición del Foro de IT Digital Security hemos visto cómo organizaciones de perfiles muy diferentes afrontan retos muy similares, en un momento en que la protección del endpoint y la capacidad de recuperarse tras un ciberataque se han convertido en elementos fundamentales de la seguridad corporativa.

FORO it Digital Security

CONSOLIDANDO LA RESILIENCIA OPERATIVA

¡Ver todos los contenidos!

ORGANIZA

PATROCINADORES GOLD

PATROCINADORES SILVER

COLABORA