

Madrid Tech Show se consolida como evento de referencia del sector tecnológico



Madrid Tech Show volvió a convertirse en escaparate tecnológico los pasados 30 y 31 de octubre para más de 400 expositores y 18.000 asistentes. Un evento que se ha convertido en foco de la tecnología relacionada con el comercio electrónico, big data, IA, el ecosistema de la nube, los centros de datos, la ciberseguridad o la conectividad, y el vehículo que recoge las principales iniciativas empresariales de la transformación digital en España.

REPORTAJE ciberseguridadTIC

Destacaba durante la inauguración Agustín Torres, presidente de CloserStill Media, que la innovación, la sostenibilidad y la eficiencia energética también se han convertido en protagonistas de este evento en un mundo que se apunta a ser más sostenible.

Ángel Asensio, presidente de la Cámara de Madrid, destacó del evento que se haya convertido en “la prueba palpable de que esta región quiere liderar la revolución tecnológica a nivel internacional. Una oportunidad de crear alianzas tecnológicas con soluciones disruptivas y personas con el deseo de cambiar el mundo a través de las nuevas tecnologías en un momento en el que las empresas digitalizadas son un 10 % más productivas”.

Miguel López, consejero de digitalización de la Comunidad de Madrid, aprovechó su presencia en el evento para destacar los ambiciosos planes de la comunidad en el entorno de los centros de datos. “Ya nos hemos consolidado como el hub digital del sur de Europa y nuestro paso es ser referencia a nivel mundial”, ha

manifestado. Actualmente Madrid alberga 30 centros de datos con una capacidad de unos 250 megavatios y proyectos importantes que permitirán alcanzar los 600 megavatios en 2026, o incluso superarlos, ha avanzado. Entre las ventajas de Madrid para acoger centros de datos figuran su posición geográfica, su ecosistema empresarial tecnológico y ser la

región líder en fibra en el sur de Europa. Todo ello sin olvidar, como ha recordado, la reciente creación de la Agencia de Ciberseguridad de la Comunidad de Madrid, con el fin de proteger a la administración autonómica de los ciberataques, colaborar con el INCIBE e impulsar el uso de soluciones ante las amenazas.

Carme Artigas, consejera de digitalización e IA



Madrid Tech Show vuelve a convertirse en escaparate tecnológico para más de 400 expositores y 25.000 visitantes

REPORTAJE **ciberseguridad**TIC

del Gobierno de España, puso el acento en que en los últimos cuatro años España se ha convertido en un referente internacional en la transformación digital. Algo que se ha logrado, en parte, por el impulso dado a la Agenda España

Digital 2026, en la que los Fondos NextGeneration han permitido poner en marcha iniciativas y programas muy transformadores con la colaboración entre administraciones y la colaboración público-privada.



Durante el evento se han repasado las principales tendencias y retos del sector de la mano de las principales empresas y organismos

Habla el mercado

Durante el evento, [Ciberseguridad TIC](#) ha querido tomarle el pulso al sector planteando una serie de preguntas a varias empresas participantes. La **primer** nació inspirada en el título de la ponencia de Begoña Villacís, directora global de Relaciones Institucionales de BeDisruptive, en la que aseguró, entre otras muchas cosas, que no hay libertad, riqueza o prosperidad si no hay seguridad.

También preguntamos si el mercado de ciberseguridad va a la velocidad que demanda la Transformación digital. Finalmente, ¿qué destacarías este año?

REPORTAJE ciberseguridadTIC

Arcserve

Carlos Franco, Technical Sales Consultant and Data Protection Specialist, Arcserve

“Cada día somos más conscientes de los riesgos que estamos sufriendo”



Explicando que Arcserve trabaja en la protección de datos más que en ciberseguridad, que es un complemento, asegura Carlos Franco que la ciberseguridad es necesaria porque hay muchos peligros hoy en día.

Preguntado por si el mercado de ciberseguridad va a la velocidad que demanda la transformación digital, dice Carlos Franco, Technical

Sales Consultant and Data Protection Specialist de Arcserve, que los clientes son conscientes de que tienen que invertir para que sus datos estén a salvo, pero que les cuesta hacerlo; “parece que el mercado dolo aprende a base de brechas, asegura.

Asegura también el ejecutivo de Arcserve que “cada día somos más conscientes de los riesgos que estamos sufriendo si no estamos protegidos”, lo que queda demostrado en la cantidad de gente que asiste al Madrid Tech Show; “nos gusta porque están todas las empresas del sector y nos permite tener un contacto directo con los clientes”.

Arexdata

Alberto Tejero Hidalgo, CEO, Arexdata

“Las empresas están cada vez más concienciadas en ciberseguridad”

¿Por qué ciberseguridad? “Porque lo que estamos viendo es que todo avanza muy rápido”, respondía Alberto Tejero Hidalgo, CEO de Arexdata, añadiendo que, en cambio, hay partes en



la transformación digital de las empresas que van bastante lentas.

Asegura que las empresas están cada vez más concienciadas en ciberseguridad y que “tenemos que conseguir que la transformación digital y la ciberseguridad vayan de la mano”.

Preguntado por lo que destacaría de lo ocurrido en el último año, explica Alberto Tejero que ha quedado claro que las empresas tienen una necesidad clara de protección del dato. Menciona de manera especial la fuga de información, el cifrado de datos o saber cómo se mueven los datos en una compañía, “que para ellas es su core de negocio”.

REPORTAJE ciberseguridadTIC

CATO Networks

Diego Solís, Sales Director of Iberia, CATO Networks

“Se necesita trabajar de manera nativa en el cloud”



“Porque hay ciberdelincuentes”, responde Diego Solís, responsable de CATO Networks en España, cuando le preguntamos por qué ciberseguridad. Recuerda que el perímetro ya no existe y el vector de ataque se ha propagado tanto que se necesita hacer frente a cualquier dispositivo y sistemas electrónico.

Respecto a si el mercado de la Ciberseguridad

va a la velocidad que demanda la Transformación Digital, asegura que sí, pero que para alcanzar esa velocidad de desarrollo, se necesita trabajar de manera nativa en el cloud y no virtualizando appliances, sino aprovechando todas las capacidades que nos da la nube como elasticidad, capacidad de computación. Apuesta Diego Solís por un modelo de arquitectura basada en microservicios que haga que cada nueva funcionalidad o requisito se pueda desarrollar de manera rápida y eficaz para que vaya totalmente alineado con las necesidades del negocio dentro del ámbito de la transformación digital de cada empresa.

Entre las ventajas de Madrid para acoger centros de datos destaca el ser la región líder en fibra en el sur de Europa

En opinión de Diego Solís, lo más destacable de este año tecnológico es esa nueva arquitectura que se está proponiendo en todos los lados y que se llama SASE.

Hornetsecurity

Paul Canales, Head of Channel Iberia, Italy & LATAM, Hornetsecurity

“La ciberseguridad va más rápido de lo que está demandando el mercado”



Tiene claro Paul Canales, responsable de canal en Iberia, Italia y Latinoamérica de Hornetsecurity, que la ciberseguridad siempre ha existido y

REPORTAJE ciberseguridadTIC

que ahora está tomado mucha relevancia porque en los últimos años la ciberdelincuencia se ha profesionalizado; “ya no es un individuo el que ataca, sino una organización delictiva que además se jacta cuando logra hacer un delito a una entidad grande”.

Preguntado sobre si el mercado de ciberseguridad va a la velocidad que demanda la transformación digital, comenta el directivo que “la ciberseguridad va más rápido de lo que está demandando el mercado”. Comenta que existen soluciones muy avanzadas y que se hace un esfuerzo muy grande para que clientes e integradores las conozcan mejor para que las puedan aplicar cuanto antes.

Durante este último año “estamos viendo que el mercado está creciendo mucho, que sigue existiendo demanda de soluciones seguridad, como protección de correo o backup”, comenta Paul Canales añadiendo que se están viendo “una tendencia muy fuerte hacia los temas de concienciación en ciberseguridad”. Recuerda al respecto que la entrada en vigor de la NIS2 va

a implicar que las empresas se vean abocadas a ver cómo forman a sus empleados en ciberseguridad para concienciar de que, al final, el usuario es la última defensa de la empresa.

Infoblox

Joaquín Gómez, director de Ciberseguridad para el Sur de Europa, Infoblox

“No intentes aplicar la ciberseguridad después de que te has transformado”



La seguridad es 100 % necesario, asegura Joaquín Gómez, director de ciberseguridad para el sur de Europa de Infoblox. Añade que las empre-

sas que no adopten capacidades en seguridad, “si no mueren hoy, van a morir mañana” porque el nivel de avance de ataques, de evolución, de intrusiones y de ciberdelincuentes es enorme.

“No intentes aplicar la ciber después de que te has transformado”, dice el directivo de Infoblox asegurando además que la transformación digital va más rápido que el mercado de ciberseguridad. “Intenta que el proceso desde el origen ya lleve la ciberseguridad como base de la transformación”, insiste.

Preguntado por lo que destacaría del último año, menciona Joaquín Gómez el aumento del fraude y la inteligencia que están aplicando los ciberdelincuentes; “son capaces de cambiar la identidad, de elevar los privilegios... y yo creo que es ahí donde debemos intentar adelantarnos”, comentaba el directivo asegurando que es posible apostando por una estrategia más proactiva. Destacaba en este punto la capacidad que tiene la compañía para analizar mundialmente los nuevos dominios para detectar las amenazas antes de que lleguen al mercado.

REPORTAJE ciberseguridadTIC

Ingecom

Carlos Valerdi, Cybersecurity Engineer & Pre-Sales, Ingecom

“2023 ha sido el año de la monitorización”



“Tenemos que entender que la ciberseguridad tiene que ser algo transversal a cualquier negocio”, dice Carlos Valerdi, Cybersecurity Engineer & Pre-Sales de Ingecom, para después añadir que así como hablamos de la seguridad física, tenemos que empezar a hablar de ciberseguridad, que es la seguridad “que protege nuestros activos digitales”.

Sobre si el mercado de ciberseguridad va a la

velocidad que demanda la transformación digital, comenta Valerdi que, siendo cierto que el mercado de ciberseguridad va rápido y que hay un gran avance a nivel de productos de ciberseguridad, “otra cosa es cómo se están adoptando en consonancia con la transformación digital”. Asegura que la transformación digital “todavía es algo muy incipiente”, que a las empresas “les cuesta entender qué es la transformación digital” porque no se trata solo de incorporar tecnología sino que es cambio de paradigma, de forma que “hasta que la transformación digital no se entienda y se adopte como realmente es, la ciberseguridad no puede ir de la mano”.

Sobre lo que ha ocurrido durante el último año destaca Carlos Valerdi que ha sido el de la monitorización. “Hemos visto que muchas empresas están empezando a preocuparse por poder tener un control y monitorizar sus activos, su infraestructura... para poder aplicar las mejoras que necesitan, pero también de anticiparse”, comenta el directivo de Ingecom añadiendo que no solo hace referencia a la monitorización puertas aden-

tro, sino también a la monitorización puertas afuera, “que es lo que llamamos ciberinteligencia”.

ITE

Arantxa Calvo Moyano, Business Development Manager & Strategic Alliances, Integración Tecnológica Empresarial

“La gestión continuada de exposición de amenazas es una tecnología disruptiva”



¿Por qué ciberseguridad? “Porque hay mucha ciberdelincuentes y los ataques se multiplican”, responde Arantxa Calvo, responsable de desarrollo de negocio y alianzas estratégicas de Inte-

REPORTAJE ciberseguridadTIC

gración Tecnológica Empresarial, añadiendo que los ciberdelincuentes “nos llevan un paso por delante, manejan mucho dinero y están siempre evolucionando en sus técnicas de ataque”.

Sobre si la transformación digital avanza a la misma velocidad que la ciberseguridad, dice Arantxa Calvo que deben ir de la mano.

Preguntada por lo que destacaría de este último año menciona la directiva de ITE que la gestión continuada de exposición de amenazas “viene pegando fuerte como tecnología disruptiva”. Explica que por muchas tecnologías que tengan los clientes, es muy difícil reducir el riesgo porque tienen muchos sistemas expuestos. Estas tecnologías de gestión continuada de exposición de amenazas “tienen una aproximación completamente distinta y aplican métodos de remediación sencillos que permite ver el problema de una manera efectiva”, con lo cual estas tecnologías, que vienen a cubrir una parcela que hasta ahora no estaba cubierta, “suponen un paso de gigante en el camino a un estadio más más tranquilo de la ciberseguridad”.

Oracle

**Pedro Llamas Flores, Cloud Engineer Senior
Director para el sur de Europa, Oracle**

“Hay un aumento de la incertidumbre sobre las repercusiones de la IA”



Afirmando que la seguridad ha sido siempre un pilar esencial para Oracle, no cree Pedro Llamas Flores que el mercado de la ciberseguridad esté yendo a la velocidad que demanda la transformación digital. Recuerda que el último estudio del ISC2 sobre la fuerza laboral en ciberseguridad demuestra un incremento del 13 % en la brecha entre la oferta y demanda mun-

Madrid Tech Show es una oportunidad de crear alianzas tecnológicas con soluciones disruptivas

dial de puestos de trabajo en ciberseguridad y que hay un aumento de la incertidumbre sobre las repercusiones positivas y negativas de la Inteligencia Artificial.

¿Qué destacarías del último año en el ámbito de la ciberseguridad? En opinión del directivo de Oracle lo más destacado del último año ha sido “el anuncio de una iniciativa de la industria para diseñar un nuevo estándar abierto de seguridad de redes y datos que ayudará a las organizaciones a proteger mejor sus datos en entornos de TI distribuidos”. Explica que este nuevo estándar permitirá a las redes aplicar colectivamente políticas de seguridad compartidas, mejorando la arquitectura de seguridad que las organizaciones ya utilizan sin necesidad de cambiar las aplicaciones y redes existentes.

REPORTAJE ciberseguridadTIC

Quest Software

César Moro Catalina, Sales Consultant, Quest Software

“Las empresas están intentando ponerse al día en ciberseguridad”



“La ciberseguridad es ahora mismo uno de los puntales básicos de cualquier entorno tecnológico de cualquier compañía”, asegura César Moro Catalina, Sales Consultant de Quest Software, añadiendo que, si no estás protegido a nivel tecnológico todo tu entorno, pues la continuidad de negocio se va a ver afectada en cualquier ataque.

En opinión del ejecutivo de la compañía, el mercado de ciberseguridad no va a la velocidad que demanda la transformación digital, “pero se están haciendo muchos avances”, algo que puede verse en como se está adaptando el uso de la inteligencia artificial para tener nuevos métodos de detección de posibles ataques, respuestas, etcétera.

A la hora de valorar qué ha pasado en el último año, dice César Moro que las empresas están apostando por la ciberseguridad e intentado ponerse al día, por lo que ha aumentado la demanda.

Los Fondos NextGeneration han permitido poner en marcha iniciativas y programas muy transformadores con la colaboración público-privada

S21sec

Ángel Martínez Munuera, Vendor Alliance Manager en S21sec

“Es necesario que entendamos que todo es software”



“Porque tenemos un mundo digital en el que todo está lleno de software”, responde Ángel Martínez Munuera, Vendor Alliance Manager en S21sec, cuando le preguntamos ¿Por qué seguridad? En referencia al título de la ponencia de Begoña Villacís, directora global de Relaciones Institucionales de BeDisruptive. Asegura el ejecutivo de S21sec que, actualmente, nuestra

REPORTAJE ciberseguridadTIC

forma de comunicarnos, nuestra forma de relacionarnos es a través de aplicaciones y que las aplicaciones tienen que ser seguras; “es necesario que entendamos que todo es software”, insiste.

¿Crees que el mercado de ciberseguridad va a la velocidad que demanda la transformación digital? “Claramente no”, responde responde Ángel Martínez Munuera, añadiendo que hay una capacidad de desarrollar software a una velocidad de vértigo y que el mercado de ciberseguridad no termina de entender “que tenemos que estar en el ciclo de desarrollo. Hay herramientas, hay conceptos, hay gente que sabe, pero la realidad es que cuando tú hablas con los clientes no estamos ahí”, asegura.

La identidad digital y el acceso a Internet es algo que, en opinión de Ángel Martínez Munuera, debemos afrontar como sociedad. Recuerda también que el uso “de los ChatGPT de turno” no está llevando a un momento de revolución y que “tendremos que adaptarnos a trabajar con ese tipo de herramientas”.

Semperis

Ray Mills, Spain Sales Director, Semperis

“Tenemos que reevaluar prioridades”



¿Por qué ciberseguridad? “Porque afecta a todo aspecto de negocio”, dice Ray Mills, el responsable de Semperis para España. Recuerda que un ciberataque es una de las razones por el que una compañía podría dejar de funcionar, “así que es crítico tener una estrategia validada para poder asegurar que, si un ataque ocurre, la información está segura”.

No cree el directivo de Semperis que el mercado de ciberseguridad vaya a la velocidad que demanda la transformación digital. Reflexiona que, en ocasiones, la transformación digital termina siendo diferente a lo que esperábamos al comienzo porque surgen necesidades que hace dos o tres años no se habían valorado. También comenta que siempre habrá algo nuevo, una vulnerabilidad, un día cero, y que la estrategia “tiene que ser flexible y adaptarse a las nuevas situaciones y retos”.

Sobre lo percibido durante el último año, comenta Ray Mills que la estrategia de migración a la nube ha evolucionado, que en muchos casos no se ha progresado con la velocidad que se esperaba y que “ahora existe la necesidad de tener que reevaluar prioridades”. Menciona cómo parecía que el Directorio Activo iba a desaparecer “porque todos íbamos a ir a la nube, pero estamos en 2023 y la gran mayoría de las empresas todavía tienen ese componente on-premise, por lo que han tenido que reevaluar su proceso.”

REPORTAJE ciberseguridadTIC

Synack

Alejandro Novo, Country Manager, Synack Spain

“La transformación digital va ligeramente por delante de la ciberseguridad”



Tiene claro Alejandro Novo que la ciberseguridad “es crucial para proteger los sistemas y los datos en un mundo que está conectado digitalmente”. Añade que existe mucha información de usuarios que, de una manera u otra, está expuesta al exterior y es susceptible de ser robada o accedida sin autorización, como son los datos personales, financieros, o médicos, por lo que

hay que establecer medidas “en el camino entre la información sensible y los ciberdelincuentes”. Aunque la ciberseguridad y la transformación digital suelen caminar de la mano, bajo el punto de vista del responsable de Synack en España, “la transformación digital va ligeramente por delante, lo que abre una pequeña ventana de oportunidad para que los ciberdelincuentes desarrollen amenazas cada vez más sofisticadas y complejas”.

Del último año destaca “el continuo incremento de los ataques ransomware y los intentos de robos de información de usuarios en diferentes mercados estratégicos”. Desde la perspectiva de la ciberseguridad, “destacaría la tendencia a reforzar la seguridad en la nube y en los entornos de inteligencia artificial y machine learning”.

Actualmente Madrid alberga 30 centros de datos con una capacidad de unos 250 megavatios

Trend Micro

Raúl Guillén, Cybersecurity Strategy Director, Trend Micro

“La ciberseguridad deber ser un elemento de obligado cumplimiento”



Tiene claro Raúl Guillén que “es fundamental que seamos capaces de incorporar ciberseguridad en fase de diseño en cada uno de los servicios y modelos operativos para evitar que la industria del cibercrimen, que además cada vez está más profesionalizada y organizada, siga atacando de forma sistemática”. Asegura que la ciberseguridad debe ser “un elemento de obligado cumplimiento y de

REPORTAJE ciberseguridadTIC

obligada adopción para asegurar y garantizar que tanto la sociedad, como las empresas, como los servicios esenciales, son resilientes”.

Preguntado sobre si el mercado de ciberseguridad va a la velocidad que demanda la transformación digital, comenta el Cybersecurity Strategy Director de Trend Micro que, históricamente, la transformación digital “ha sido uno de los pilares que ha liderado la inversión y la transformación de los negocios”, y que, como consecuencia de todos los ataques que estamos viendo en los últimos meses, la conciencia y el nivel de madurez en ciberseguridad, “está creciendo por encima del crecimiento de la transformación en sí misma”. Añade que queda mucho por hacer, pero que “hay una oportunidad muy grande para todo el ecosistema, porque la ciberseguridad sigue creciendo año tras año a doble dígito y creo que no estamos viendo nada más que la punta del iceberg”.

Respecto a lo que destacaría de lo ocurrido en el último año, dice Raúl Guillén que se está viendo cómo determinadas tecnologías habilitadoras,

“como la inteligencia artificial, el 5G y el Internet de las cosas, están acelerando el proceso de adopción de determinadas industrias a nivel de modelo operativo”. Añade que la IA en sí misma, “está asegurando y garantizando la eficiencia de los procesos y de las compañías”, y está “democratizando el conocimiento experto, lo que redundará en que se está endureciendo la batalla entre el bien y el mal”.

V-Valley

David Gasca González, Sales & Marketing Manager Cybersecurity Area, V-Valley

“Tenemos tecnología suficiente para protegernos de casi todos los ataques”

¿Por qué ciberseguridad? “Por la exposición que tienen las empresas al mundo digital”, responde David Gasca, Sales & Marketing Manager Cybersecurity Area, V-Valley, añadiendo que “cada vez estamos más expuestos. Todos los datos de las empresas están conectados y necesitamos protegerlos”. Asegura que cada vez hay más vectores de ataque y que la cibersegu-



ridad se ha convertido en un elemento crítico. En opinión del directivo de V-Valley la digitalización avanza demasiado rápido; “muchas empresas ni siquiera lo hacen con recursos capacitados para poder hacerlo de una manera organizada y profesional. Dice también Gasca que “tenemos tecnología suficiente para protegernos de casi todos los ataques”, pero que requiere tiempo el poder implementarlas de la manera correcta.

Respecto a lo que ha ocurrido durante el último año destaca David Gasca el impulso a la gestión de identidades, así como a la protección de la nube, “que está sin proteger”; gestión de los

REPORTAJE ciberseguridadTIC

ataques de denegación de servicios y los entornos de trabajo multi distribuido.

Menciona otro tipo de soluciones que están empezando a adoptar clientes más maduros, “clientes que ya tienen un SOC, una infraestructura y necesitan saber dónde seguir invirtiendo en seguridad”. Habla David Gasca de “soluciones interesantes que te muestran por qué puntos estás más expuesto, qué deberías solucionar y dónde debes seguir haciendo inversiones en seguridad. Y ese tipo de soluciones, la verdad, es que están teniendo mucho interés en el cliente maduro”.

Veracode

Eduardo García Sancho, Country Manager Iberia, Veracode

“La ciberseguridad es algo imprescindible”

Asegura Eduardo García Sancho que la ciberseguridad es algo imprescindible porque los ciberataques están aumentando. Añade además que se debe tener una postura de seguridad capaz de “proteger nuestros activos más valiosos”.



Sobre si el mercado de ciberseguridad va a la velocidad que demanda la transformación digital, comenta el responsable de Veracode para la región de Iberia que depende del sector al que nos refiramos. Estamos viendo ahora mucha ciberdelincuencia en segmento público, “que va mucho más despacio en ciberseguridad de lo que sería deseable”, comenta, añadiendo que, sin embargo, en segmentos como el financiero, la adopción de ciberseguridad va mucho más rápido que la media de otros sectores.

Durante el último año... Veracode ha multiplicado sus cifras y abriendo nuevos sectores con

nuevas herramientas, como la integración de la inteligencia artificial en un segmento en el cual no era muy habitual y para la búsqueda de vulnerabilidades.

XM Cyber

Raúl Pérez, Technical Director, XM Cyber

“Vamos a la velocidad que hay que ir”



No hay más que ver las noticias para darse cuenta de cómo se han incrementado todos los problemas de ciberseguridad y ataques con la guerra de Israel o Ucrania, recuerda Raúl Pérez, Technical Director de XM-Cyber, cuando

REPORTAJE ciberseguridadTIC

le preguntamos por qué ciberseguridad. Dice también el directivo que el gasto en soluciones de ciberseguridad se está incrementando y que cada año nacen cientos de jóvenes empresas con productos novedosos.

Sobre si el mercado de ciberseguridad va a la velocidad que demanda la transformación digital, comenta que muchas veces la velocidad no depende de la transformación o los directivos que la llevan a cabo. “Vamos a la velocidad que hay que ir”, asegura, añadiendo que algunas cosas, si se hacen deprisa, van mal, “sobre todo en seguridad”. Recuerda de hace unos años bastaba con tener un firewall y un antivirus y que ahora cada empresa maneja una media de 40 0 50, por lo que cree que el mercado se está adaptando; “estamos creciendo y vamos a una velocidad de crucero buena”.

Sobre este último año asegura que ha sido “un auténtico terremoto”, que estamos viendo un cambio significativo en lo que es la guerra y que “este año ha sido un punto aparte en cuanto a lo que significa ciberseguridad a nivel de Estado”.

Zerolynx

Juan Antonio Calles, CEO, Zerolynx

“O invertimos en ciberseguridad o la batalla está perdida. No hay muchas más opciones”



Dice Juan Antonio Calles, CEO de Zerolynx, que la ciberseguridad está en auge, y que, hoy en día, “es la diferencia entre que la empresa subsista o se extinga cuando hay un incidente de seguridad, un ransomware, una estafa de alto nivel”.

Preguntado sobre si el mercado de ciberseguridad va a la velocidad que demanda la transformación digital comenta el directivo que el

España se ha convertido en un referente internacional de transformación digital

mercado de ciberseguridad está madurando, que es cierto que la ciberdelincuencia va diez pasos por delante, pero porque “tienen recursos ilimitados”. Menciona la problemática de la inversión en seguridad, y asegura que “en ciberseguridad no hay que mirar tanto el dinero porque esto no es una subasta de pescado. Los clientes tienen que percibir que hay que invertir en ciberseguridad”.

Del último año, lo que destaca Juan Antonio Calles son “los grandes ciberataques a empresas que no nos imaginaríamos que iban a atacar”. Asegura que el hecho de que hayan atacado esas empresas “con todo el dinero que invierten en seguridad es una referencia del grado de madurez que tiene la delincuencia”, lo que refuerza su mensaje: “o invertimos o la batalla está perdida. No hay muchas más opciones”. 