it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Marzo 2022 - nº 50

La CIBERGUERRA se hace realidad

‘La IA nos ayuda muchísimo, pero hay que acompañarla con inteligencia humana’ José Israel Nadal, Age2

Encuentro ITDS. No aborde los desafíos de hoy con las soluciones de ayer: adopte un enfoque centralizado

‘Se tiende a securizar muy bien el dato, y no el dispositivo’ Francisco Moreda, Unidad /fsafe de fibratel

IT Trends. La transformación del puesto de trabajo. Nuevas necesidades de conexión, productividad y seguridad

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

it Digital Security

Directora Rosalía Arroyo, rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez

Diseño revistas digitales Contracorriente

Producción audiovisual Miss Wallace, Alberto Varet

Fotografía Ania Lewandowska

it Digital MEDIA GROUP

Director General Juan Ramón Melara, juanramon.melara@itdmgroup.es

Director de Contenidos Miguel Ángel Gómez, miguelangel.gomez@itdmgroup.es

Directora IT Televisión y Lead Gen Arancha Asenjo, arancha.asenjo@itdmgroup.es

Directora División Web Bárbara Madariaga, barbara.madariaga@itdmgroup.es

Director de Operaciones Ángel Porras, angel.porras@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

La ciberguerra se hace realidad

Hace años que se acuñó el término de ciberguerra, una guerra informática, digital, que traslada el conflicto armado al ciberespacio y que hace de las tecnologías de comunicación e información su campo de operaciones. La guerra fría, sigilosa, que sucedió a la II Guerra Mundial, se ha vivido en el mundo de los ceros y unos desde hace años; los ciberataques atribuidos a las naciones estado no han parado de aumentar y pocas son las grandes potencias que no han entrado en el juego.

Ahora, en pleno siglo XXI, Europa se ve asolada por una guerra con misiles, tanques y cazas. Y muertos. Y mientras en la superficie la destrucción se hace patente, visible, en el mundo digital hackers y ciberdelincuentes lanzan sus ataques. Y es que la guerra también es híbrida.

Además de ciberguerra, en este número de IT Digital Security entrevistamos a José Israel Nadal, el CISO de Age2; Juan Francisco Moreda, responsable de la Unidad /fsafe de fibratel, y a Álex Benito, Senior Manager de Next Generation e IBM en Tech Data Advanced Solutions.

En el terreno de la actualidad son protagonistas Armis y Tehtris. La primera es una empresa a la que poco le queda para lanzar una OPI y hacerse pública, que busca aportar visibilidad en el IT, OT e IoT, y que llega a España de la mano de Vesku Turtia. La segunda es una empresa europea que compite en el mercado XDR con una solución sin agente y una misión: luchar contra el ciberespionaje y el cibersabotaje.

Os resumimos un nuevo #EncuentroITDS, patrocinado por Lacework, en el que se ha planteado cómo afrontar el reto de la seguridad cloud con las tecnologías que están demostrando ser claves en seguridad: machine learning, analítica de conducta y detección de anomalías, y en el que han participado Isaac López, Director de Plataforma de Aplazame; Enric Lluelles, Principal Software Engineer de Factorial; Joan Tomàs i Buliart, Director de sistemas de Marfeel; Mariusz Dekarski, CTO de Ofertia; César Camargo, CEO de Sngular; Luiz Kemmer, Regional Sales Manager EMEA de Lacework; Joan García Regional Sales Manager, Spain & Portugal de Lacework y Ton Machielsen, Sales Engineer de Lacework.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

itds

Sumario

Actualidad

Encuentros ITDS

Entrevistas

‘La IA nos ayuda muchísimo, pero hay que acompañarla con inteligencia humana’

José Israel Nadal, Age2

‘Se tiende a securizar muy bien el dato, y no el dispositivo’

Francisco Moreda, Unidad /fsafe de fibratel

“Crece el interés por la seguridad como servicio”

Álex Benito, Tech Data Advanced Solutions

No solo IT

Ciberseguridad desde una perspectiva diferente

Maica Aguilar Carneros

La era DeFi

José Manuel Navarro

Índice de anunciantes

Revista IT Trends

2021

SONICWALL®

INFORME DE CIBERAMENAZAS

SONICWALL.COM | @SONICWALLSPAIN

A medida que las situaciones de trabajo evolucionaron en 2021, también lo hicieron los **métodos de los actores de las amenazas y los perpetradores motivados**.

En la **actualización semestral del Informe de Ciberamenazas 2021 de SonicWall**, se analiza cómo los actores de las amenazas utilizan cualquier medio necesario (**controles de seguridad laxos, vulnerabilidades sin parches, ataques de día cero y debilidades en la cadena de suministro**) para obtener beneficios maliciosos y provocar disturbios a nivel mundial.

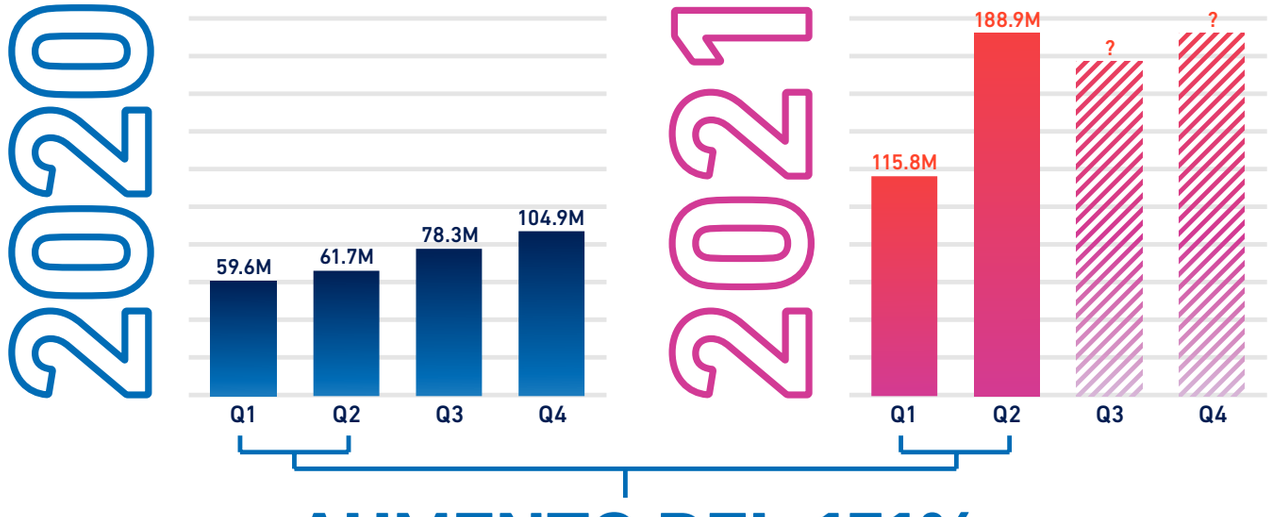
OBTENGA EL INFORME COMPLETO

sonicwall.com/threatreport

EL RANSOMWARE ALCANZA SU MÁXIMO HISTÓRICO

Los ataques de ransomware en el primer semestre de 2021 ya han eclipsado todo el volumen total de 2020: **un aumento del 151% en lo que va de año.**

En los primeros seis meses de 2021, el volumen mundial de ransomware alcanzó la cifra sin precedentes de **304,7 millones** de intentos de ataque.



TENDENCIAS MUNDIALES DE LOS CIBERATAQUES

-22%
2.5 billones
ATAQUES DE MALWARE

+151%
304.7 millones
ATAQUES DE RANSOMWARE

+59%
32.2 millones
ATAQUES DE IoT

+26%
2.1 millones
AMENAZAS CIFRADAS

+23%
51.1 millones
ATAQUES DE CRYPTOJACKING

+9%
2.5 trillones
INTENTOS DE INTRUSIÓN

Armis,
la empresa que viene a resolver la falta de visibilidad

Armis Security es una solución de seguridad sin agentes para el mundo del IoT que permite a las empresas ver y controlar dispositivos y redes no administrados o no autorizados. Fundada en 2015 la compañía abre oficina en España de la mano de Vesku Turtia.

Infatigable. Así nos referimos a un profesional que ha sabido enfrentarse a la dura tarea que supone estrenar marca en España, algo que Vesku Turtia ha hecho con varias empresas. Lo vimos con FireEye y años después con Nozomi Networks y con Cybereason. Ahora vuelve a las andadas con Armis Security, una empresa que en 2019 fue vendida a Insight Venture Partners por 1.100 millones de dólares, que en 2021 levantó 425 millones de dólares en dos rondas de financiación, que actualmente tiene un valor de mercado de 3.400 millones de dólares y se espera que en los próximos meses se haga pública.

De los administrados a los no administrados, las empresas tienen dificultades para identificar todos los dispositivos que las rodean y poder protegerse. Con una tecnología sin agentes, Armis descubre todos los dispositivos y los riesgos asociados en su entorno, detecta amenazas y actúa automáticamente para proteger sus sistemas y datos críticos. Gartner reconoce a Armis como empresa relevante dentro del mercado de seguridad de tecnología operativa, que define como

ARMIS ASSET MANAGEMENT

CLICAR PARA VER EL VÍDEO

Armis es una combinación de plataforma y servicio que destaca por dos elementos clave: funciona sin agente y de manera pasiva

hardware y software que detecta o provoca un cambio a través de la monitorización y/o control directo de dispositivos físicos, procesos y eventos.

Explica Vesku Turtia que Armis no es un producto sino "un servicio y una plataforma que ha venido a resolver y mejorar la situación de siempre: la falta de visibilidad". Establece la compañía tres objetivos definidos: Discovery, Analyze and Protect, que el directivo de la compañía traduce como Inventariado, monitorización continua y protección gracias a las integraciones de una compañía que dice ser "amigo de todos" para que un EDR, un NAC o un CPMD funcionen mejor y que se integra con las herramientas de SOC; "nosotros no somos un SOAR, pero hacemos que el SOAR funcione mejor.

Aunque se relaciona a Armis con el mundo del IoT, asegura Vesku Turtia que es una plataforma que funciona también tanto en el mundo OT como en el IT; "hacemos el inventario de todo tipo de activos, tanto de las herramientas que una empresa puede tener en la nube, como de las que tiene instaladas en los servidores y portátiles". La explosión de los dispositivos IoT ha sido exponencial en los últimos años, "y la fuerza de Armis es que la plataforma tiene una inteligencia de más de dos mil millones de dispositivos que estamos traqueando", dice el directivo, añadiendo que esa cifra les permite haber establecido 20 millones de perfiles de distintos dispositivos que les permite saber, por ejemplo, qué tipo de cámaras IP pueden tener cierto tipo de vulnerabilidades.

Uno de los sectores clave para Armis es el sanitario. Los hospitales están llenos de dispositivos IoT, así como aparatos con versiones obsoletas de sistemas operativos que ya ni siquiera cuentan con soporte. Es una situación en la que un ciberataque puede poner en peligro la vida de los pacientes, una situación en la que la visibilidad,

"Armis ha venido a resolver y mejorar la situación de siempre: la falta de visibilidad"

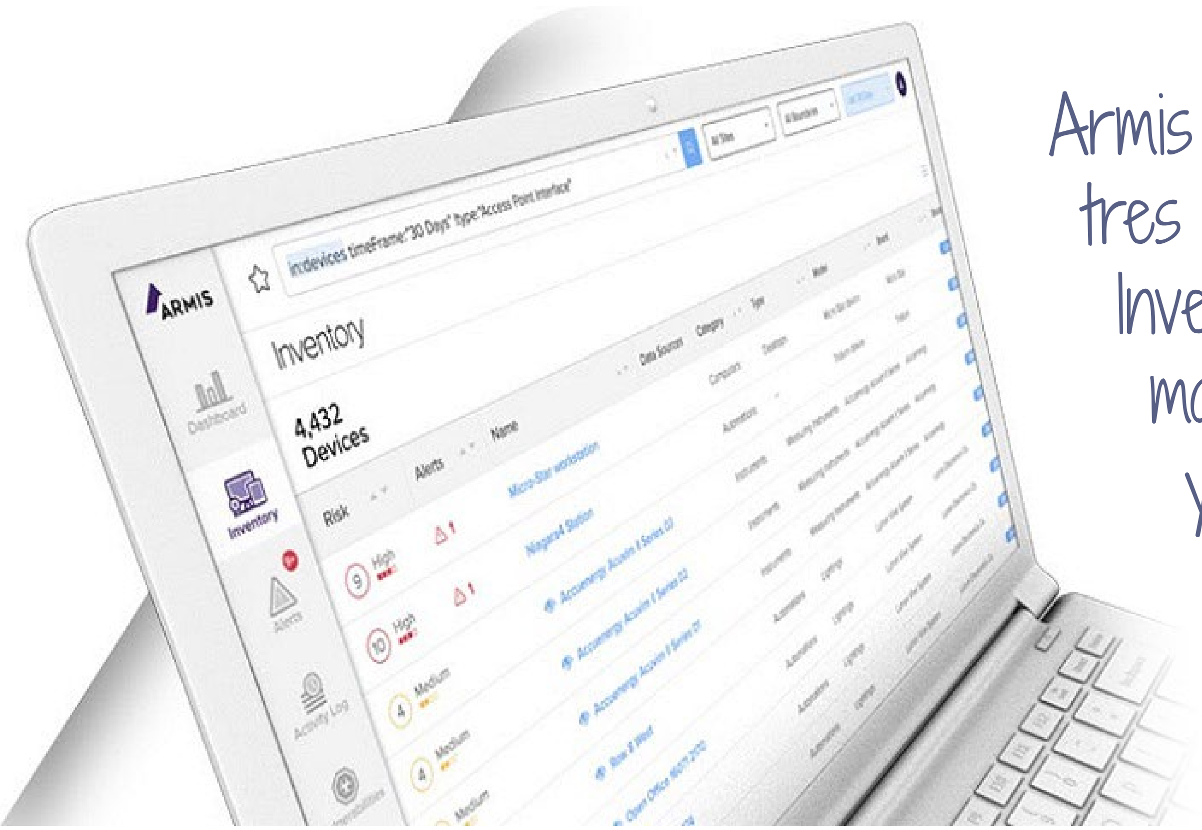
Vesku Turtia,
Regional Sales Director, Armis

el saber lo que tienes en la red para poder gestionarlos y protegerlo es, si cabe, mucho más importante. El inventario, asegura Vesku Turtia, "es un problema desde hace muchos años y Armis nació para resolver ese problema"

Armis Security en España

Los crecimientos de Armis son grandes. La compañía ocupa el puesto número 25 en el Deloitte Fast 500, que reconoce a las 500 empresas de tecnología de más rápido crecimiento en Norteamérica. Hace casi dos años que Armis aterrizó en Europa, donde ya realiza negocios importante en UK o tiene una plantilla de doce personas en Francia. Como es habitual la entrada en los mercado del Sur de Europa, como España o Italia, ha sido más tardía, pero ya están aquí. Hace cuatro meses que Armis Security llega a España de la mano de Vesku Turtia. Y entra fuerte en el mercado. Ya se ha fichado a Rocío Vaquero como responsable de un canal de distribución que se está creando [ya se ha firmado un acuerdo de mayorista con Lidera], en marzo se amplía la platilla con un ingeniero y se buscan dos personas más.

En nuestro país, donde existe tanto el interés como la necesidad de tener una buena visibilidad y monitorización continua, la compañía ya está realizando algunos pilotos. Reconoce Turtia que existen herramientas que te ofrecen un inventario de lo que tienes, pero que los inventarios pueden cambiar de un día para otro y que por eso "la monitorización continua es muy importante", así como el conocimiento de los dispositivos de IoT.



Armis se centra en tres funciones clave: Inventariado de activos, monitorización continua y protección

Enlaces de interés...

- [Armis]
- [Claroty compra Medigate después de recibir una inversión de 400 millones de dólares - 10 DIC 2021]

Clientes

¿Sabes qué es lo que tienes conectado a la red? Es la pregunta mágica que se plantea a los clientes, una pregunta que se lleva haciendo desde hace años, muchos, pero que no termina de calar. La situación actual, no sólo porque los ciberataques son más y más sofisticados, sino por la situación geopolítica, hace que saber dar respuesta a esa pregunta sea de vital importancia.

Las empresas necesitan un enfoque de seguridad pasivo y sin agentes que asegure todo tipo de dispositivos conectados para: generar un inventario completo de todos los dispositivos conectados; asegurarse de que todos los dispositivos y la tecnología sean detectables; ofrecer una cobertura completa para los controles de seguridad, los dispositivos y la comunicación; identifique los riesgos asociados con cada dispositivo; supervisar de forma pasiva el comportamiento y los patrones de comunicación de cada dispositivo y tomar acciones automatizadas para frustrar a los atacantes.

Insiste el responsable de Armis para el mercado de Iberia que hay y ha habido soluciones de inventariado en el mercado, pero no una oferta como la de Armis, una combinación de plataforma y servicio que destaca por dos elementos clave: funciona sin agente y de manera pasiva.

Compartir en RRSS

La educación, uno de los sectores más afectados por el ransomware.

Sophos Endpoint

Intercept X

Bloquee los ataques de ransomware antes de que causen estragos en su entorno con tecnología antiransomware que detecta procesos de cifrado malicioso y los neutraliza antes de que puedan propagarse por la red.

sophos.com/es-es/endpoint

SOPHOS
Cybersecurity evolved.

21-09-20 ES(DD)

Tehtris, el fabricante de XDR europeo que tiene claro que la automatización es el futuro de la ciberseguridad

Única empresa europea en estar presente en el Market Guide of XDR de Gartner, Tehtris se fundó en 2010 y cuenta con soluciones fáciles de implementar que son válidas tanto para multinacionales como para pequeñas empresas.

Marzo 2022

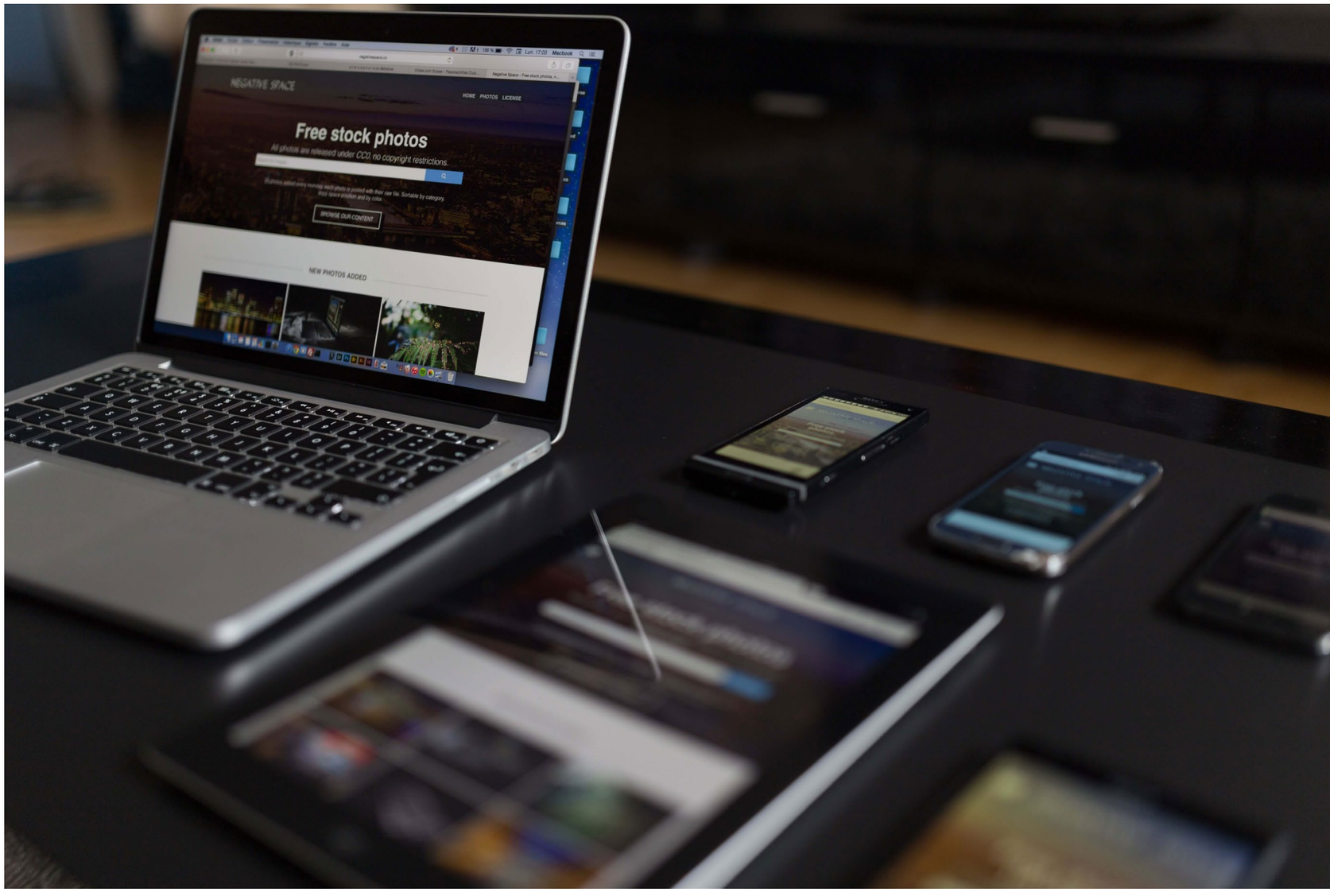
En 2020 Tehtris recaudaba 20 millones de euros en una ronda de financiación Serie A que le permite difundir un mensaje: “proteger las organizaciones públicas y privadas contra los ataques conocidos o desconocidos gracias a una detección y una neutralización de las amenazas en tiempo real y sin acción humana”. Lo asegura Paul Enault, Cybersecurity Business Developer Southern Europe de la compañía, tras anunciar una expansión por Europa que contempla la apertura de filiales en España y Alemania, la creación de equipos comerciales en nuevos territorios, así como con el cierre de nuevas alianzas europeas, que ya se encuentran activas en Suiza, Bélgica y Luxemburgo.

Tehtris comenzó haciendo labores de pentesting hasta que se dieron cuenta de que había que dar un paso más, había que ofrecer una respuesta a todos los fallos que encontraban en sus clientes. Se adentraron en lo que posteriormente se bautizó como el EDR (Endpoint, Detection and Response) y siguieron añadiendo capas de tecnología, así como mucha automatización entre los productos que iban creando. Sin darse cuenta, casi sin que el mercado hubiera creado las siglas que lo definen, la compañía tenía en sus manos una plataforma XDR (eXtended Detection and Response)

Uno de los elementos que definen a la compañía, que le diferencian, es la automatización. Asegura Paul Enault que en Tehtris pronto entendieron

> "Tehtris es una empresa europea orgullosa de ser europea, que aloja los datos en servidores europeos de empresas europeas"
>
> Paul Enault, Cybersecurity Business Developer Southern Europe, Tehtris

El diferencial de Tehtris desde el punto de vista tecnológico es "nuestra capacidad de detección"



que el ser humano no iba a poder hacer frente a ataques cada vez más sofisticados, y que "la automatización iba a ser el futuro de la ciberseguridad".

Jugar en el mundo del EDR/XDR supone competir con un buen puñado de empresas. No sólo con algunas con muchos años de presencia en el mercado que han evolucionado su oferta hacia estos conceptos, sino con otras que, siendo más jóvenes, se han posicionado como referentes. El diferencial de Tehtris desde el punto de vista tecnológico es "nuestra capacidad de detección", dice Paul Enault. Explica que todos hacen detección, pero que antes que nada la compañía era experta en automatización, y gracias a eso "somos muy buenos en detección de amenazas desconocidas".

Otro punto muy importante es la retención de datos; "en lugar de un par de semanas, nosotros vamos a hacer una retención de datos de seis meses, porque en muchos canos nos damos cuenta de que la amenaza, el atacante, ya estaba en el sistema de información de hace mucho tiempo, a veces años. Y gracias a una retención de datos amplificada a seis meses, los analista de seguridad tienen la posibilidad ver mucho más en el pasado y entender cómo entró el atacante en el sistema de información".

Menciona el SOAR (Security Orchestration, Automation & Response) como otro elemento diferenciador de la propuesta de Tehtris, que lo incluye por defecto y sin coste adicional, junto con un CyberThreat Intelligent, en su plataforma.

Otro punto diferencial de la compañía francesa es tener "una visión muy ética de la ciberseguridad" en

Tehtris está en medio de una expansión por Europa que contempla la apertura de filiales en España y Alemania este año

Enlaces de interés...

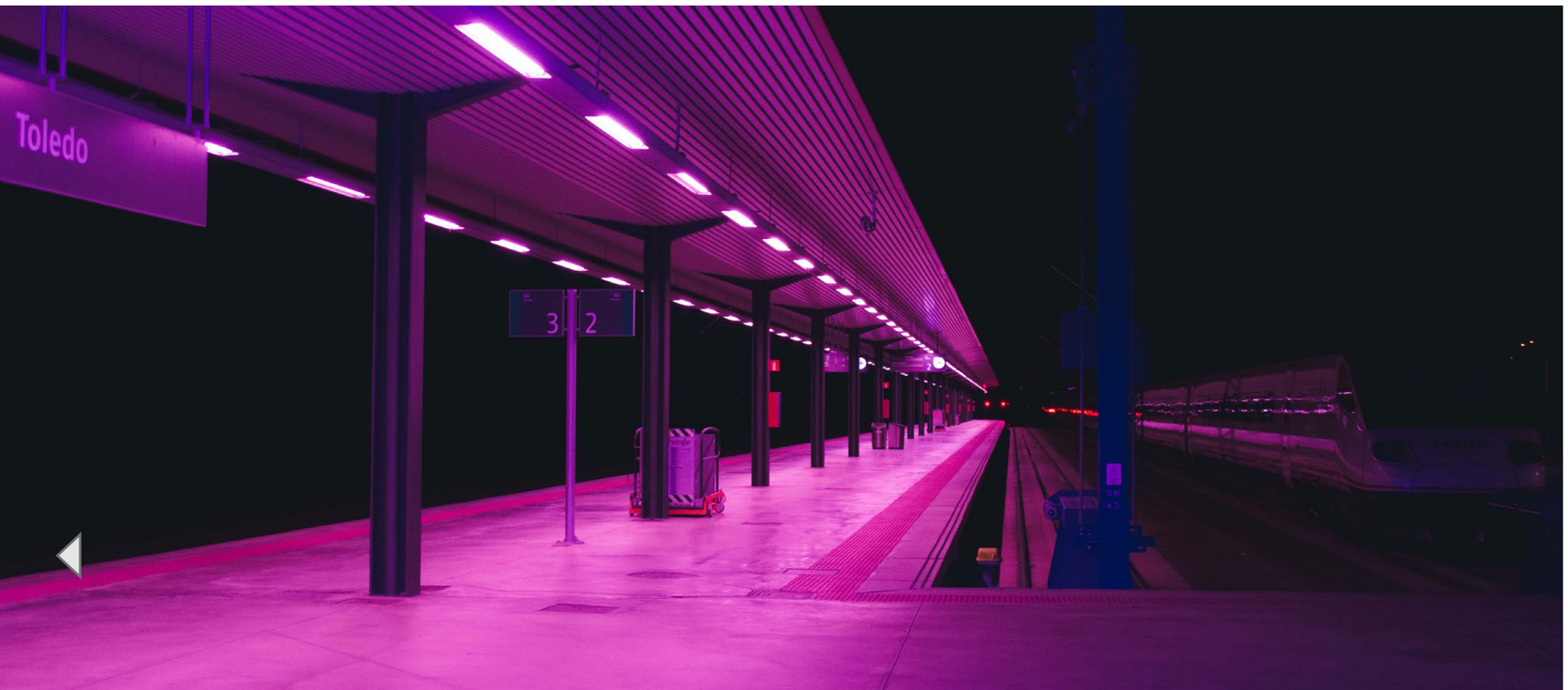
- Las empresas priorizarán la automatización de la ciberseguridad en 2022
- Tehtris

cuando a que se ha limitado la cantidad de operaciones que se pueden realizar de forma manual y la cantidad de información que se va a filtrar, que se hará de manera muy segura.

Por último, "Tehtris es una empresa europea orgullosa de ser europea, que aloja los datos en servidores europeos de empresas europeas".

Clientes

Las ofertas de detección y respuesta, sean EDR, XDR o NDR, no son fáciles de gestionar en cuanto que generan un montón de información que después hay que analizar. Son, por lo tanto, un gran reto para muchos clientes que adoptaron esta nueva moda sin saber muy bien dónde se metían. ¿Cuántas empresas están preparadas para adoptar una solución de detección y respuesta? Habla Paul Enault de un mercado dividido en tres capas: empresas muy pequeñas, micropymes, poco maduras a nivel tecnológico, con poco presupuesto y que piensan que van a ganar la guerra con un antivirus; el mundo pyme, que ya tiene un conocimiento más avanzado y algo más de presupuesto que están buscando un bundle EPP-EDR o EDR-SIEM; una tercer capa que son las grandes cuentas, con mucho conocimiento y presupuesto y que habla de XDR y de automatización. Hecha la división, asegura el directivo de Tehtris que la compañía busca negocio en el segmento alto y medio del mercado porque no solo ofrecen un XDR, sino que han creado soluciones a medida, como un bundle que une EDR y SIEM "a un precio muy competitivo y con una configuración preestablecida más fácil de desplegar".



Compartir en RRSS

STORMSHIELD

La opción europea en ciberseguridad

El partner de confianza
para
securizar sus
infraestructuras operacionales y sensibles

www.stormshield.com

‘La IA nos ayuda muchísimo, pero hay que acompañarla con inteligencia humana’

(José Israel Nadal, Age2)

José Israel Nadal Vidal es el CISO de Age2, un proveedor de servicios tanto de ciberseguridad como de gobierno de TI o cloud. El cargo le llega después de su paso por el Ministerio de Defensa donde se dedicaba más a las TI, hasta que en 2003 empezó a adentrarse en el mundo de la ciberseguridad formando parte de equipos de Red Team y gestión de vulnerabilidades hasta convertirse en CISO, cargo que ha ocupado en diferentes empresas desde hace más de tres años.

Rosalía Arroyo

Como CISO de un proveedor de servicios tiene la labor de proteger tanto la empresa como los propios servicios de ciberseguridad que provee, que en muchas ocasiones se encarga de testear, un proceso en el que tiene mucho valor su experiencia como miembro de un Red Team. Además, como auditor de la ISO 27001, asesora a ciertos clientes que quieren empezar a desplegar una base normativa. Se le suman a este responsable de seguridad conocimientos de protección de datos, todo lo cual ayuda a acompañar a los clientes “no sólo en la parte tecnológica sino en la parte normativa”.

Sobre la evolución de la figura de CISO, que dice que “ni existía” cuando empezó en el mundo de la ciberseguridad, asegura que ha ido cobrando fuerza dentro de la empresa, la misma que ha cobrado la información, convertida en pilar fundamental de los negocios.

Le preguntamos si cree que la ciberseguridad se ha convertido en una prioridad para la empresa española para que nos responda que no, que “está lejos de ser una prioridad”, entre

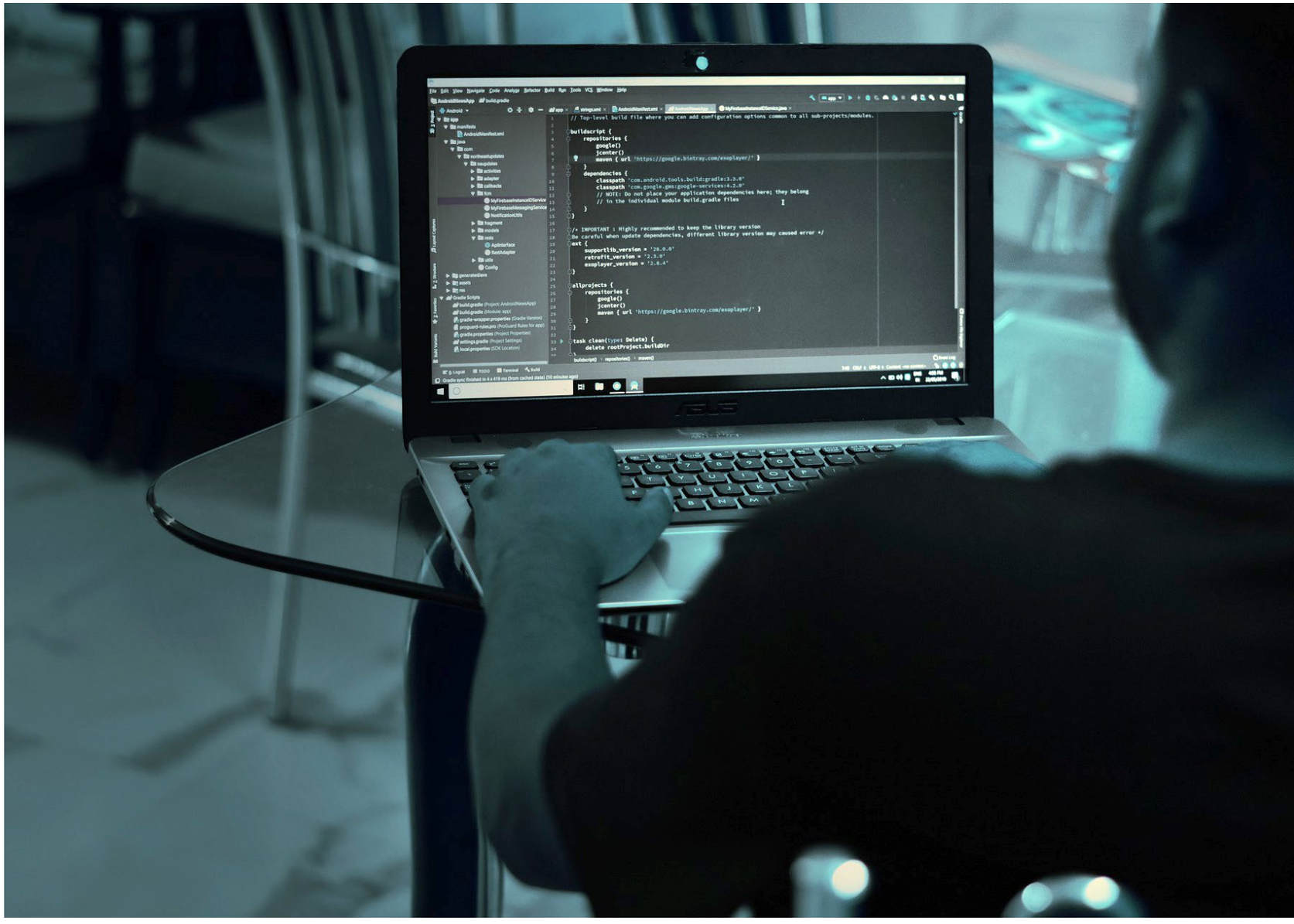
"La amenaza que más me preocupa es la que afecta a los entornos industriales o infraestructuras críticas"

otras cosas porque es difícil calcular su retorno de la inversión, que en ciberseguridad se llama ROSI (Retorno sobre la Inversión en Seguridad). Recuerda también José Israel Nadal Vidal que cada día atacan a más empresas y es entonces cuando se acuerdan de que tenían los sistemas mal configurados, o fallos en su seguridad.

"Amenazas me quitan el sueño todas", responde el CISO de Age2 cuando le preguntamos qué amenaza le desvela, especificando que la que más le preocupa es la que afecta a los entornos industriales o infraestructuras críticas, y otras que cuesta más detectar, como las amenazas persistentes avanzadas (APTs).

Sin querer darle un peso específico, para José Israel Nadal la concienciación del usuario es un elemento muy importante dentro de la seguridad. Asegura que la ciberseguridad es un camino, no un destino, y que "todos hacemos ciberseguridad", para después comentar que ha visto sistemas muy protegidos "que se han venido abajo con el click de un usuario".

"Las tecnologías relacionadas con Zero Trust serán necesarias en el futuro"



En cuanto a la inteligencia artificial, cada vez más presente en cualquier tecnología, incluida por supuesto la de seguridad, ¿cómo confiar en que es tan inteligente como pensamos? Dice el directivo de Age2 que la IA "nos ayuda muchísimo", pero que "hay que acompañarla con inteligencia humana, que es al final las que es capaz de discernir si un ataque es un falso positivo". Añade además que nos queda IA para rato, "una IA mejor porque estará más entrenada".

"Lo básico es pelearte para obtener presupuesto", dice el CISO de Age2, que además es profesor docente en la Escuela Internacional de Gerencia, cuando le preguntamos por tecnologías básicas de seguridad que deberían ser imprescindibles en cualquier empresa. Además de un antivirus, que es lo más básico que se puede tener, José Israel Nadal recomienda un SIEM para tener visibilidad de lo que ocurre, además de un operador de SIEM, porque "llegado el caso de un incidente podemos prevenirlo o tener capacidad forense para poder ver qué ha pasado".

Asegura también este directivo que ve un creciente interés entre los jóvenes por la ciberseguridad. "Una de las facetas buenas de ser profesor es que también aprendo con ellos", dice, Nadal, que además de hacking ético enseña los secretos de la tecnología SIEM. Habla de la necesidad de formación y certificación constante como un posible elemento de desmotivación, junto con la presión de pensar si te has visto atacado; "tiene cierto desgaste", dice el directivo recordando que se tiene que luchar por los presupuestos, con los clientes y con los usuarios.

"La ciberseguridad está lejos de ser una prioridad en la empresa española"

Respecto a las tecnologías que serán necesarias en un futuro menciona el CISO de Age 2 las relacionadas con Zero Trust "que, no siendo un concepto innovador, porque hace tiempo que existe, sí se ha visto impulsado por la experiencia del COVID, el teletrabajo y la descentralización". Recuerda que el perímetro se ha perdido y que cada vez hay más servicios y más usuarios conectándose desde distintas partes del mundo con diferentes dispositivos, por lo que "será necesario adoptar filosofías Zero Trust".

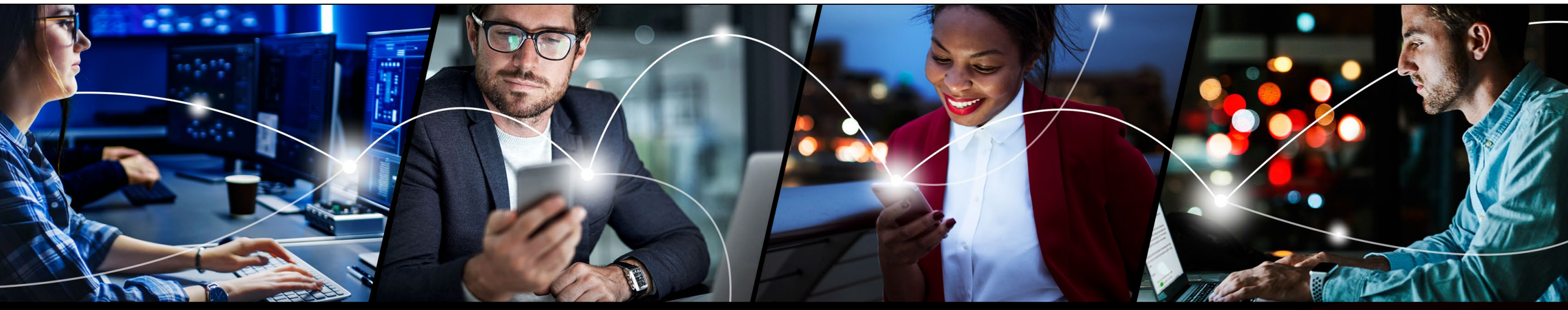
Sobre el futuro, dice el directivo que el ransomware, que no deja de aumentar y hacerse más sofisticado, es algo que ve cada día y que obliga a recordarles a sus clientes la importancia de las copias de seguridad; que le preocupan los ataques contra entornos industriales, donde nos encontramos con máquinas con más de 20 años, cuando no se pensaba en la seguridad, o con gente que no ha tenido que preocuparse por la ciberseguridad.

Enlaces de interés...

- "Resisten los que se adaptan" (Belén Pérez, CISO, Grupo Nueva Pescanova)
- 'Identificar los roles críticos en la organización, que no necesariamente son los del comité de dirección, es fundamental' (Gabriel Moliné, Leroy Merlín)
- 'En los próximos años la tendencia en ciberseguridad será el análisis de comportamiento' (Mario Andrés, Mercadona)
- 'Identificar los roles críticos en la organización, que no necesariamente son los del comité de dirección, es fundamental' (Gabriel Moliné, Leroy Merlín)

Compartir en RRSS

Seguridad unificada para un mundo RECONECTADO



SEGURIDAD DE RED

AUTENTICACIÓN MULTIFACTOR

NUBE SEGURA WI-FI

SEGURIDAD ENDPOINT

Unified Security Platform™

CLARIDAD Y CONTROL | **SEGURIDAD INTEGRAL** | **CONOCIMIENTO COMPARTIDO** | **ALINEACIÓN OPERATIVA** | **AUTOMATIZACIÓN**

Contacto: +34 917 932 531

Email: spain@watchguard.com

www.watchguard.com

‘Se tiende a securizar muy bien el dato, y no el dispositivo’

(Francisco Moreda, Unidad /fsafe de fibratel)

Las empresas están buscando una revisión de su estado de seguridad. Así lo asegura Juan Francisco Moreda, el responsable de /fsafe, la unidad de ciberseguridad de fibratel, un integrador global de soluciones IT. Dice que hace tiempo que las empresas están cambiando, adoptando entornos híbridos, y eso les está llevando a interesarse por su estado de ciberseguridad, “cómo están y qué necesitan mejorar”, sobre todo después de que la pandemia sanitaria provocara un cambio con demasiadas prisas.

Rosalía Arroyo

En cuanto a las amenazas que más les preocupan, menciona los ataques a la cadena de suministro. Explica que las empresas quieren saber cómo controlar esa cadena de suministro, que los accesos de los proveedores a los datos empresariales sean lo más restringidos posible; “cómo confiar en que esa empresa externa cumple con unos requisitos mínimos de seguridad, o que tiene el mismo nivel de seguridad que tienes tú”. Asegura que es un tema que siempre está sobre la mesa y que a lo que se tiende es “a securizar muy

"La ciberseguridad se mueve de manera continua, y lo que tenemos que hacer es formarnos día a día para poder ayudar a nuestros clientes"

bien el dato y no tanto el dispositivo", dando permisos sobre ese dato dependiendo de quién accede y desde dónde.

Además, a las empresas les preocupa el ransomware, un ransomware que ha evolucionado mucho y para el que ya no basta con tener una buena copia de seguridad. "Muchas veces nos encontramos con que la recuperación tras el ataque es muy rápida y muy sencilla, pero poco después empiezan a pedir dinero porque han exfiltrado un montón de datos y amenazan con hacerlos públicos", dice el directivo de fibratel, que ayuda a sus clientes a tener visibilidad de lo que ocurre con sus datos, sus usuarios y sus dispositivos "para no trabajar de manera reactiva frente a un ransomware, sino proactiva".

Servicios gestionados

"La ciberseguridad se mueve de manera continua, y lo que tenemos que hacer es formarnos día a

"Hay ciertos automatismos, pero necesitas gente. Por eso el MSSP es, a día de hoy, algo primordial"

día para poder ayudar a nuestros clientes", dice el responsable de /fsafe, asegurando que la oferta de servicios gestionados es la que más está creciendo.

Explica que un gran porcentaje de los clientes de fibratel son empresas con entre 100 y 500 empleados, con departamentos de IT reducidos y poca dedicación a una ciberseguridad que cambia muy rápidamente, que exige estar aprendiendo y revisando lo que se tiene de manera constante "porque hay ciertos automatismos, pero necesitas gente. Por eso el MSSP es, a día de hoy, algo primordial".

Menciona Juan Francisco Moreda los servicios de firewall o SWG gestionado como parte de la oferta de /fsafe, además de realizar análisis en busca de vulnerabilidades que les ayuden a corregirlas indicándoles a través de un informe cuál de ellas corre más prisa parchear.

Cambio acelerado

Asegurando que la pandemia ha cambiado tanto la forma de vivir como la de trabajar, explica Moreda que las empresas se vieron obligadas a realizar una serie de cambios que afectaban a sus empleados y que les llevó a acelerar la adopción de la nube o levantar VPNs de un día para otro. Es algo "a lo que se han acostumbrado rápidamente, pero han perdido el foco de seguridad", dice el directivo de Fibratel. Añade que muchas empresas ya se han dado cuenta de ello "y se está viendo más inversión en tecnologías que securizan la cloud, además de en la parte de concienciación".

Pasamos de hablar de SASE para centrarnos en SSE; se avanza con Zero Trust hasta que nos topamos con Cybersecurity Mesh… ¿cómo se sigue el ritmo? "Muchos clientes preguntan de manera específica por estos conceptos y confían en nosotros

"Se está viendo más inversión en tecnologías que securizan la cloud, además de en la parte de concienciación"

Enlaces de interés...

- "El dato es algo primordial y hay que protegerlo muy bien" Juan Francisco Moreda, Fibratel
- Sólo tres de cada diez pequeñas empresas españolas protege su página web
- La preocupación por la ciberseguridad es el mayor obstáculo para adoptar la nube

para adoptarlos de la manera adecuada", dice Juan Francisco Moreda. En todo caso, añade, la mayoría de estas siglas hacen referencia a conceptos que llevan mucho tiempo en el mercado, pero que se reinventan bajo un mismo nombre.

A la hora de escoger a los fabricantes con los que trabajar, /fsafe pone foco en "buscar lo que cuadre mejor con el tipo de cliente con el que trabajamos y que sea una mejora para ellos"; también se tiene en cuenta el feedback de clientes y lo que dicen las consultoras teniendo muy claro que "no podemos ir a todos los fabricantes, porque para poder dar un buen servicio tengo que conocer bien el producto y tener gente formada".

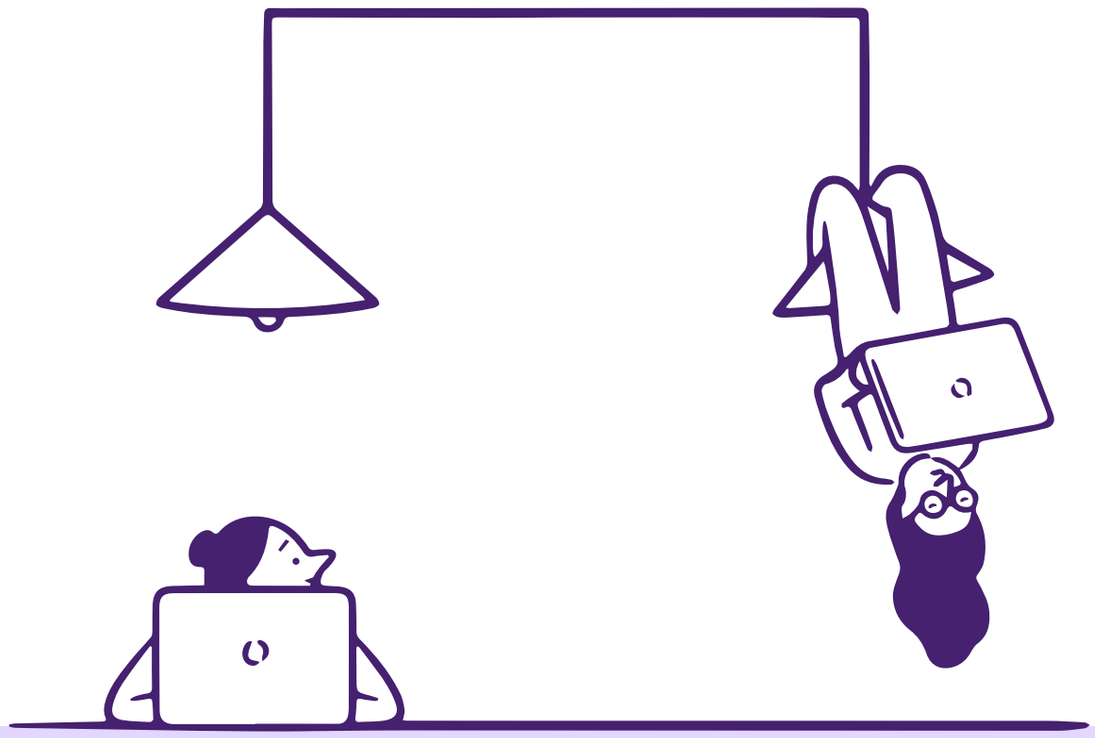
Entre la amplia variedad de fabricantes con los que se trabaja nos llama la atención Cohesity, sobre la que nos cuenta Moreda que se está dando a conocer en el mercado de copias de seguridad porque es inmutable a ataques de ransomware, es cloud nativa y fácilmente escalable.

La compañía tiene una amplia oferta tecnológica que va desde el NGFW a la protección endpoint, SWG, seguridad del email, SD-WAN, CASB, Cloud Security, Seguridad OT, Backup, MFA & Zero Trust, escaneo de vulnerabilidades y BAS y NAC. Una lista en la que el peso de cada una de estas propuestas dentro de la facturación global, va de más a menos.

A futuro no se prevén cambios radicales. Seguiremos viendo, reflexiona el responsable de /fsafe, cómo muchas empresas van a seguir caminando hacia la transformación digital.

Compartir en RRSS

Tus empleados
se merecen una
tecnología tan
única como ellos.



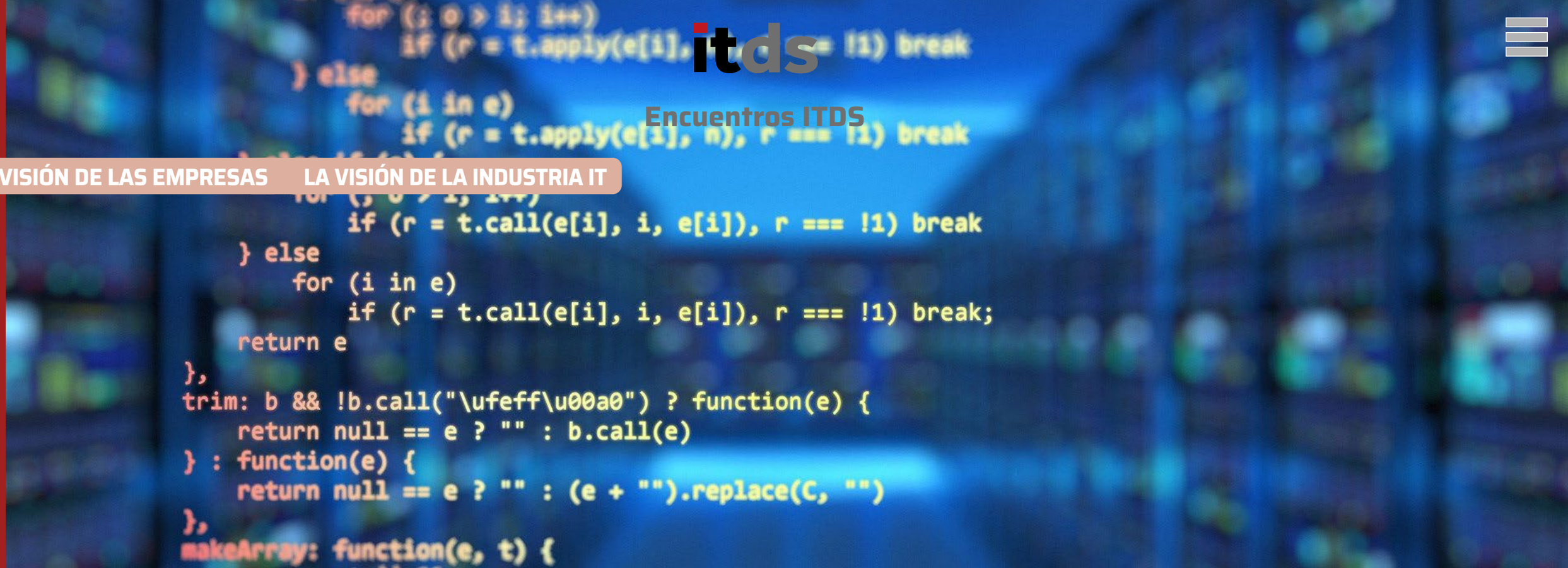
citrix™

No aborde los desafíos de hoy con las soluciones de ayer: **adopte un enfoque centralizado**

Organiza: it Digital Security

Patrocina: LACEWORK

Marzo 2022



No aborde los desafíos de hoy con las soluciones de ayer: adopte un enfoque centralizado

Asumido el reto de la nube, no así la seguridad de la misma, son ahora los contenedores y microservicios los que marcan la diferencia, ayudando a algunas de las empresas de software más innovadoras a transformar sus procesos de desarrollo de aplicaciones y su infraestructura de TI para lograr una eficiencia sin precedentes.

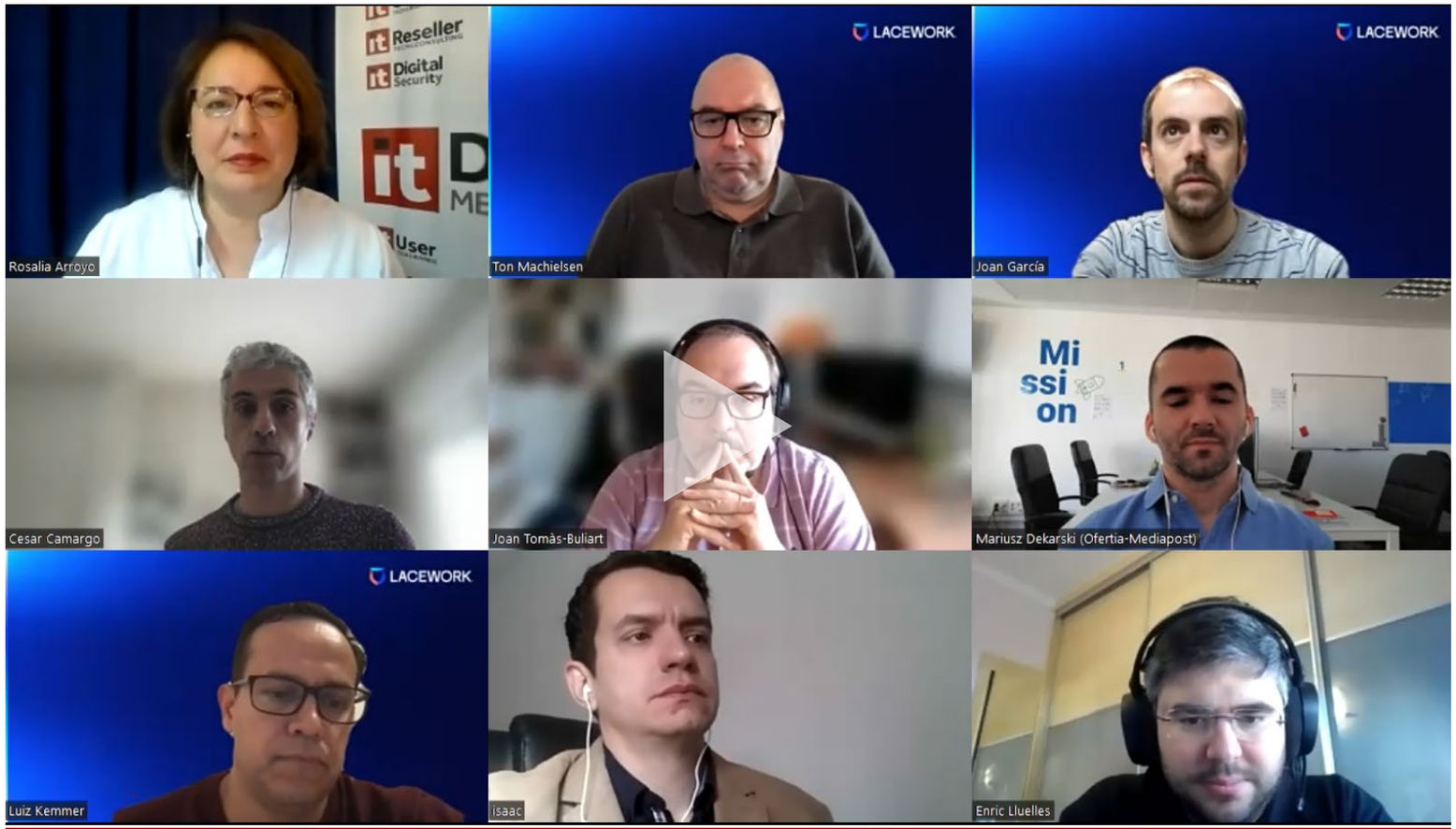
La historia más reciente nos demuestra que la seguridad tiene que ir de la mano de los avances. Acompáñanos para saber cómo afrontar el siguiente paso y proteger las cargas de trabajo en la nube, añadir seguridad a los contenedores, controlar la actividad de APIs y usuarios, descubrir vulnerabilidades, garantizar el cumplimiento, monitorizar la integridad de los archivos y, en general, añadir mayor visibilidad y seguridad a los entornos cambiantes de manera automática.

Cómo afrontar el reto de la seguridad cloud con las tecnologías que están demostrando ser claves en seguridad: machine learning, analítica de conducta y detección de anomalías, ha sido uno de los objetivos de un encuentro patrocinado por Lacework en el que han participado Isaac López, Director de Plataforma de Aplazame; Enric Lluelles, Principal Software Engineer de Factorial; Joan Tomàs i Buliart, Director de sistemas de Marfeel; Mariusz Dekarski, CTO de Ofertia; César Camargo,

itds

Encuentros ITDS

LA VISIÓN DE LAS EMPRESAS LA VISIÓN DE LA INDUSTRIA IT



ENCUENTROS ITDS
NUEVOS ENFOQUES PARA LA SEGURIDAD DE HOY

CLICAR PARA VER EL VÍDEO

CEO de Sngular; Luiz Kemmer, Regional Sales Manager EMEA de Lacework; Joan García Regional Sales Manager, Spain & Portugal de Lacework y Ton Machielsen, Sales Engineer de Lacework.

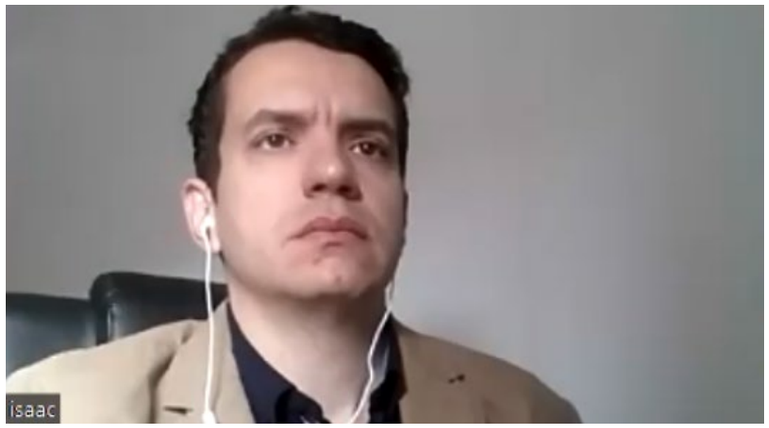
El debate arrancaba con la bienvenida de Luiz Kemmer, Regional Sales Manager EMEA, Lacework, una compañía experta en monitorizar y detectar de manera efectiva configuraciones incorrectas, vulnerabilidades y amenazas en su entorno de nube. Se habló de principales retos a los que se enfrentan las empresas, se planteó un cambio en el enfoque de seguridad por la adopción masiva de los servicios en la nube, cómo se ha afrontado la implementación de contenedores o si la visibilidad, en arquitecturas cada vez más complejas, es suficiente.

it whitepapers

IMPACTO FINANCIERO DE LACEWORK

Este documento es una versión abreviada de un estudio encargado por Lacework y realizado por Forrester para calcular el impacto económico de proteger los entornos multinube frente al valor que los clientes de Lacework obtienen para su negocio.

LA VISIÓN DE LAS EMPRESAS



"El aplicar técnicas de control automático (DevSecOps) para enviar código rápidamente a producción puede ser un arma de doble filo"

Isaac López, Aplazame

Isaac López, Director de Plataforma,
APLAZAME

"Uno de los retos principales a los que se enfrenta una organización es la posibilidad de tomar decisiones enfocadas a la seguridad. Al igual que se sigue la tendencia de tomar decisiones orientadas por los datos en organizaciones Data Driven, es necesario aprovechar los mismos en términos de seguridad y que las decisiones lleguen a toda la organización sin olvidar ningún escalafón", asegura Isaac López, el Director de Plataforma de Aplazame. Explica que la transmisión de conocimiento en cuanto a buenas prácticas respecto a la seguridad deben llegar a través de cursos de formación a todos los empleados. El que haya una nueva "exigencia" en el día a día de un empleado es a veces muy complicado ya que las jerarquías de responsabilidad y la capacidad de los equipos no dejan margen para acometer estas nuevas peticiones.

Para Isaac López la adopción de servicios nativos en la nube no ha tenido un impacto importante en la seguridad. Habla más de un cambio en la exposición desde el punto de vista de que "hoy en día cualquiera puede acceder a tutoriales para ejercitar un ataque donde el objetivo puede ser la página principal o el portal de acceso de empleados/clientes de una compañía. Evidentemente estos accesos están lo suficientemente protegidos frente a ataques más estándares", pero Isaac indica que "si el atacante quisiera seguir investigando podría profundizar, gracias al acceso abierto a esta información que existe en la red. Ejemplos son los **Zero Day Exploit** cuyo análisis se detalla en ocasiones mucho antes de tener una solución disponible."

Planteado si la implementando de servicios en contenedores ha cambiado la superficie de ataque y si ha impactado en la mayoría de las políticas de seguridad, dice el Director de Plataforma de Aplazame, "la superficie de ataque no se ve afectada por el utilizar contenedores sino por el modo en que estos se usan para desplegar una solución productiva. Si antes se desplegaba un "paquete" de software y ahora se dispone un aplicativo contenerizado, ambos podían estar expuestos al mismo tipo de ataques. La diferencia radica en que es necesario conocer la tecnología

y entender cómo se está desplegando la solución. En este sentido técnicas de análisis de vulnerabilidades en los contenedores con herramientas de análisis automático sobre los pipelines de construcción y despliegue en CI/CD son grandes apoyos para mitigar el problema.”

“Todo el mundo somos conscientes de la importancia de escribir código seguro”, dice Isaac López pero “el aplicar técnicas de control automático (DevSecOps) para enviar código rápidamente a producción puede ser un arma de doble filo”, ya que según comenta “el confiar en éstas puede no ser suficiente” así añade que “la educación, en este caso de los desarrolladores, vuelve a ser un reto”. Habla también de la responsabilidad que tienen ahora los desarrolladores en cuanto a que tiene que tratar datos confidenciales de cliente y cumplir con normativas como GDPR, lo que lleva a que “ya no solo hay que preocuparse de un ciberataque que genere una escalada de privilegios o modificar una configuración, sino controlar un adecuado acceso a esos datos”.

“Los proveedores de Cloud son muy conscientes de la necesidad de tener un control de los activos”, responde Isaac López cuando le preguntamos por la visibilidad de los entornos cloud. Asegurando que aunque no es posible conseguir un 100% de seguridad, los proveedores son los primeros interesados en ofrecer esa visibilidad “y que están haciendo un buen trabajo prueba de ello son las certificaciones que ofrecen en sus plataformas o las soluciones transversales de control dentro de sus portfolios”

Enric Lluelles, Principal Software Engineer, FACTORIAL

"Mantener los niveles de cumplimiento cuando cada semana se añaden nuevos servicios es un reto"

Enric Lluelles, Factorial

El crecimiento del equipo, que se ha triplicado en los últimos años, ha llevado a que se haya hecho complicado mantener el control de las políticas. Lo asegura Enric Lluelles cuando le preguntamos por los retos a los que se enfrenta su empresa. Menciona también el reto del cumplimiento para una empresa que cada semana añade nuevos servicios y tiene que hacer frente a la agestión de contraseñas, el uso de SSO (Single Sign On), credenciales y privilegios, que ha llevado a la creación de un equipo específico de seguridad. Se evoluciona también hacia un enfoque más proactivo de la seguridad con la creación de un equipo con conocimientos internos y capaz de buscar exploits.

Plantea Enric Lluelles, Principal Software Engineer de Factorial, que en un entorno de adopción de servicios nativos cloud hay que plantearse quién es el responsable de verificar que la unión entre dos cuentas o servicios en un proveedor de nube no ha generado ningún exploit que deje a alguna de las partes abiertas al mundo; "en nuestro caso el responsable siempre ha sido el equipo de infraestructura y sistemas", pero la adopción masiva de servicios hace "que el equipo que debería gestionar esta unión y este control de privilegios se convierta en un cuello de botella. El principal problema ha sido gestionar esto".

Tener conocimiento de dónde están los datos es algo que afecta a todas las arquitecturas, y con los contenedores no ha sido diferente, asegura Enric Lluelles, añadiendo que la principal afectación de Factorial es encontrar el punto ideal en el que los containers te dan la rapidez arquitectural y al mismo tiempo "mantener el nivel de compliance que nos han marcado los clientes a medida que nosotros como empresa pasamos de tener un target de clientes SMB a clientes un poco más Enterprise".

¿Es posible enviar código rápidamente integrando seguridad y cumplimiento? "Supongo que sí, pero de lo que estoy seguro es que es más complicado", responde Enric explicando que en las nuevas arquitecturas en las que muchas partes interactúan entre ellas, "ser consciente en todo momento de esas interacciones, de qué información sensible pueden dejar por ahí y qué vulnerabilidad exponen al resto del mundo cada vez es más difícil".

"La pregunta es corta, pero la respuesta es difícil", asegura Enric cuando le planteamos si tiene visibilidad de todos sus activos. Las tareas de pentesting ayudan a comprobar que sí que se tiene ese control y se es proactivo en la búsqueda de herramientas y buenas prácticas "que nos hagan la vida más fácil".

"Tener una monitorización continua de qué hay desplegado, qué recursos tienes y qué estás haciendo es básico"

Joan Tomàs i Buliart, Marfeel

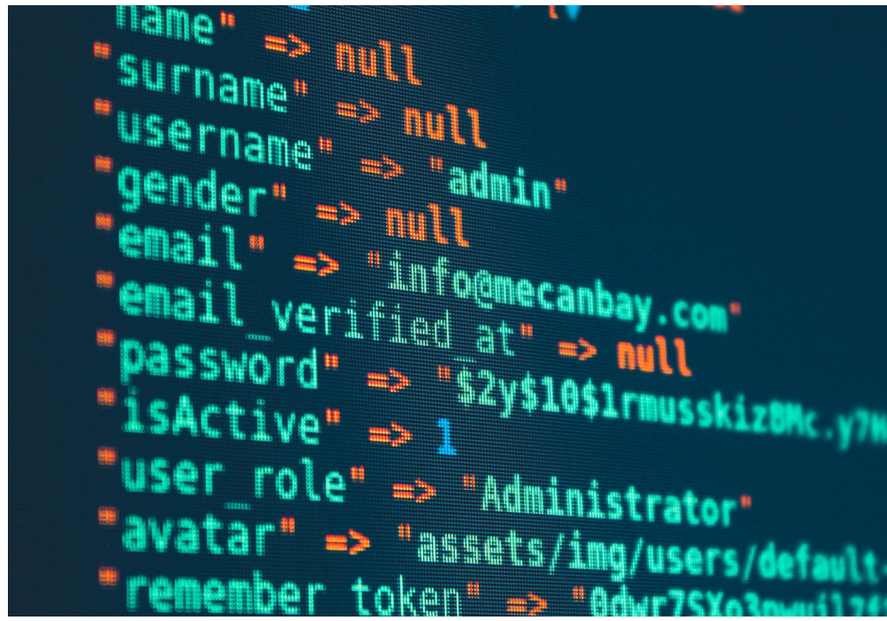
Joan Tomàs i Buliart, Director de sistemas, MARFEEL

Asegurando que en los últimos dos años ha cambiado el paradigma de Marfeel por la apertura de una nueva vertical de negocio basada en analítica que ha incrementado muchísimo el tráfico, explicaba su director de sistemas que tener una explosión de servicios "supone que hacer un mínimo seguimiento de qué está pasando en cada uno de esos microservicios sea un reto a nivel de monitorización y también en la parte de código".

Preguntado por la complejidad que añade la adopción de servicios nativos cloud en las empresas, explica Joan Tomàs i Buliart que Marfeel arrancó hace diez años directamente en cloud, lo que ha permitido, por ejemplo, que la gestión de usuarios quede muy bien documentada, y que "haya una trazabilidad en el código que gestiona esa infraestructura". Menciona que también se utilizan herramientas que machean lo que hay desplegado y lo que dice tu código que tiene que haber desplegado, "lo que hace que todo sea mucho más simple". Aseguran también el directivo que "tener una monitorización continua de qué hay desplegado, qué recursos tienes y qué estás haciendo es básico".

Recoge el director de sistemas de Marfeel que la adopción de contenedores permite "hacer un primer análisis claro de lo que vas a desplegar y saber qué vulnerabilidades y qué problemas tiene antes de que lo despliegues. En este sentido yo creo que ahí hemos ido a mejor". Asegura también que los estándares y herramientas existentes están ayudando a adoptar unas buenas prácticas que al final se reflejan en la calidad de lo que se acaba desplegando, "aunque a veces se descuida la seguridad del sistema de despliegue, que es quién despliega ese artefacto".

Cuando planteamos si se entiende la importancia de escribir código seguro, menciona Joan Tomàs i Buliart el problema que existe a la hora de encontrar este tipo de perfiles; "nos apoyamos en herramientas y poco a poco se va poniendo la óptica de la seguridad dentro del desarrollo", pero es complicado en cuanto a los conocimientos que hay que



tener, y depende del marco normativo y el tipo de datos que usa una aplicación.

"Asegurar al cien por cien que no se me escapa nada de mi infraestructura es extremadamente difícil", asegura Joan Tomàs i Buliart, añadiendo que cada vez se van cubriendo más cosas y que se cuenta con sistemas que permiten crear alarmas donde se tienen muy en cuenta lo que ha ocurrido en el pasado para decidir si la situación actual es normal, o no.

Mariusz Dekarski, CTO, OFERTIA

Entre los retos a los que se enfrentan las empresas asegura Mariusz Dekarski, CTO de Ofertia, que se “prioriza el sacar nuevas funcionalidades y no se piensa en seguridad hasta que llegamos a un momento que es crítico”, una falta de entendimiento que dice ser preocupante. Se suma la falta de expertos que colaboren a la hora de establecer los niveles de riesgo y saber qué se necesita para hacer un despliegue de manera segura; “si falta este know-how no sabes cómo prepararte, y solo puedes responder”, asegura el directivo.

Menciona también Mariusz Dekarski el reto que aún supone adoptar la nube para muchas empresas, “que no saben cómo establecer las reglas de seguridad y preparar sus entornos”, así como el reto, eterno, del presupuesto.

Habla más de continuidad que de disrupción Mariusz Dekarski cuando planteamos cómo ha cambiado el enfoque de seguridad con la adopción de servicios nativos en la nube. Asegura que en Ofertia lo que se lleva es hacerlo todo en un modo de infraestructura como código, lo que facilita la gestión de políticas y usuarios; “tenemos control absoluto de quién tiene acceso a qué recursos”, dice el directivo, añadiendo que la capa de monitorización permite detectar la actividad sospechosa.

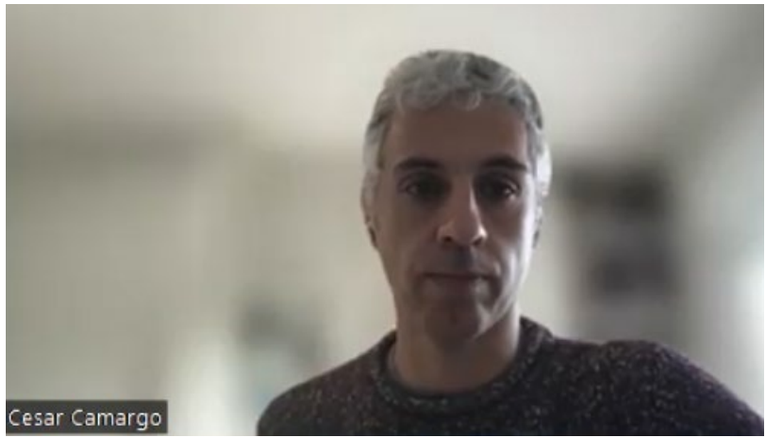
Asegurando que los contenedores son un medio para hacer microservicios y preparar toda la infraestructura para este tipo de arquitectura, menciona el CTO de Ofertia que el control de seguridad a nivel de accesos entre servicios, a redes o VPC es fundamental.

Reconoce Mariuz Dekarski que en ocasiones se trata la seguridad como un enemigo del desarrollo porque lo frena y añade horas de trabajo, y que en estos casos lo que ayuda es la formación de los desarrolladores.

Realizar una monitorización en todas las capas posibles ayuda a tener controlados todos los activos y obtener una visibilidad en sistemas cada vez más complejos. Las herramientas de detección de anomalías que ayudan a dar respuesta a los problemas son importantes, así como la aplicación de estándares como una línea base que permite poder vigilar si algo sale fuera de él, dice Mariusz Dekarski.

"Adoptar la nube sigue siendo un reto para muchas empresas"

Mariusz Dekarski, Ofertia

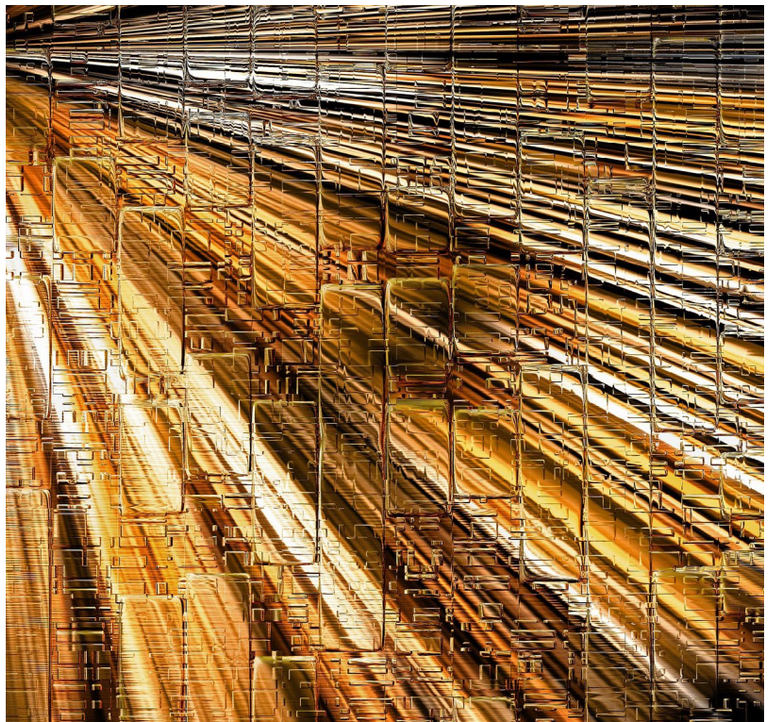


César Camargo, CEO, SNGULAR

"Lo más importante es que entendamos que la seguridad es parte de tu propio equipo multidisciplinar"

César Camargo, Sngular

"Las amenazas que en realidad estaban latentes pero que no percibíamos tanto, se han hecho mucho más visibles a más miembros de las organizaciones, incluidos los equipos de desarrollo", dice César Camargo, CEO de Sngular, cuando planteamos cuáles son los retos a los que se enfrentan las empresas. Añade el directivo que "a estas altura nadie se plantea un desarrollo en un entorno mínimamente corporativo sin tener ciertas bases seguras, sin tener ciertos chequeos realizados y sin algún tipo de plataforma o herramienta que te soporte en esos procesos".



El directivo está de acuerdo en que la gestión de servicios nativos en la nube se ha disparado y ha añadido mayor complejidad a la gestión de la seguridad, sobre todo cuando se trabaja en grandes clientes y verticales muy regulados.

Recuerda César Camargo los tiempos en lo que se hablaba de tener una docena de aplicaciones en un en un servidor web, "y jamás te plantearías cientos, ni mucho menos miles, que es lo que nos permiten los contenedores". El siguiente paso, continúa, es securizar ese contendor, que al estar basado en código es "mucho más gestionable de lo que tendríamos en los modelos anteriores"; recuerda también que la existencia de estándares y el uso extendido de los contenedores hace que se vaya mejorando la seguridad de los mismos, y reconoce que la exposición se ha multiplicado porque "tenemos que tratar cada contenedor como una identidad".

¿Se entiende la importancia de escribir código seguro? "Se va entendiendo, pero tenemos mucho trabajo que hacer ahí", responde César Camargo, añadiendo que cada vez se apuesta más por el Agile Testing, pero que aún no se ha conseguido que la seguridad se vaya consolidando desde el principio y se considera parte del proyecto. "Eso es algo que la industria tiene que empujar", dice el CEO de Sngular para terminar diciendo que "para mí lo más importante es que entendamos que la seguridad es parte de tu propio equipo multidisciplinar".

"Asumiendo que la seguridad completa no existe y que la visibilidad completa tampoco, de lo que se trata es de poner recursos y herramientas para conseguirlo, sobre todo cuando tu infraestructura empieza a crecer", responde César Camargo cuando planteamos durante el debate si tiene visibilidad de todos sus activos. Comenta también que en arquitecturas cada vez más complejas la generación de alertas y la capacidad de detectar es muy valiosa, pero que lo que hoy parece suficiente, lo que hoy parece válido, no se verá así dentro de unos años.

LA VISIÓN DE LA INDUSTRIA IT

LACEWORK

Durante su intervención Joan García, Regional Sales Manager para España y Portugal de Lacework, confirmaba que los retos y situaciones planteadas por los portavoces de Aplazame, Factorial, Ofertia, Marfeel y Sngular coinciden con lo que la compañía percibe en el mercado, empezando porque "nadie adopta cloud, contenedores y una arquitectura basada en microservicios per sé, sino con el objetivo de ser ágiles en el desarrollo".

Aseguraba también el directivo que las aproximaciones clásicas de la ciberseguridad siempre se han basado en definir lo que estaba bien y lo que estaba mal a través de reglas y de listas negras y blancas, y que al final "esas reglas no dejan de ser puertas que ponen freno a la rapidez que aporta esta nueva ola tecnológica de cloud, microservicios y contenedores".

Afirmaba también el responsable de Lacerwork para el mercado de Iberia que el mundo de la seguridad y el mundo del desarrollo tienen que trabajar unidos para poder ir rápido sin renunciar a la seguridad. Aseguraba que la clave para resolver esta problemática en este mundo moderno es unir el Build-Time con el RunTime, porque puedes desplegar toda con infraestructura y usuarios como código, controlando los permisos y quién puede hablar con quién, pero, "¿y si en el RunTime algo no va bien? ¿y si alguien gana acceso al plano de control y crea usuarios, cambia permisos, despliega máquinas que no estaban en los scripts de infraestructura como código? ¿cómo nos damos cuenta a tiempo de que ha habido un comportamiento anómalo en el RunTime?". En el mundo de contenedores y microservicios entender si se levanta un proceso que no toca en un contenedor que no toca y contacta a otro microservicio que no toca "es un reto para los equipos de seguridad porque es de una complejidad tremenda".

Ton Machielsen, Sales Engineer, Lacework

Aseguraba también Joan García que se han visto amenazas en las que lo que se ha hecho es atacar el repositorio, inyectar un código malo en una librería que luego se está usando en las aplicaciones, y es aquí donde está el futuro de la seguridad: en saber detectar que alguien, o algo, no está funcionando como debiera mediante la detección del comportamiento anómalo en tiempo real".

Durante el debate se planteó un caso de éxito, el de una Fintech española cuyo reto era el

"El mundo de la seguridad y el mundo del desarrollo tienen que estar unidos para ir rápido"

Joan García, Lacework

conseguir visibilidad para mantener el compliance de una manera continua bajo el riesgo de perder su licencia bancaria. Trabajar con Lacework les permitió, con un despliegue muy corto, tener una visión real de todos los puntos de marco normativo, y a qué distancia estaban de su cumplimiento.

Explicaba Luiz Kemmer, Regional Sales Manager para la región de EMEA de Lacework, que "para el CISO, que contaba con un equipo de tan solo tres personas, esta visibilidad supuso una ventaja enorme", además de poder mirar en el runtime las anomalías existentes.

Comentaba Ton Machielsen, Sales Engineer de Lacework, que en relación con la visibilidad hay varios aspectos a tener en cuenta. Por un lado, la gestión de activos, que exige tener visibilidad de todo lo que tenemos, y por otro lado "la gestión del rendimiento y la gestión de la seguridad, que son aspectos que están interrelacionados porque una brecha de seguridad puede provocar una anomalía en la gestión del rendimiento".

Mencionaba el caso de Log4Java ocurrido a finales de 2021 para plantear que quién hubiera pensado que en un entorno en el que está todo controlado y no hay anomalías "una aplicación Java hablara con un servidor LDAP para descargar un payload en un servidor web"; aseguraba que nadie ha creado reglas preventivas para este comportamiento y cómo, desde el punto de vista de la visibilidad, lo importante es detectar como anómalo un comportamiento en el que confiamos, algo que no se ha visto antes. "Hemos de tener visibilidad en este tipo de comportamientos", concluía.

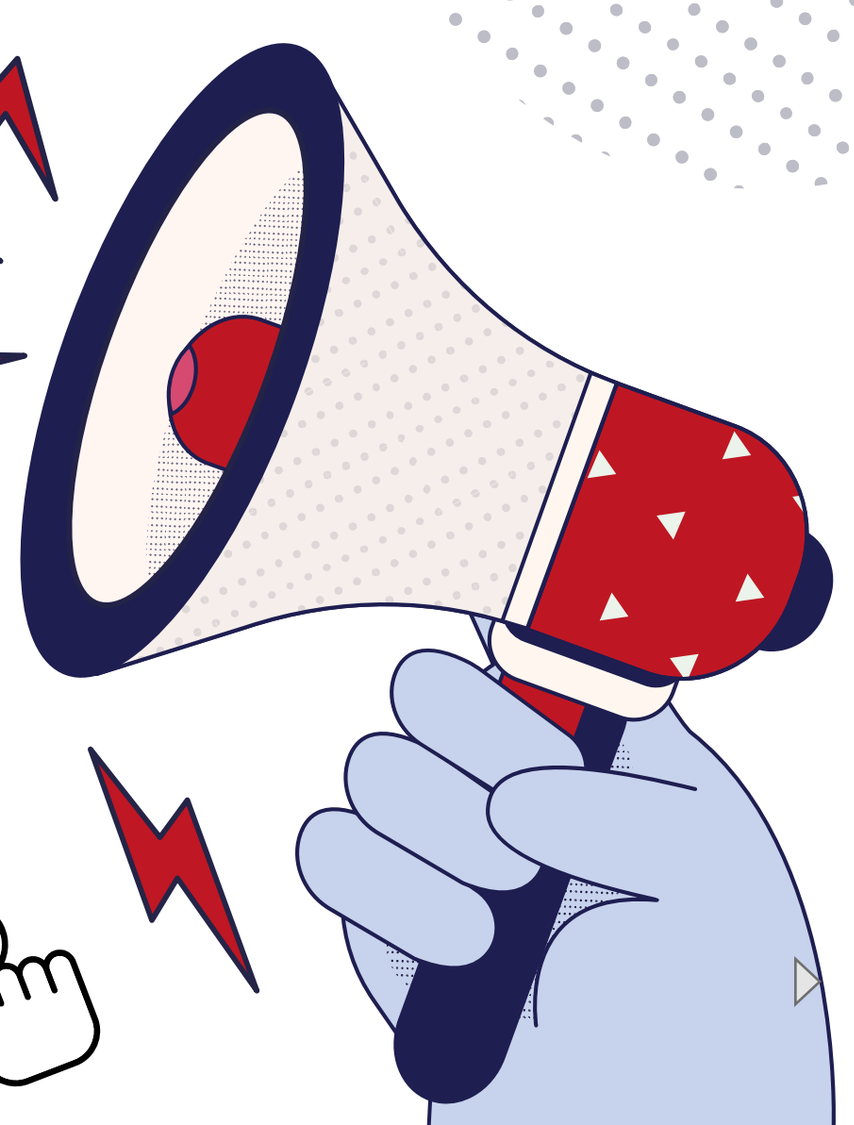
Luiz Kemmer, Regional Sales Manager EMEA, Lacework

Administración Pública Digital

NUEVA WEB

¡VISÍTANOS!

www.administracionpublicadigital.es



“Crece el interés por la seguridad como servicio”

(Álex Benito, Tech Data Advanced Solutions)

Iniciado el negocio de seguridad con fabricantes pure player, hace años que Tech Data Advanced Solutions se abrió a los grandes proveedores del mundo de IT con un negocio de ciberseguridad que ha ido evolucionando hacia modelos de MSSP y una oferta diferencial.

“Soluciones de seguridad que sean sencillas, tanto en la implementación como en la gestión”. Esto es lo que el mercado demanda según Álex Benito, Senior Manager de Next Generation e IBM en Tech Data Advanced Solutions, un mayorista que trabaja con grandes empresas con un negocio importante de seguridad, como pueden ser IBM, VMware o Cisco, además de otros fabricantes específicos. De manera más concreta dice que las empresas piden herramientas que les ayuden a cumplir con la normativa, incluidas tecnologías de doble factor de autenticación (2FA), gestión de cuentas privilegiadas, etc.

Menciona también el directivo que cada vez tienen más clientes con SOC propios en los que se está invirtiendo, lo que pone de manifiesto que el Soc-as-a-Service es tendencia, aunque, en opinión de Álex Benito, “aún no es un mercado maduro”.

¿Cómo ha ido evolucionando el negocio de ciberseguridad en Tech Data? “Hay diferencia entre Tech Data Internacional y Tech Data España, donde se empezó más tarde”, responde el directivo. Inicialmente el foco se puso en los pure player, los

fabricantes “que tienen un foco exclusivo en seguridad, son especialistas y son muy valiosos para todo el canal”, entre los que se incluyen RSA, SonicWall, Radware, Stormshield o Lookout. Sin dejar de lado a este grupo, hace un par de años Tech Data miró también hacia los grandes proveedores del mundo de IT con un negocio de ciberseguridad importante como IBM, Cisco, VMware o Micro Focus, “con los que estamos teniendo mucho éxito” y con buenas perspectivas para el futuro. De forma que “empezamos con pure players, hemos seguido con los más generalistas y ahora mismo seguimos trabajando las dos vertientes”.

Sin contar con fabricantes especialmente disruptores en su oferta, asegura el directivo de Tech Data Advanced Solutions que con los que trabajan se cubren todas las áreas de ciberseguridad que necesita cualquier empresa y que lo que se busca cuando se analiza un nuevo fabricantes “es que realmente ofrezca una solución diferencial, algunas peculiaridades que sean interesantes, y que se establezca una buena relación entre ambas partes”. A la hora de buscar, o aceptar, nuevas incorporaciones “la decisión se basa más en lo que pueden aportar a nuestros clientes que en lo que podrían aportarnos a nosotros”.

"Las arquitecturas de seguridad han evolucionado para intentar dar respuesta a la desaparición del perímetro tradicional"

Preguntado por el impacto que la experiencia de Tech Data en el cloud a la hora de potenciar, o no, su negocio de ciberseguridad, dice Álex Benito que ha facilitado las sinergias entre un mundo y otro, “y nos va a facilitar mucho más el crecimiento en el mercado de ciberseguridad”. Explica el directivo que desde hace tiempo se mantienen reuniones entre el área de cloud y el área de ciberseguridad para, dentro del portafolio de Tech Data, “ofrecer servicios de ciberseguridad basados en cloud”.

“El de los MSSPs es un mundo complejo”, asegura Álex Benito. Dice que es un mundo que está evolucionando mucho “justo en la línea que hemos comentado: el desarrollo por nuestra parte de un portfolio de servicios profesionales que además de este mix entre cloud y seguridad, se pueden ofrecer de manera local o internacionalmente”. Añade el directivo que este tipo de servicios está ayudando a los MSSP, o futuros MSSP, “porque la posibilidad de dar servicios profesionales está ayudando a transformar el canal”.

Define como “curiosa” la reacción del mercado en el área de ciberseguridad en tiempos de pandemia. Al comienzo de la misma esperaba Álex Benito que la inversión en ciberseguridad fuera enorme debido a la pérdida definitiva de perímetro de seguridad dentro de las empresas, y la necesidad de tener que poner más seguridad alrededor del endpoint y del usuario. Si bien es cierto que el negocio de ciberseguridad creció, “no fue tanto como algunos esperábamos”, dice, añadiendo que lo que sí se ha visto es que las arquitecturas de seguridad han evolucionado para intentar dar respuesta a la desaparición del perímetro tradicional.

El de ciberseguridad es un mercado en constante evolución. Pasamos de hablar de SASE para centrarnos en SSE; se avanza con Zero Trust hasta que nos topamos con Cybersecurity Mesh… ¿cómo se sigue el ritmo? Responde Álex Benito que no se ha producido un gran cambio entre lo que se pensaba en seguridad hace uno o dos años y lo que

"La posibilidad de dar servicios profesionales está ayudando a transformar el canal"

A la hora de trabajar con nuevos fabricantes lo que pesa es lo que pueden aportar a los clientes

se piensa ahora, “aunque es verdad que cada día aparecen siglas nuevas y que lo que hay detrás de ellas son conceptos muy importantes en los que trabajan todas las empresas que se dedican a la seguridad”.

Asegurando que todo lo que se ofrece como servicio es tendencia desde hace años, para este 2022 espera Álex Benito un mayor interés por las soluciones SASE y mayor foco en la ciberseguridad como servicio.

Enlaces de interés...

- Tech Data Advanced Solutions
- `No descartamos la compra de un mayorista para crecer en el área de seguridad´: Santiago Méndez, de Tech Data

Compartir en RRSS

FORO it Digital Security

SASE

EL FUTURO DE LA SEGURIDAD DE LA RED

EVENTO ONLINE,
28 DE ABRIL DE 2022

IT TRENDS

MARZO 2022

La transformación del puesto de trabajo:

nuevas necesidades de conexión, productividad y seguridad

UNA PUBLICACIÓN DE IT Digital MEDIA GROUP

it TRENDS

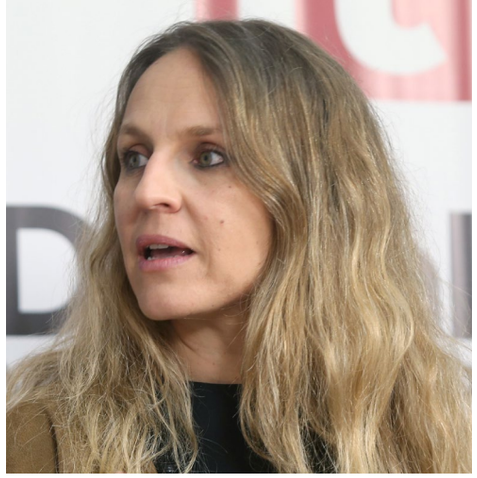
Directora Arancha Asenjo arancha.asenjo@itdmgroup.es
Subdirectora Susana Herrero susana.herrero@itdmgroup.es
Redacción y colaboradores Alberto Varet, Ricardo Gómez, Hilda Gómez, Arantxa Herranz,Reyes Alonso
Diseño revistas digitales Eva Herrero
Producción audiovisual Miss Wallace, Alberto Varet
Fotografía Ania Lewandowska

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es
Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es
Directora IT Events & Lead Gen Programs
Arancha Asenjo arancha.asenjo@itdmgroup.es
Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es
Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

La empresa distribuida se convertirá en el modelo más común



Mucho se ha hablado en estos dos últimos años sobre los cambios en el modelo de trabajo. Pasada la urgencia de mantenerse aislados y seguir siendo productivos, las empresas empezaron a plantearse un formato híbrido que permita -cuando sea posible- compaginar el teletrabajo o trabajo en movilidad y el desempeño de la labor en las instalaciones corporativas.

Según Gartner, éstas son las empresas que están en el camino correcto. La consultora estima que, en 2023, el 75% de las organizaciones que viren hacia un concepto de empresa distribuida verán crecer sus ingresos un 25% más rápido que sus competidores. Vale la pena, por tanto, plantearse la adopción de esta fórmula, para la que los responsables de IT deberán implantar, como mínimo, nuevas formas de colaboración para trabajadores en remoto y on premise, acceso remoto seguro, gestión de la experiencia digital del empleado, y automatización de las operaciones de TI. De forma concreta, esto supone incorporar suites de colaboración y aplicaciones en cloud, autenticación multifactor, acceso a la red Zero-Trust, plataformas cloud nativas, analítica del puesto de trabajo, o gestión del endpoint, entre otros.

De todas estas soluciones, del nivel de madurez alcanzado por las empresas en estas estrategias de puesto de trabajo digital y seguro, y de las mejores prácticas para implantarlo, hablamos en el último Encuentro IT Trends "Transformación del trabajo. El empleado conectado", en el que participaron **Logitech, NFON, Check Point, WatchGuard, CITRIX, Canon, SonicWall y ESET**, con la visión práctica del puesto de trabajo en la Administración Pública de la mano de **ASTIC** y del sector privado con **Haya Real** Estate.

En nuestras páginas podrás encontrar también otros reportajes y contenidos que toman el pulso a la adopción de las TIC en sectores tan diferentes como son la universidad y la construcción.

Además, adelantarte que nos convertimos en una revista bimestral. El próximo número lo tendrás en tus manos a mediados de abril. Mientras tanto, puedes seguir la actualidad de las tendencias tecnológicas en nuestra web www.ittrends.es. ■

Arancha Asenjo
Directora IT Trends

itTRENDS

El cambio tecnológico y cultural en el paradigma de la universidad digital

Tras el esfuerzo de habilitación inmediata de sistemas digitales que permitieran la continuidad de las actividades educativas en los inicios de la pandemia, el futuro de las enseñanzas superiores conlleva un cambio organizativo, cultural y tecnológico que integre las tecnologías emergentes situando al estudiante en el centro para recuperar el papel de liderazgo de la Universidad en la transformación social.

Según los últimos datos publicados por el Ministerio de Universidades, en España existen 83 universidades y, de ellas, 33 son privadas. Con la llegada de la pandemia, el conjunto del sistema universitario español sufrió el mayor impacto de su historia, al margen de conflictos bélicos, viéndose obligado a habilitar en tiempo récord sistemas digitales para continuar su funcionamiento de forma remota.

Tal como refleja el Informe CYD 2020 de la Fundación conocimiento y Desarrollo, casi el 86% de las universidades llevaron a cabo medidas para adaptar su actividad docente a un modelo online antes del 14 de marzo de 2020 y cerca de un 90% cerró sus instalaciones, al menos parcialmente. De la noche a la mañana, el porcentaje de enseñanzas totalmente online que impartían las universidades españolas presenciales pasó de un 5% a más del 83%. ¿Un milagro?

UNA DIGITALIZACIÓN QUE COMENZÓ HACE AÑOS

Lo cierto es que, aunque en parte fue absolutamente asombroso, el sistema universitario español ya llevaba varios lustros adaptándose a las demandas de una sociedad cada vez más digitalizada. Sobre todo en el ámbito privado, con entidades más flexibles y, por tanto, menos resistentes al cambio.

"Las universidades que ya estaban inmersas en esta adaptación antes de la época de pandemia han podido hacer frente, de una manera más efectiva, a la situación que nos ha tocado vivir e incluso aprovechar esta coyuntura de cambio obligatorio para avanzar en sus procesos de transformación. En U-tad, fuimos capaces de adaptarnos muy rápidamente a las necesidades especiales que supuso la crisis de la COVID-19 porque contábamos con la experiencia de metodologías de formación en formato híbrido", afirma Pilar López, directora de Tecnología Académica y E-Learning en el Centro Universitario U-tad.

En la misma línea, se manifiesta Emiliano Blasco Doñamayor, vicerrector de Transformación Digital en la Universidad CEU San Pablo: "en el CEU, la apuesta por la tecnología y la innovación es tradicional y lo venimos haciendo como parte de nuestra vocación docente y de servicio desde el principio de nuestra actividad como institución educativa".

Tras el hito marcado durante el confinamiento con un gran esfuerzo por parte de toda la comunidad educativa, ahora se trata de afrontar una transformación digital fruto de la reflexión y la planificación que conduzca al paradigma de la universidad digital. Una universidad que, como asegura el propio Blasco Doñamayor reclamando su posición de liderazgo, "es desde siempre el centro de la cultura e innovación en la sociedad y su misión debe estar orientada a este fin".

Cristina Villalonga, directora de Global Campus Nebrija de la Universidad Nebrija, se extiende un poco más y añade que la Universidad no solo tiene que saber adaptarse a los cambios tecnológicos, sino también a los cambios sociales, culturales y profesionales. En su opinión, debe estar conectada con el contexto y el entorno, y abierta a un proceso de reflexión, reinvención e innovación continuo para poder dar respuesta a las necesidades y desafíos de cada momento.

PILAR LÓPEZ,
directora de Tecnología Académica y E-Learning en el Centro Universitario U-tad

TRANSFORMACIÓN DIGITAL EN TODAS LAS DIMENSIONES DE LA ACTIVIDAD UNIVERSITARIA

José María Ortiz, vicerrector de Organización y Transformación Digital de la Universidad Pontificia Comillas, considera que uno de los pilares para

EMILIANO BLASCO DOÑAMAYOR, vicerrector de Transformación Digital en la Universidad CEU San Pablo

alcanzar ese reto es maximizar la experiencia digital de los estudiantes. A este respecto, ve fundamental analizar su student journey, pero también incorporar nuevas tecnologías disruptivas que permitan transformar en términos de eficiencia los procesos operativos y aumentar significativamente su valor, o integrar la cultura del gobierno del dato como socio necesario e imprescindible para promover una mejora continua que forme parte del ADN de la labor de gestión.

Desde luego, la transformación digital afecta a todos los ámbitos de la actividad universitaria. Joaquín Rodríguez, director de Tecnología para el Aprendizaje de la Institución Educativa SEK, bajo cuyo paraguas está la Universidad Camilo José Cela, se muestra convencido de que todos los departamentos de una organización educativa están implicados directamente en el cambio. Así, señala que la transformación digital trae consigo cambios en los modelos de dirección y gobernanza, en las prácticas de enseñanza y aprendizaje, en las modalidades de comunicación y trabajo colaborativo, en la manera en la que se investiga y publica...

Igualmente, exige nuevas metodologías y formas de docencia que sean capaces de aglutinar entornos y recursos presenciales y online, itinerarios formativos dinámicos, entornos disruptivos de aprendizaje, plataformas adaptativas, nuevas titulaciones que combinen humanística y tecnología y, por supuesto, una experiencia única y completa para el estudiante (y el profesor) en todos sus aspectos vitales, tal y como apunta José Antonio Marcos, CIO y director de la Oficina de Transformación Digital de la Universidad Francisco de Vitoria.

COMPETENCIAS DIGITALES Y REORGANIZACIÓN

En una primera fase, para el CIO de la UFV, la mayor dificultad está en la resistencia de las personas a salir de su zona de confort, lo que comúnmente denominamos "el miedo al cambio". Dado que es un proceso que implica a toda la institución y va más allá de la mera implantación de tecnología, resulta imperativo realizar un diagnóstico inicial del punto de partida y una planificación de la hoja de ruta que va a definir el camino hacia el futuro de la Universidad.

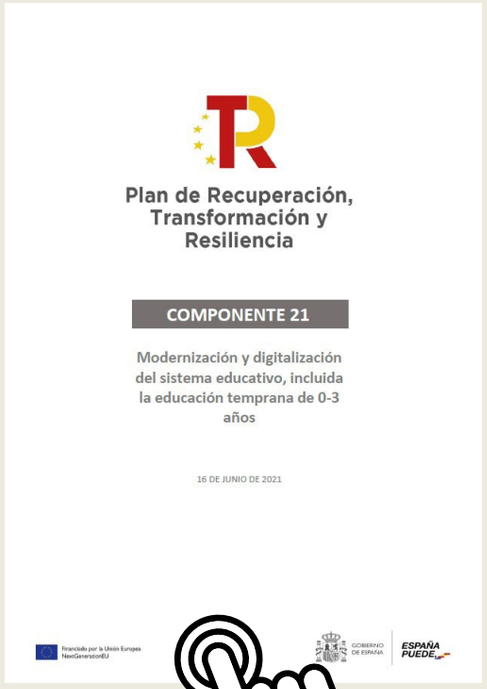
CRISTINA VILLALONGA, directora de Global Campus Nebrija de la Universidad Nebrija

A este aspecto, Joaquín Rodríguez desvela: “nos ha forzado a repensarnos como una organización más horizontal y colaborativa, en base a nodos que cooperan en la resolución de retos y problemas, lo que nos ha obligado, por último, a pensar en el tipo de competencias que queremos promover y cultivar para que todo esto sea posible”. Y es que, en este escenario de disrupción en la enseñanza superior, la capacitación digital de alumnos, profesores y personal es una cuestión que destacan todos los responsables de instituciones privadas entrevistados.

"Contamos con programas de competencia digital docente, para mejorar la enseñanza en los espacios digitales, y acciones específicas para el desarrollo de competencias y habilidades digitales del alumnado. En este sentido, formamos no solo en aquellas skills vinculadas al desarrollo profesional, sino también aquellas que permitan al estudiantado desenvolverse como ciudadanos digitales con libertad, responsabilidad y seguridad", apunta la directiva de la Universidad Nebrija. En cambio, para un centro universitario tecnológico como U-tad, donde la tecnología es intrínseca a su concepción, con un promedio de uso de 3-4 herramientas de software por asignatura, el desafío se ha centrado en que estudiantes y claustro pudieran acceder desde el campus virtual a los recursos necesarios para el desarrollo del proceso educativo de forma simplificada desde cualquier lugar y dispositivo. Y, obviamente, esta actualización de infraestructuras y procesos se ha potenciado en todos los centros

COMPONENTE 21 DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA

El Componente 21 del Plan de Recuperación, Transformación y Resiliencia del Gobierno se dedica íntegramente a la modernización y digitalización del sistema educativo español para orientarlo hacia un modelo de enseñanza personalizado, inclusivo y flexible, contemplando la formación del profesorado en el uso de nuevas técnicas educativas en las escuelas, así como la conectividad de la red universitaria y la adaptación de sus programas y sistemas a las nuevas tecnologías y al aprendizaje híbrido. En su desarrollo, recoge los principales retos y objetivos para modernizar la Educación, entre los que destacan la mejora de los resultados educativos, la modernización del sistema universitario y la recualificación e internacionalización del personal docente e investigador. También persigue estimular la innovación y transformación digital desde la universidad buscando que las propias universidades puedan convertirse en actores centrales en los procesos de transición digital, además de detallar su contribución global a la transición ecológica y digital.



LOS CAMBIOS TECNOLÓGICOS MÁS SIGNIFICATIVOS

El vicerrector de la Universidad de Comillas nos habla de las ventajas de la administración electrónica, materializada de forma muy especial en la digitalización de procesos relevantes dentro de su Secretaría General. "En este departamento, se han fomentado sistemas de autoservicio para la comunidad universitaria, que también han conseguido una reducción de tiempos muy significativa", indica José María Ortiz. Por su parte, José Antonio Marcos, de la UFV, explica que han migra-

JOSÉ MARÍA ORTIZ,
vicerrector de Organización y Transformación Digital de la Universidad Pontificia Comillas

do sus sistemas a estructuras cloud escalables, desplegado redes colaborativas de conocimiento y desarrollo e implantado nuevos sistemas para la prevención y control en ciberseguridad. Asimismo, asegura que se han creado y se están creando nuevos edificios y espacios en el campus con un alto índice de eficiencia energética al que contribuye su domotización, se han digitalizado todas las aulas de la Universidad y grandes salas de reuniones o eventos, o se han diseñado espacios de investigación y descubrimiento compartido, como un learning space en que se despliegan un ágora digital, dos espacios de cocreación , dos espacios de coworking y múltiples cabinas para videoconferencias.

En la CEU San Pablo, la mejora de los servicios universitarios ha logrado reducir la burocracia a la que tenía que responder el claustro, mientras que los mostradores virtuales ahora permiten a los estudiantes realizar gestiones de forma remota. No obstante, según confiesa el vicerrector Emiliano Blasco Doñamayor, uno de los mayores beneficios ha sido el refuerzo de un sentimiento de comunidad y de pertenencia a la institución, lo que "ha demostrado ser el caldo de cultivo para la investigación y creación de nuevas sinergias".

El reconocimiento es otro estímulo para la innovación. De hecho, el Premio Magisterio a los Protagonistas de la Educación 2021 en la categoría de Educación Superior y el Blackboard Catalyst Award en la categoría Leading Change que ha recogido la Universidad Nebrija por su modelo de Presencialidad Híbrida, los conminan a seguir avanzando en la inmersión y personalización del aprendizaje.

TECNOLOGÍAS EMERGENTES EN LA UNIVERSIDAD: PRÓXIMOS PASOS

En el rol de liderazgo que debe asumir la Universidad como promotora de la transformación social en una economía digital, las tecnologías emergentes tienen que ocupar un primer plano en sus procesos de enseñanza-aprendizaje, gestión, investigación y transferencia de conocimiento. Se trata de buscar la excelencia educativa reinventado la educación superior para

JOAQUÍN RODRÍGUEZ,
director de Tecnología para el Aprendizaje de la Institución Educativa SEK

JOSÉ ANTONIO MARCOS,
CIO y director de la Oficina de Transformación Digital de la Universidad Francisco de Vitoria

alcanzar una Universidad innovadora, abierta y conectada. Es por ello por lo que en entidades como la CEU San Pablo ya están desarrollando proyectos en torno a la Inteligencia Artificial, el metaverso o el análisis y gestión de datos. También la Universidad Francisco de Vitoria se apoya en la investigación en tecnologías disruptivas. Así lo ve su CIO, José Antonio Marcos: "la Inteligencia Artificial y el Machine Learning nos permitirán mejorar nuestros procesos de toma de decisiones basados en el tratamiento de datos de múltiples fuentes y aplicaciones de la Universidad en un campus conectado (nuevas titulaciones, plataformas de aprendizaje adaptativo, modernización de la gestión y los servicios, la experiencia en la Universidad, o la gestión del tráfico y reducción de la huella de carbono). La domotización inteligente de los edificios mejorará aún más la eficiencia y sostenibilidad en el campus. La realidad virtual y aumentada combinada con el 5G posibilitarán entornos inmersivos de aprendizaje en formato híbrido que permitirán que cualquier persona pueda estudiar en la Universidad desde cualquier lugar y en cualquier momento. El blockchain y la robotización mejorarán la gestión y administración inteligente de servicios y la posibilidad de plataformas adaptativas de aprendizaje".

OBJETIVOS ALINEADOS CON LA UE Y EL GOBIERNO DE ESPAÑA

Es un viaje en el que por primera vez hay unas ambiciosas directrices comunes nacionales e internacionales. La Brújula Digital europea o el Componente 21 del Plan de Recuperación, Transformación y Resiliencia son algunas de las iniciativas que funcionan como guías.

"En nuestro caso –aclara Joaquín Rodríguez de la Institución SEK– tenemos presente desde el mismo momento de su publicación las recomendaciones de la Unión Europea referentes a las 'Organizaciones educativas digitalmente competentes' y a los distintos marcos competenciales para el profesorado y el alumnado. También participamos con regularidad en los distintos grupos de trabajo de la CRUE, dedicados al análisis

e implementación de muchas de las recomendaciones provenientes del 'European framework for the digital competence of educators' o de otras líneas de trabajo relacionadas con sistemas de acreditación, estándares o big data educativo. En mi opinión, esta vertiente de colaboración estratégica entre instituciones de educación superior será de vital importancia para afrontar la complejidad de los asuntos a los que tendremos que hacer frente los próximos años".

De igual modo, en la Universidad de Comillas están elaborando un plan director de transformación digital alineado con los objetivos de la UE y el Gobierno de España basado en cuatro ejes estratégicos de actuación: la promoción de un ecosistema de educación digital; el impulso de la experiencia global de los usuarios; la mejora de los modelos de gobernanzas y la toma de decisiones basadas en datos; y la promoción de un smart campus, el cual también se vincula con el compromiso por la transición ecológica definido en el PRTR.

En definitiva, reinventar la educación superior pasa por una transformación digital focalizada en la innovación y una intensidad tecnológica que ponga al alumnado en el centro y persiga metas de desarrollo de pensamiento crítico y creatividad, equidad, compromiso medioambiental y cohesión social. ■

ORGANIZACIONES EDUCATIVAS DIGITALMENTE COMPETENTES

Este informe del Centro Común de Investigación (Joint Research Centre, JRC), el servicio científico propio de la Comisión Europea, presenta las líneas clave para que los países de la UE puedan rediseñar sus estrategias organizativas, de modo que mejoren su capacidad de innovación y exploten todo el potencial de las tecnologías y contenidos digitales.

Con la progresiva incorporación de las tecnologías digitales en todos los niveles de la educación, este documento pretende ayudar a consolidar el progreso en este sentido y asegurar su escala y sostenibilidad. Por ello, presenta el Marco Europeo para Organizaciones Digitalmente Competentes (DigCompOrg), con el que se pretende facilitar la transparencia y la comparabilidad entre iniciativas relacionadas emprendidas por toda Europa. Sus principales objetivos son invitar a la autorreflexión y la autoevaluación dentro de las organizaciones educativas a medida que vayan profundizando en su implicación con el aprendizaje y pedagogías digitales, así como permitir a los responsables de la elaboración de las políticas diseñar, implementar y evaluar intervenciones para la integración y uso eficaz de las tecnologías de aprendizaje digital.

MÁS INFORMACIÓN

- 5 tendencias en innovación cloud para 2022
- El mercado de soluciones de inteligencia artificial seguirá creciendo a partir de 2022
- Nuevas tecnologías que revolucionarán el ecosistema digital

Si te ha gustado este artículo, compártelo

EL TRABAJO HÍBRIDO EN ACCIÓN

Muchas empresas están en fase de descubrir un nuevo mundo. Un mundo en el que el trabajo ya no está vinculado a una sola ubicación. En el que pueden capacitar a sus empleados para que se conecten, colaboren y hagan el trabajo de forma segura, sin importar donde estén.
Pero, ¿encontrarán lo que buscan? ¿O se trata de un sueño imposible?

Si se hace bien, el trabajo híbrido puede suponer que todo el mundo salga ganando, así como ofrecer mejores resultados y una mayor flexibilidad y libertad a los empleados. Adaptar tu modelo de trabajo es más fácil de lo que supones, si tienes un socio de confianza que te acompañe en el proceso.

Descarga la novela gráfica y descubre cómo impulsar tu negocio.

Canon

Entornos híbridos: la nueva normalidad en la fuerza laboral

Tras varios años hablando del teletrabajo y de sus ventajas, la realidad surgida de la irrupción de la Covid-19 aceleró una trasformación que ha alterado por completo los entornos laborales que conocíamos. Ahora, dos años después, todo parece indicar que la vuelta atrás es imposible, pero que la huida hacia delante tampoco es una opción, con lo que nos vemos abocados a un planteamiento híbrido que permita concentrar lo mejor de ambos mundos.

No parece que el puesto de trabajo presencial vaya a imponerse en la globalidad de las empresas, pero tampoco lo va a hacer el puesto remoto, con lo que la nueva realidad laboral apunta a unos entornos híbridos que fusionen las ventajas de ambos modelos, pero que también tienen unos retos en cuanto a seguridad, colaboración y productividad, que las empresas no pueden pasar por alto.

Recogía recientemente Harvard Business Review en un artículo titulado 11 tendencias que darán forma al trabajo en 2022 y más allá, los cambios culturales que tendrán que asumir trabajadores y empresas en esta nueva realidad, que, tal y como explican los expertos de la publicación, no serán pocos ni sencillos.

Sin embargo, los avances tecnológicos hacen posible una evolución que va a facilitar una realidad híbrida que permita a la fuerza laboral trabajar allí donde quieran o necesiten hacerlo, sin que ello suponga un menoscabo de la productividad o de la seguridad necesaria para el negocio.

Permitir que los trabajadores cumplan con sus funciones fuera de la oficina es solo un paso en este modelo híbrido. Es necesario un cambio cultural en la empresa que defina una estrategia pensada para la nueva realidad

LA NUEVA REALIDAD

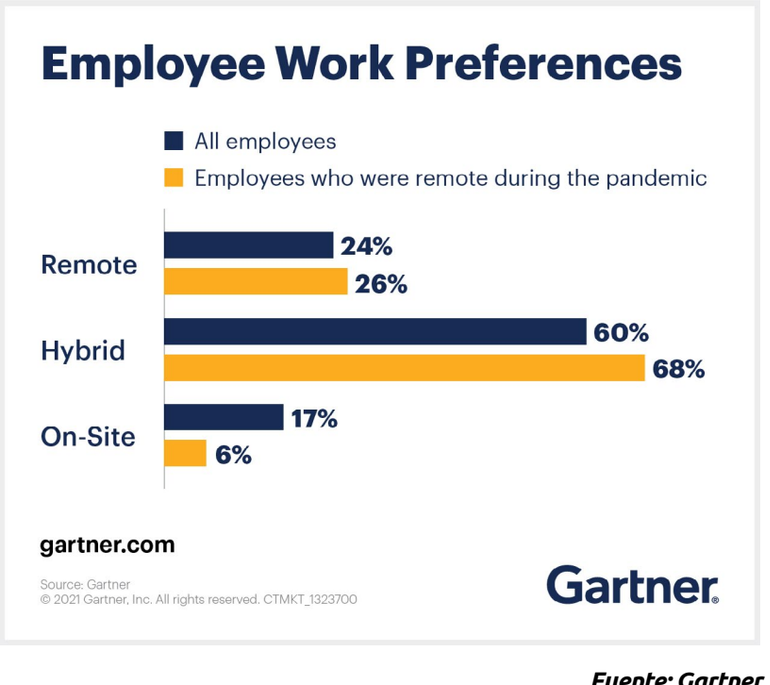
Los empleados se han acostumbrado a trabajar desde casa, y no hay forma de volver atrás. La nueva realidad a partir de este 2022 es el trabajo híbrido, lo que significa apoyar a una fuerza laboral que incluye tanto a usuarios internos como remotos. Los trabajadores exigen estas opciones de trabajo híbridas, y, si no las obtienen, irán a trabajar a una empresa que las proporciona, inmersos como estamos en una guerra por la obtención y la retención del talento.

Crear un entorno de trabajo híbrido no es simplemente una cuestión de dar permiso a los empleados para trabajar desde casa unos días a la semana. Eso es simplemente aplicar una nueva política o dos a un viejo sistema que fue diseñado para empleados internos, con trabajadores remotos como una idea de último recurso. El cambio al trabajo híbrido es una oportunidad para una realineación estratégica del negocio que mantendrá a las empresas competitivas a medida que la relación entre empleadores y empleados continúa redefiniéndose.

DEFINIENDO EL TRABAJO HÍBRIDO

El principal elemento de esta realidad híbrida es la irrelevancia del lugar desde el que el empleado se conecta y trabaja. La empresa debe garantizar que el trabajador puede acceder a los datos y recursos que necesita allí donde los necesita, sin que ello suponga un retroceso en la seguridad o en la productividad imprescindible para el negocio. De hecho, una encuesta publicada por Mercer, realizada a empresas de Estados Unidos, deja claro que el 94% de los encuestados estimaban que la productividad con el trabajo remoto a raíz de la pandemia había crecido o, al menos, se había mantenido. Aunque esta percepción es diferente si hablamos de las empresas, tal y como señala una encuesta de Gartner, que muestra que el 64% de los empleadores consideran que los trabajadores on-site son más productivos.

Asimismo, las compañías deben asegurar la colaboración entre los miembros de la fuerza laboral a través de herramientas específicas y tecnología de comunicaciones que consigan ofrecerles una sensación de "seguir en la oficina" aunque se encuentren a muchos kilómetros de distancia.



Fuente: Gartner

Clica en la imagen para ver la galería completa

Pero, como decíamos, permitir que los trabajadores cumplan con sus funciones fuera de la oficina es solo un paso en este modelo híbrido. Es necesario un cambio cultural en la empresa que defina una estrategia pensada para la nueva realidad. Todos los responsables de la toma de decisiones en la organización deben estar de acuerdo con las mismas políticas y principios generales, desde los directivos de TI hasta los de Re-

cursos Humanos, pasando, por supuesto, por el CEO. Al mismo tiempo, la flexibilidad es esencial para ayudar a retener talento en la empresa. Para ello, las empresas se están volviendo más competitivas no solo en salario y beneficios, sino también en flexibilidad de horarios. Las empresas están descubriendo que la relación empleador/empleado es más que solo hacer el trabajo de hoy. Se trata de mantener una relación a largo plazo donde se eliminan los obstáculos que impiden que cada empleado alcance su máximo potencial. En este sentido, Brian Kropp, jefe de Investigación de RR.HH. de Gartner señalaba que "forzar a los empleados a volver a acuerdos de trabajo no flexibles podría dejar a las organizaciones vulnerables a que el talento sea activamente cazado por los empleadores que ofrecen el tipo de flexibilidad que los empleados han llegado a esperar durante la pandemia. Los empleados han demostrado que pueden ser productivos a distancia y ahora desafían a los empleadores para que les expliquen por qué deberían volver".

UNA NUEVA APROXIMACIÓN A LA SEGURIDAD

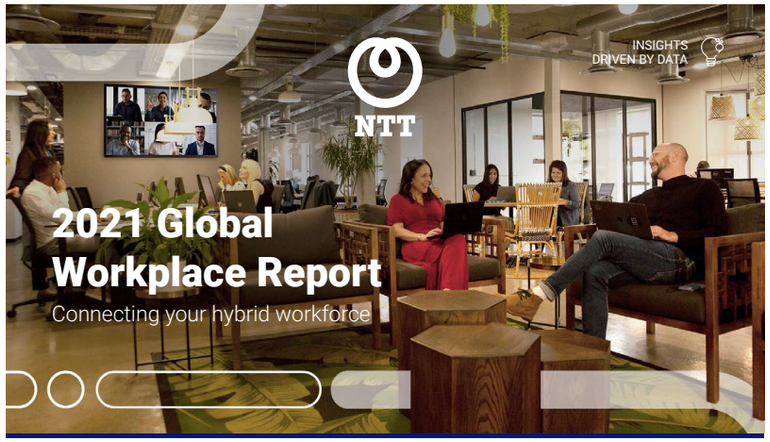
Más allá de esta renovación en la relación con el trabajador, no hace mucho tiempo que la mayoría de la TI corporativa se centraba en un centro de datos en el sitio que controlaba y administraba toda la actividad de los empleados internos. Los trabajadores remotos tenían que conectarse a través de una VPN para atravesar el perímetro de seguridad, pero eso era suficiente porque no había tantos trabajadores remotos.

Obviamente, ese modelo está desactualizado ahora, porque hay muchos más trabajadores remotos. Las conexiones VPN pueden ser temporales, y si la mitad de su fuerza laboral necesita acceso fuera del sitio, simplemente no es viable pedirles a todos que usen VPN. Asimismo, muchas empresas están moviendo la mayoría de sus sistemas de TI a la nube, donde todos tienen el mismo acceso, sin importar dónde se encuentren, lo que provoca que los firewalls que protegían el centro de datos interno de intrusos externos tampoco sean la respuesta, porque la confianza se basaba en la ubicación. A medida que se disuelve la distinción entre el acceso interno y remoto a los recursos de la empresa, también lo hace la necesidad de diferenciar entre el nivel de seguridad necesario para el acceso in situ y fuera del sitio. En los sistemas de TI actuales, todos tienen el mismo nivel de confianza: ninguno.

Cada activo y cuenta comienza con una base de confianza cero (Zero Trust), y tiene que demostrar su valía con cada acceso. Ninguna cuenta, ningún dispositivo, ninguna conexión obtiene ningún tipo de pase de seguridad de forma predeterminada. Esta mentalidad de confianza cero elimina la necesidad de que el personal de TI administre diferentes niveles de seguridad y mantiene los sistemas en general más seguros.

OTRAS TECNOLOGÍAS PARA EL TRABAJO HÍBRIDO

Algunas organizaciones están adoptando un enfoque de digitalización centrado en la nube en apoyo de sus estrategias en el lugar de trabajo. Sin embargo, muchos aún no están maximizando sus inversiones en tecnología. Necesitan una infraestructura de red moderna que admita los cambios en los espacios de trabajo físicos y habilidades internas para garantizar la integración y optimización de las tecnologías existentes.



Fuente: NTT

Clica en la imagen para ver la galería completa

Aquellos que se han digitalizado con éxito están viendo los resultados: en un mejor trabajo en equipo, una mayor agilidad empresarial, mejores experiencias de empleados y clientes, y un rendimiento comercial.

Las redes y los servicios de conectividad deben ser resistentes y seguros, y la calidad de servicio (QoS) a un nivel que permita resultados comerciales para diferentes perfiles de empleados.

Las soluciones basadas en Edge Computing, IA, computación en la nube y análisis de datos generarían información en tiempo real para que las empresas la utilicen a medida que hacen la transición a modelos de trabajo híbridos. Los datos recopilados de los dispositivos y sensores conectados instalados en todo el lugar de trabajo ayudarían a las empresas a optimizar sus recursos y garantizar un entorno de trabajo seguro.

Junto con las herramientas de seguridad ya mencionadas, guardar información en un servidor basado en la nube es un requisito clave para el trabajo híbrido. Al pasar a la nube, las empresas pueden aumentar las capacidades de ancho de banda de Internet, reducir los costes de mantenimiento y conservación de la infraestructura local y disfrutar de la capacidad de escalar hacia arriba o hacia abajo cuando sea necesario.

Y es que a medida que las personas aumentan el trabajo desde una variedad de ubicaciones, los empleados buscan aplicaciones basadas en la nube que guarden datos automáticamente y faciliten el intercambio y el acceso. Por su parte, las empresas ahora pueden usar herramientas móviles para elevar sus experiencias de colaboración.

Por otra parte, la actividad empresarial continúa evolucionando en la mejora de los procesos, y tecnologías como la Automatización o la IA pueden ayudarles en este terreno, mientras conviven con la nueva realidad laboral, porque liberarán recursos asignados hasta ahora a tareas repetitivas y aportarán inteligencia a la toma de decisiones. Esto, junto con nuevas capacidades a la hora de definir las aplicaciones, incluidas tendencias para la creación de estas herramientas con poco (low-code) o sin ningún código (no-code), facilitarán un nuevo nivel de colaboración entre desarrollo y negocio no alcanzado hasta ahora. ■

MÁS INFORMACIÓN

- Fórum Económico Mundial: Tecnología para el futuro trabajo híbrido
- Harvard Business Review: 11 tendencias que darán forma al trabajo en 2022 y más allá
- PwC: El futuro del trabajo
- Cultura empresarial para el trabajo híbrido
- Gartner: riesgos a considerar de la vuelta de los trabajadores a la oficina
- Harvard Business Review: la tecnología define la experiencia del empleado

Si te ha gustado este artículo, compártelo

Cualquier sitio puede ser una oficina si tu quieres que lo sea.

Ofrece a tus empleados la flexibilidad de trabajar desde cualquier lugar y en cualquier dispositivo, incluso mediante los dispositivos personales, con el workspace de Citrix.

citrix™

CARMEN CABANILLAS, Subdirectora General de Gobernanza de los Registros en Dirección General de Gobernanza Pública y presidenta de ASTIC

“La mayoría de los empleados públicos están en disposición de teletrabajar”

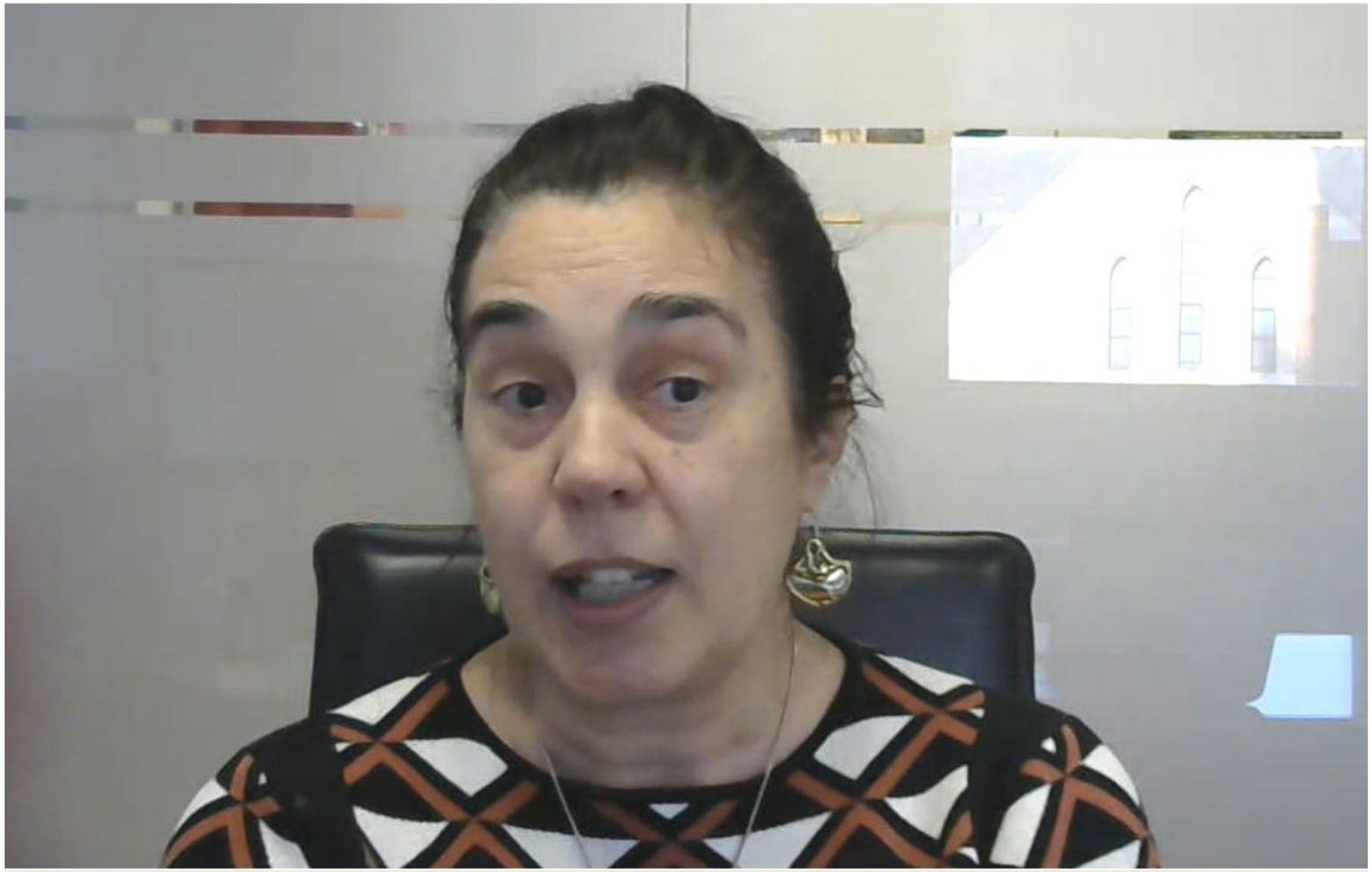
Uno de los ámbitos donde más se notó el salto al teletrabajo fue en la Administración Pública, donde estaba mucho menos implantado que en la empresa privada. Por este motivo, hemos conversado con Carmen Cabanillas, Subdirectora General de Gobernanza de los Registros en Dirección General de Gobernanza Pública y presidenta de ASTIC, para que nos ofreciese su valoración sobre el cambio vivido en estos dos años en este terreno.

ENTREVISTA: Carmen Cabanillas, de ASTIC, nos explica la adaptación de la Administración a la realidad del trabajo remoto. Clica en la imagen para ver el vídeo.

Tal y como nos explicaba Carmen Cabanillas, “antes de la pandemia es cierto que teníamos poca implantación del teletrabajo en las Administraciones Públicas. Algunas entidades específicas sí lo tenían muy regulado, pero en la mayoría no era así. Podíamos encontrar pilotos o grupos muy específicos en los que sí se estaba teletrabajando. Uno de ellos era nuestro colectivo, el personal de Tecnologías de la Información y Comunicaciones, pero realmente hablamos de una corriente escasa. Sin embargo, con la pandemia hemos conseguido avanzar en este sistema de trabajo más flexible y llevarlo al 80-90% de los empleados cuyos puestos lo permiten, porque otros sí requieren una presencia física, como puede ser la atención en oficinas u otros puestos muy específicos”.

“El grueso de los empleados públicos”, continuaba, “están en disposición de teletrabajar. Se ha hecho un esfuerzo muy notable y en poco tiempo hemos cambiado la posición de partida”.

Pero este cambio acelerado ha traído consigo una serie de retos que la Subdirectora General de Gobernanza de los Registros en Dirección General de Gobernanza Pública y presidenta de ASTIC resume diciendo que “hemos tenido que reinventarnos para poder ofrecer los servicios en plena pandemia.



“El grueso de los empleados públicos están en disposición de teletrabajar. Se ha hecho un esfuerzo muy notable y en poco tiempo hemos cambiado la posición de partida”

Esta etapa complicada ha venido acompañada de un incremento de inversión económica, porque no disponíamos del equipamiento preciso, hemos tenido que dotar a los empleados del ancho de banda que necesitaban, proporcionarles licencias de todo tipo, incrementar la seguridad con la introducción de dobles factores de au-

tenticación... También hemos contado con la voluntad de los empleados públicos de adaptarse en un tiempo récord, sin apenas formación, a esta nueva forma de trabajo".

Después de este esfuerzo, recalcaba, "parece que la apuesta no se va a mantener y vamos a volver a una situación de presencialidad, pese a que la UE quiere que la Administración Publica sea un motor que sirva de guía para la sociedad. Por eso, nos gustaría llamar la atención sobre si no sería mas adecuado mantener el esfuerzo e intentar apostar por un trabajo más flexible, porque uno de los problemas a los que nos enfrentamos es la escasez de personal, y las nuevas generaciones lo que más valoran es un puesto de trabajo flexible, no uno para toda la vida. Además, el teletrabajo nos permite alinearnos con otras políticas europeas y nacionales, como la apuesta por el Medio Ambiente o por luchar contra la España Vaciada. Tenemos que ser el motor, el espejo en el que se mire la sociedad".

En este cambio en el modelo de trabajo se han tenido en cuenta diferentes tecnologías, pero otros elementos, como la Experiencia de Usuario, tal y como explica Carmen Cabanillas, "no, por la situación de partida. No fue algo planificado, sino que hubo que adaptarse sobre la marcha. Es cierto que se han ido corrigiendo errores iniciales, sobre todo a nivel técnico, apostando por tecnología que proporcione la propia Administración, porque es más seguro, eficiente y efectivo. Se ha hecho un análisis y se han ido tomando acciones correctoras, pero este proceso no ha terminado, es necesario mejorarlo, y atender una de las grandes carencias, la formación de los empleados públicos, tanto en seguridad como en protección de datos o usabilidad de la tecnología. Todo se hizo tan rápido, que se dieron unas recomendaciones muy sencillas, y es algo que habría que mejorar".

"La Administración debe ser más flexible y aprovechar la disponibilidad de fondos europeos para apostar por estas fórmulas de trabajo que demandan los profesionales"

Por último, quisimos conocer la opinión de ASTIC sobre el Real Decreto que regula el teletrabajo en la Administración Pública. En este sentido, Carmen Cabanillas afirma que la posición de la asociación que ella preside es de apoyo, "sobre todo, en el ámbito técnico, donde tenemos una gran carencia de profesionales. Muchos puestos no se cubren porque no tenemos especialistas, y, en el caso español, esta carencia es grave, porque competimos con empresas de todo el mundo, porque éstas ven claro que se trata de una tendencia muy importante para las nuevas generaciones de trabajadores, y corremos el riesgo de quedarnos atrás y no poder ofrecer los elementos motivadores para captar nuevo talento que necesitamos e, incluso, mantener el que tenemos. Nos preocupa bastante, y pensamos que el proyecto es demasiado rígido, estricto, y creemos que hay cuestiones específicas que deberían adecuarse al caso o al colectivo concreto, porque cuando intentas contemplar todo con una misma norma, puedes dejar fuera elementos importantes. La Administración debe ser más flexible y aprovechar la disponibilidad de fondos europeos para apostar por estas fórmulas de trabajo que demandan los profesionales". ■

ANTONIO SÁENZ SEGOVIA, Director de Operaciones IT de Haya Real Estate

“Tanto la persona como el servicio pueden estar en cualquier lugar, con lo que el planteamiento y la TI que lo soporte tienen que ser completamente diferentes”

El cambio en el puesto de trabajo está suponiendo un impacto importante para las empresas, que deben adaptar su TI y su seguridad para responder a una demanda cada vez mayor de los empleados en lo que a experiencia de uso se refiere. Y para conocer estos retos de primera mano, hemos hablado con Antonio Sáenz Segovia, Director de Operaciones IT de Haya Real Estate.

ENTREVISTA: Antonio Sáenz Segovia, de Haya Real State, nos explica qué retos han tenido que afrontar para adaptarse a un modelo de trabajo híbrido. Clica en la imagen para ver el vídeo.

Haya Real State es una empresa de gestión del crédito y activos inmobiliarios. Según nos explica este responsable, “hace años, cuando hablábamos de infraestructura, lo hacíamos de oficinas

y centros de datos, y ahora lo hacemos de personas y de servicios. La realidad es mucho más fluida ahora, y tanto la persona como el servicio pueden estar en cualquier lugar, con lo que el planteamiento y la TI que lo soporte tienen que ser completamente diferentes. En el caso de las empresas de nueva creación, es necesario diseñar la infraestructura tecnológica pensando en las personas y apoyándose en cloud. Pero si es una empresa que tiene que evolucionar a ese entorno, tiene que hacerlo con tecnologías como SASE o Zero Trust, que nos permitan controlar la situación desde un punto de vista de personas, no de ubicaciones".

El trabajo remoto no es nuevo, aunque se haya visto acelerado, y, en opinión de Sáenz Segovia, "el primer reto ha sido la transformación digital, trabajando para poder afrontar una serie de cambios como tener a toda la plantilla teletrabajando en dos semanas. Teníamos las herramientas, pero las usábamos muy poco porque no era necesario. Para responder, incrementamos las capacidades tecnológicas de las conexiones por VPN, aumentamos la adopción de herramientas colaborativas, preparamos a los usuarios a través de las propias herramientas, adaptamos los procesos a la nueva realidad... Tres o cuatro años antes esto hubiera sido impensable, porque lo cierto es que se habían ido dando pasos previos que nos permitieron una adaptación más sencilla".

"La experiencia de uso es fundamental, porque los nuestros no son usuarios de tecnología, sino de negocio, que usan la tecnología como una herramienta"

Una exigencia de los trabajadores es la experiencia de uso, "y hemos debido tenerlo en cuenta, porque los nuestros no son usuarios de tecnología, sino de negocio, que usan la tecnología como una herramienta. Trabajamos con equipos para tener su respuesta y poder llevar esa experiencia al resto de los usuarios, si bien tuvimos que hacerlo en muy poco tiempo. Además, hay procesos y tecnologías que han aprovechado esta situación como un punto de inflexión en su adopción".

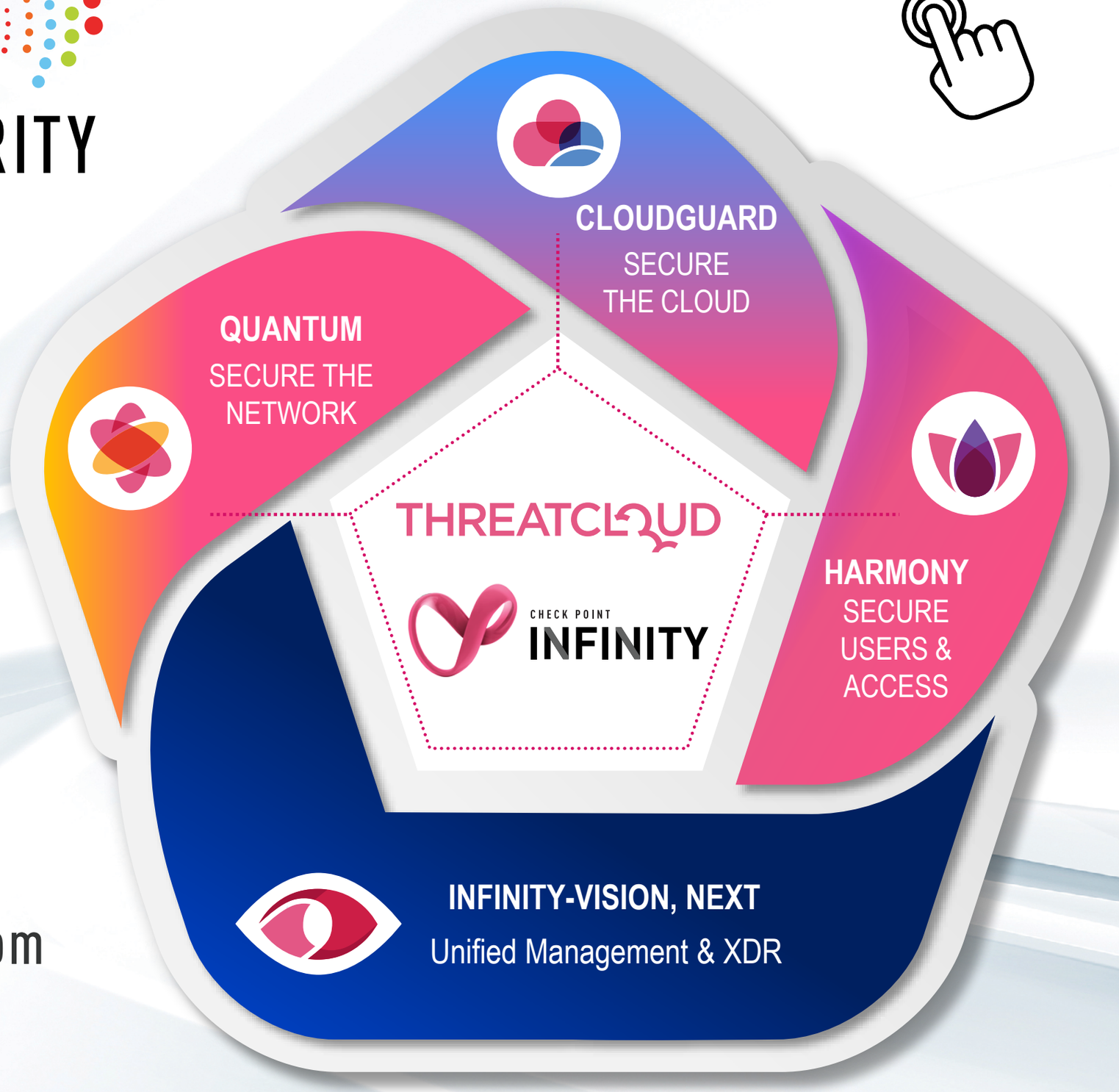
Otro reto a tener en cuenta es el impacto del modelo híbrido en la gestión de TI. Para el Director de Operaciones IT de Haya Real Estate, "hace dos años salimos del paso como pudimos, pero ahora estamos tomando el control de la situación con el foco puesto en la persona. Da igual desde dónde o cómo se conecte, debemos darle la misma experiencia una vez que lo hemos identificado. Hay que ser conscientes de que cuando está en la oficina asumimos que tiene unas medidas de seguridad, pero no así cuando se conecta desde su casa. Hay que tener en cuenta que el entorno se amplía y hay que mitigar los posibles riesgos de trabajar desde ubicaciones diferentes a la oficina".

Para finalizar, quisimos saber qué hemos aprendido de esta situación. Desde la perspectiva de Antonio Sáenz Segovia, "primero, tener un inventario detallado de lo que había. Controlar personas, equipos y necesidades de cada uno de ellos, algo muy complejo en grandes organizaciones. Por supuesto, no olvidar la seguridad, que es imprescindible, aunque el usuario no sea consciente. Por último, el equipo humano, que es el que hace todo esto posible". ■

Si te ha gustado este artículo, compártelo

CHECK POINT™

YOU DESERVE THE BEST SECURITY



MÁS INFORMACIÓN:

www.checkpoint.com/es

info_iberia@checkpoint.com

#ENCUENTROSITTRENDS

Tecnologías habilitadoras de un puesto de trabajo conectado, en movilidad e híbrido

Los entornos laborales han cambiado mucho en los últimos años. Una de las principales razones, pero no la única, ha sido el teletrabajo. La evolución de las tecnologías aplicables en el puesto de trabajo para conseguir un empleado más conectado y con un mejor acceso a la inteligencia de negocio, hacen que la realidad del trabajador sea completamente diferente.

Para hablar de cómo estas tecnologías y tendencias han modificado los entornos laborales, organizamos una mesa redonda dentro del Encuentro IT Trends La transformación del trabajo: el empleado, que reunió a María Jesús Gras, Head of Enterprise Iberia de Logitech; Agustín Sánchez Fonseca, Responsable de Desarrollo de Negocio de NFON Iberia; Manuel de Dios, Field Sales Manager de Citrix; y Eva Sán-

María Jesús Gras, Head of Enterprise Iberia de Logitech; Agustín Sánchez Fonseca, Responsable de Desarrollo de Negocio de NFON Iberia; Manuel de Dios, Field Sales Manager de Citrix; y Eva Sánchez Caballero, Directora de Transformación Digital de Canon España, participaron en este debate moderado por Arancha Asenjo, Directora de IT Trends. Clica en la imagen para ver el vídeo.

“Trabajar en la nube es algo normal ya a estas alturas, pero no debemos olvidar que el puesto de trabajo debe adaptarse a las personas para ofrecer una adecuada experiencia de uso”

EVA SÁNCHEZ CABALLERO, DIRECTORA DE TRANSFORMACIÓN DIGITAL DE CANON ESPAÑA

chez Caballero, Directora de Transformación Digital de Canon España, que, moderados por Arancha Asenjo, Directora de IT Trends, conversaron sobre la nueva realidad del puesto de trabajo.

ELEMENTOS TRANSFORMADORES

En los últimos dos años, la Covid-19 ha provocado una gran transformación en los entornos laborales. Pero no ha sido el único elemento que ha contribuido a ello. A este respecto, Eva Sánchez Caballero apuntaba que “la Covid-19 llegó y aceleró lo que llevábamos años contando que iba a pasar, la transformación digital. Pero la evolución de esta transformación va de personas, y una de las cosas que ha cambiado es la percepción de cómo deben encarar estas personas el nuevo puesto de trabajo. Hay que analizar cómo se están haciendo las cosas, para ver si se pueden simplificar y eliminar procesos. Después, habrá que optimizarlos y automatizarlos. Trabajar en la nube es algo normal ya a estas alturas, pero no debemos olvidar que el puesto de trabajo debe adaptarse a las personas para ofrecer una adecuada experiencia de uso”.

En opinión de Manuel de Dios, “el mayor problema no es la tecnología, sino que el reto está en las personas, y debemos ser capaces de transmitir qué pueden hacer, qué capacidades tienen. Llevamos años trabajando en el puesto remoto, híbrido… y tecnológicamente casi todo está resuelto, pero queda la parte de las personas para que sepan lo que pueden hacer. Evidentemente hay procesos obsoletos que ya no necesitamos hacer, pero es necesaria una labor de concienciación por parte del sector, porque cada día cambia. En estos meses nos hemos felicitado por la capacidad de adaptación de los clientes, porque la imperiosa necesidad del teletrabajo nos ha sorprendido, pero ellos han sido capaces de reaccionar. También hay que concienciar sobre la seguridad, porque un mundo digital abre nuevas puertas al cibercrimen, y la protección de activos digitales es algo que tenemos que asumir rápidamente”.

Todos estos cambios están teniendo gran impacto en la sociedad. Desde la perspectiva de María Jesús Gras, “vivimos un constante cambio, muy

“La complejidad de escenarios es donde está el reto, en cómo lo gestiona la empresa y cómo adopta la tecnología en cada caso”

MANUEL DE DIOS, FIELD SALES MANAGER DE CITRIX

acelerado, y todas las empresas tienen que estar capacitadas para adaptarse continuamente. La pandemia nos ha puesto a prueba y ha demostrado que remotamente podemos ser productivos y eficientes. Ahora estamos en una fase de gran incertidumbre, y tenemos que adaptarnos a la realidad de un trabajo híbrido. Esto va a forzar grandes inversiones, y las empresas deben estar preparadas para asumirlas”.

Concluía Agustín Sánchez Fonseca esta primera ronda destacando que “la evolución de personas y procesos es un tema de cultura, porque hay empresas que no han querido todavía adaptar sus procesos y es necesario que impere una cultura hacia la tecnología, compuesta, por una parte, por los elementos habilitadores para consumir la información que está disponible en la nube, y, por otra, integrar todas las piezas necesarias para permitir que cada perfil dentro de cada empresa cuente con una solución ideal para desarrollar su labor. Lo cierto es que donde no se están haciendo los deberes es en la parte cultural, y debemos explicarles que no toda la tecnología vale y que es necesario cambiar los procesos y apostar por las herramientas adecuadas”.

TECNOLOGÍAS PARA UNA NUEVA REALIDAD

Como decían los diferentes portavoces, el apartado tecnológico de la digitalización del puesto de trabajo ya está solventado. Por este motivo, quisimos saber qué tecnologías son las que respaldan esta nueva realidad de los entornos laborales, con un empleado más conectado y digital. Desde NFON, Agustín Sánchez Fonseca apuntaba que “en la parte de hardware, tecnologías y dispositivos para poder procesar imagen y sonido. A partir de ahí, necesitamos un acceso seguro para el consumo de los diferentes servicios digitales, ya estén en la nube o en un entorno on-premise. De hecho, en esta mesa podemos encontrar las diferentes tecnologías que lo habilitan, más allá del PC. Nosotros estamos en la parte de las comunicaciones unificadas, incluyendo voz, vídeo, compartir información y documentos... Es una necesidad para todo tipo de empresas, independientemente del tamaño y el sector. Y, por encima de todo esto, una cultura que permita decidir cuáles son las herramientas adecuadas que faciliten a cada empleado cumplir con sus objetivos en la empresa”.

“Vivimos un constante cambio, muy acelerado, y todas las empresas tienen que estar capacitadas para adaptarse continuamente”

MARÍA JESÚS GRAS, HEAD OF ENTERPRISE IBERIA DE LOGITECH

Indicaba Manuel de Dios, de Citrix, que “tenemos que empezar a pensar que hay puestos que no son deslocalizables, y la presencialidad del trabajador es básica. Pero sí hay muchos que lo son, y que pueden desarrollarse desde cualquier parte. Yo tengo mi puesto de trabajo donde tenga mis herramientas, que, en mi caso, son mis aplicaciones y mis datos, se consuman como se consuman. Con las diferentes tecnologías estamos permitiendo que cada uno pueda hacerse el traje a medida que necesita. Tecnológicamente ya no hay diferencia entre lo que necesito para trabajar desde la oficina, en mi casa o en un aeropuerto. Hemos humanizado el puesto de trabajo, porque se adapta a nuestra realidad. En definitiva, la tecnología es importante, pero lo más necesario es un cambio de mentalidad”.

Pero para una empresa, continúa Manuel de Dios, “es imposible conocer todas las tecnologías que digitalizan un puesto de trabajo. Es fundamental la capa de integración que convierta estas tecnologías en soluciones concretas, porque la empresa consume un producto o servicio que soluciona una necesidad concreta. La capa intermedia entre tecnología y consumidores es el elemento diferenciador de esta evolución”.

Coincidía con ambos portavoces Eva Sánchez Caballero desde Canon, al señalar que “tenemos que entender la tecnología como un facilitador que ha permitido la evolución. En nuestro caso, hemos querido hablar con las personas que ‘sufren’ los procesos en las empresas, para poder aportar la tecnología que se adapta a esas necesidades y que permite al trabajador abordar sus funciones de una manera digital, apostando por un cambio cultural que permita la evolución, no una imposición”.

En palabras de María Jesús Gras, de Logitech, “según mi experiencia, hasta hace un par de años, las Comunicaciones Unificadas eran, principalmente, tecnologías de audio, porque apenas se usaba el vídeo. Nuestro foco ahora es la videocolaboración. Es importante para las empresas elegir soluciones profesionales, porque no sirve cualquier dispositivo o herramienta. Las empresas deben apostar por tecnologías homologadas y con posibilidad de evolución en el tiempo y con el soporte necesario para que el departamento de TI pueda estar tranquilo porque el equipamiento está actualizado y listo para ser utilizado, ya sea desde casa o desde la oficina. Además, la empresa deberá adaptar sus salas para que estén preparadas para la labor que van a desempeñar. Ha

“No se trata de obligar a los usuarios y las empresas a usar una tecnología concreta, sino de lo contrario, de usar las piezas necesarias a la hora de definir la solución más eficiente”

AGUSTÍN SÁNCHEZ FONSECA, RESPONSABLE DE DESARROLLO DE NEGOCIO DE NFON IBERIA

llegado el momento de replantearse la tecnología y apostar por la más adecuada”.

LO QUE ESTÁ POR VENIR

Más allá de lo que es una realidad hoy en día, ¿cómo se prevé que evolucione la tecnología alrededor del puesto de trabajo? En opinión de María Jesús Gras, “cada empresa tiene que definir la plataforma por la que se va a decantar y cada empleado, en función de su trabajo, la modalidad por la que va a optar. Para ese trabajo híbrido, es necesario que esté disponible la tecnología en función de las necesidades de cada uno, abriendo la puerta, a nivel empresarial, a nuevo talento más allá del que podría atraer físicamente a las empresas, y, a nivel personal, un mayor grado de conciliación, una reducción de los desplazamientos, mayor eficiencia...”. “Desde el punto de vista tecnológico”, explicaba Manuel de Dios, “vemos una continuidad sobre lo que hemos venido haciendo. La evolución no se puede evitar, y el siguiente paso es de transformación de las personas más que de la tecnología. La complejidad de escenarios es donde está el reto, en cómo lo gestiona la empresa y cómo adopta la tecnología en cada caso. Ahí es donde estará el reto en los próximos años, porque las mayores sorpresas a los proveedores nos las dan los clientes y cómo han sido capaces de adaptar la tecnología a sus necesidades específicas”.

Para Eva Sánchez Caballero, “es difícil saber cuándo empezó la transformación, porque lo que ha habido es una evolución. Vemos que hay tendencias que están empezando a coger velocidad de crucero a la hora de evaluar procesos, y la tecnología ahí es un facilitador”.

“La evolución tecnológica la vemos más como una democratización”, comentaba Agustín Sánchez Fonseca, que añadía que “estas herramientas van a evolucionar a partir de la flexibilidad y la sencillez de uso. En la medida en que la tecnología sea flexible y conveniente, tendremos que definir la arquitectura en cada caso en busca de la mayor eficiencia. No se trata de obligar a los usuarios y las empresas a usar una tecnología concreta, sino de lo contrario, de usar las piezas necesarias a la hora de definir la solución más eficiente”. ■

MÁS INFORMACIÓN

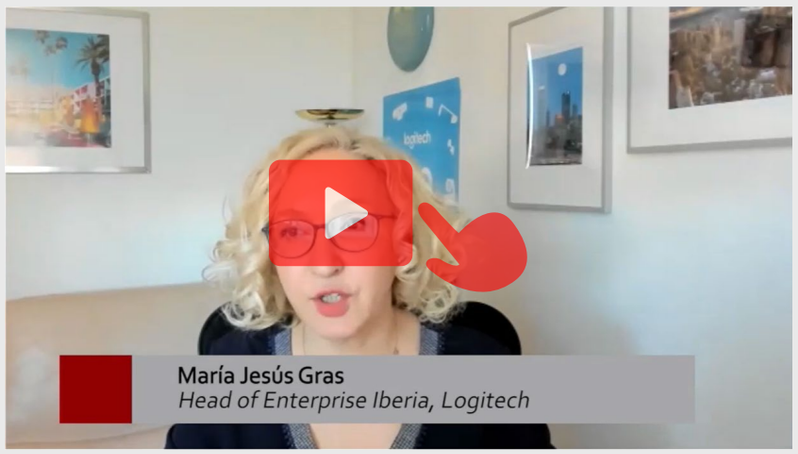
- El trabajo híbrido en acción
- Videoconferencias en el lugar de trabajo moderno
- Reconstruir el comercio minorista con una base digital

Si te ha gustado este artículo, compártelo

Tecnologías habilitadoras de un puesto de trabajo conectado, en movilidad e híbrido

“La Transformación Digital va de personas, y debemos lograr una experiencia positiva para ellas”, Eva Sánchez Caballero, Directora de Transformación Digital de Canon España

“El usuario y el puesto de trabajo siempre han sido nuestros focos de atención”, Manuel de Dios, Field Sales Manager de Citrix



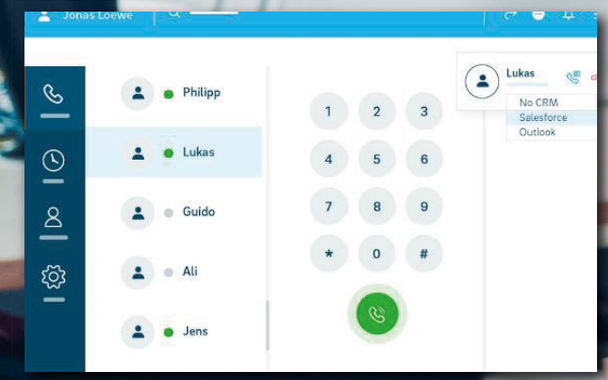
“Podemos ser igual de productivos sin necesidad de ir a la oficina”, María Jesús Gras, Head of Enterprise Iberia de Logitech

“Ofrecemos a las empresas lo que necesitan los diferentes perfiles de trabajadores”, Agustín Sánchez Fonseca, Responsable de Desarrollo de Negocio de NFON

cloudya

Digitaliza las comunicaciones de tu empresa.

NFON
Cloud Telephone System



Más info **nfon.com**

partners.iberia@nfon.com

nfon.com

910 616 600

#ENCUENTROSITTRENDS

Nuevas medidas de protección para un puesto de trabajo híbrido

La evolución del puesto de trabajo digital trae consigo una inevitable transformación de la seguridad, que debe enfrentarse a nuevos retos al tener que proteger una fuerza laboral que ya no se concentra en un único punto cuyos límites están asegurados, sino que puede conectarse desde cualquier ubicación, con diferentes dispositivos y en distintos momentos.

Eusebio Nieva, Director Técnico de Check Point; Miguel Carrero, VP Security Service Providers & Strategic Accounts de WatchGuard; Sergio Martínez, Country Manager de SonicWall; y David Sánchez, Director comercial de ESET, participaron en este debate que fue moderado por Arancha Asenjo, Directora de IT Trends. Clica en la imagen para ver el vídeo.

Precisamente de las necesidades de seguridad y de los nuevos retos a los que se enfrentan las empresas alrededor del puesto de trabajo remoto o híbrido es de lo que hablamos en esta mesa redonda del Encuentro IT Trends La transformación del trabajo: el empleado, que reunió a Eusebio Nieva, Director Técnico de Check Point; Miguel Carrero, VP

“Para luchar contra las amenazas necesitas un conjunto de herramientas que, aunque se solapen, nos permitan componer una seguridad más adecuada”

EUSEBIO NIEVA, DIRECTOR TÉCNICO DE CHECK POINT

Security Service Providers & Strategic Accounts de WatchGuard; Sergio Martínez, Country Manager de SonicWall; y David Sánchez, Director Comercial de ESET, moderados por Arancha Asenjo, Directora de IT Trends.

TRANSFORMACIÓN DE LA SEGURIDAD

Los procesos de transformación llevan consigo también una evolución en la aproximación a la seguridad. En este sentido, Miguel Carrero, VP Security Service Providers & Strategic Accounts de WatchGuard, apuntaba que todo empieza por asumir “el nuevo entorno, eliminar el calificativo de temporal y asimilar que el trabajo híbrido está aquí para quedarse. Y esto implica que vamos a trabajar desde distintos puntos físicos, lo que supone diferencias entre los entornos de telecomunicaciones y conexión en cada caso, si bien también hay elementos comunes, como puede ser el end-point, un mismo dispositivo conectado de maneras diferentes. El perímetro no desaparece, pero sí cambia y se difumina. Asimismo, hay que entender que ha habido una aceleración muy importante de las empresas hacia entornos cloud, que también tiene muchas implicaciones en la seguridad, de ahí que haya que aplicar un nuevo modelo que, en nuestro caso, da relevancia al end-point en el concepto de la identidad, algo que hay que verificar independientemente de dónde, cómo o a qué te estés conectando. Sin olvidar los elementos de una red que cambia el perímetro de las comunicaciones. Manejar todo esto desde un punto unificado y central no es sencillo, pero creemos que es donde está la clave del modelo de seguridad para un entorno híbrido”.

Coincidía con él Sergio Martínez, Country Manager de SonicWall, cuando afirmaba que, “efectivamente, el perímetro no desaparece, sino que hay múltiples perímetros. Según el Informe de Ciberamenazas 2022 que hemos presentado, se mantiene el incremento del ransomware, que se ha más que doblado en los últimos meses. Pero vemos otra tendencia también muy interesante, el uso de la encriptación por parte de las amenazas. Nos

“Hemos de centrarnos en el usuario, que es el elemento más importante, y que debe entender que la seguridad es fundamental”

DAVID SÁNCHEZ, DIRECTOR COMERCIAL DE ESET

aproximamos al 80% de tráfico encriptado, y, si los firewalls no son capaces de ver dentro de este tráfico encriptado, no pueden analizar si hay amenazas. Eso se ha agravado durante la pandemia por el despliegue de estrategias BYOD en muchas empresas, y la movilidad, y esto traslada la respuestas de la seguridad, cada vez más, al end-point. Por tanto, es muy importante su gestión. La defensa por capas toma todavía más protagonismo en el entorno en el que nos encontramos”.

“La tendencia”, añadía Eusebio Nieva, Director Técnico de Check Point, “es centralizar la defensa más importante en el end-point, porque es uno de los elementos sujetos a más cambios, porque se ha convertido en el perímetro. Por eso, hemos de tener en cuenta la adopción de arquitecturas globales para poner puntos de control allí donde sean necesarios. Si tomamos como ejemplo las últimas tendencias de Zero Trust, donde no te puedes fiar de nadie y todo debe ser comprobado antes de dar el acceso, el end-point es una parte importante, pero también hay que securizar el punto desde el que se conectan, el acceso en sí mismo, o el punto de entrada al servicio al cual el usuario tiene derecho. La pieza central de todo es la gestión de la identidad, porque, si no sabes quién se conecta, Zero Trust pierde su sentido. Tenemos que ser capaces de comprobar la identidad en todo el ciclo y poner esos puestos de control en todos y cada uno de los puntos implicados. Así, minimizamos el impacto de los ataques, que en más de 50% de los casos, provienen de un robo de credenciales”.

Concluía David Sánchez, Director Comercial de ESET, esta primera ronda de opiniones indicando que no solo hay que proteger el end-point, “sino también todos los elementos conectados a nuestra red. El número de dispositivos conectados aumenta y, con ello, la superficie de ataque. Si hablamos de la gestión de sistemas o plataformas, necesitamos contar con una solución de monitorización que pueda centralizar datos y alertas. Hemos detectado que el uso del cifrado y de la doble encriptación han sido importantes en los últimos meses”.

DIFERENTES ESLABONES DE UNA MISMA CADENA

Como veíamos, la seguridad no es algo que afecte a un único elemento o punto de la infraestructura, sino que todos los importantes. Recordaba desde WatchGuard Miguel Carrero que “ha cambiado también la forma en que trabaja el profesional de la seguridad. Vemos una apuesta por la externalización de las labores de seguridad y, en muchos casos, el profesional de la protección no está integrado con el resto de los elementos, pero la eficiencia de las tecnologías de securización en las operaciones de seguridad es absolutamente crítico. Son muchos los elementos que hay que tener en cuenta, pero necesitamos que estén integrados en una plataforma con capacidades de automatización que incrementen la eficiencia”.

Múltiples elementos, diferentes amenazas y distintos vectores de ataque. La realidad de la seguridad ha cambiado, y hay que cambiar con ella.

“Tenemos un entorno con potenciales riesgos catastróficos y no es sencillo que los usuarios lo entiendan, pero hay que insistir en ello, porque este es el punto débil donde tenemos que centrar nuestro foco”

SERGIO MARTÍNEZ, COUNTRY MANAGER DE SONICWALL

Para SonicWall, en palabras de Sergio Martínez, “hay que dejar de ver la ciberseguridad como una mera colección de dispositivos y verlo de otra forma. Por eso es importante una defensa por capas, empezando en el nuevo perímetro, porque nunca ha habido tantas amenazas y de corte tan desconocido. Conviene, asimismo, compartimentar con estrategias de Confianza Cero, pero eso también requiere un elemento central para poder analizar la información y detectar amenazas, aunque estas provengan de tráfico encriptado. De ahí que el uso de SandBox también sea una estrategia adecuada, como lo es el punto de acceso seguro. Por último, hay que cerrar el círculo y que el coste sea adecuado para que las empresas puedan defenderse de manera eficiente”.

En opinión de David Sánchez, de ESET, “más que ver lo que falta, conviene ver cómo se está aplicando el plan de seguridad. Según los datos de nuestros análisis, el número de ataques a usuarios remotos en los últimos cuatro meses en España fue de 51.000 millones, duplicando a Italia, que ocupa la segunda posición. Por eso es fundamental que estos entornos híbrido estén convenientemente protegidos. Además, no podemos olvidar que nuestro tejido productivo está formado por pequeñas empresas, y que tampoco se está definiendo, desde un punto de vista legal, de manera suficiente en puesto de trabajo híbrido o remoto. En definitiva, creo que nos falta mucho camino por recorrer.

SONICWALL: INFORME DE CIBERAMENAZAS 2022

“Tenemos que ser capaces de transmitir”, comentaba Eusebio Nieva desde Check Point, “que la seguridad es el habilitador de hacer negocios en internet. No hay otro camino. El número de amenazas es tan grande que necesitas seguridad sí o sí. Tiene que ser algo que esté planificado desde el primer momento, desde la puesta en marcha de cualquiera de los servicios. Por desgracia, con la pandemia, algunos de estos servicios, sobre todo los de teletrabajo o trabajo remoto, no

“Es fundamental que la seguridad no vaya contra la experiencia de uso, porque el usuario tiene que aceptarla y participar en ella”

MIGUEL CARRERO, VP SECURITY SERVICE PROVIDERS & STRATEGIC ACCOUNTS DE WATCHGUARD

han sido planificados con la seguridad adecuada, pero ahora sí podemos y es el momento de hacerlo. Sin embargo, seguimos viendo que se planifica el acceso remoto y la seguridad se añade a posteriori, y esto es un error. Además, hemos de tener una visión global, y tener claro cómo queremos consumir los servicios de seguridad, porque no todos tenemos que ofrecerlos internamente, y algunos pueden ser consumidos por servicios ofrecidos por terceros. Si no tomamos las medidas adecuadas, estamos abocados al fracaso. No basta con proporcionar al usuario un antivirus, sino que hay que contar con otros servicios añadidos, como, por ejemplo, la seguridad de la navegación, porque ahora no están protegidos por el perímetro de la empresa, como ocurría antes”.

Apuntaba Miguel Carrero que “hay muchos elementos de ciberseguridad, pero quizá la complejidad es el mayor enemigo. Si tenemos las herramientas para son complejas o no se pueden implementar, tenemos un problema, y, por eso, hablamos de una plataforma unificada de seguridad, que incorpore estas capas necesarias paro entrelazadas de forma eficiente y sencilla. Hay que mantener las características adecuadas en cada una de las dimensiones, que no es algo trivial, pero sin incrementar la complejidad”.

Otro elemento fundamental, añadía, “es la proactividad. A la velocidad de surgen las amenazas, no podemos limitarnos a reaccionar. Hay que ser proactivos. Anticiparse al ataque a partir del conocimiento obtenido por lo que ya ha ocurrido, es esencial para asegurar el éxito”.

UN ELEMENTO EN CONSTANTE EVOLUCIÓN

Hemos visto que las amenazas y, por ende, la seguridad, son cambiantes. Pero ¿hacia dónde nos dirigimos? Comentaba Eusebio Nieva que “cada vez más, el cifrado es más importante, pero incluso para el malware. Del mismo modo vemos que hay veces que este malware se aloja en un espacio considerado seguro, como puede ser una tienda de aplicaciones. El problema es que algunas de las tecnologías que eran la solución frente a amenazas, hay que complementarlas con otras que nos ayuden a dar una respuesta más eficiente. Para luchar contra las amenazas necesitas un conjunto de herramientas que, aunque se solapen, nos permitan componer una seguridad más adecuada. Necesitamos una defensa para múltiples amenazas,

lo suficientemente flexible para adaptarte a las nuevas que puedan ir surgiendo. La complejidad es enemiga de la seguridad, pero esta es enemiga de lo fácil. Y no podemos olvidar la concienciación del usuario, porque es fundamental para atajar las nuevas amenazas".

Añadía Sergio Martínez el riesgo que supone "la enorme ampliación de la superficie de exposición, con un aluvión de dispositivos smart que no cuentan con la seguridad necesaria. Es necesaria una respuesta global frente al cibercrimen. Tenemos un entorno con potenciales riesgos catastróficos y no es sencillo que la gente, los usuarios, lo entiendan, pero hay que insistir en ello, porque el punto débil es el usuario, y es donde tenemos que centrar nuestro foco".

En esa línea, es fundamental que la seguridad no vaya, tal y como indicaba Miguel Carrero, "contra la experiencia de uso, porque el usuario tiene que aceptar y participar en la seguridad. Cada vez contamos con más tecnologías que permiten, de una forma amigable y sencilla, introducir elementos de identificación que son absolutamente críticos. Al usuario hay que concienciarlo y hacerle partícipe, sin que la seguridad afecte a su trabajo de forma negativa".

Destacaba David Sánchez que los delincuentes también "seguirán evolucionando, y tenemos que estar preparados para ello. Hemos de centrarnos en el usuario, que es el elemento más importante, y que debe entender que la seguridad es fundamental. Por otra parte, vemos muchos casos en los que cuando alguien recibe un ataque no se notifica, y esto es un problema que también hay que afrontar".

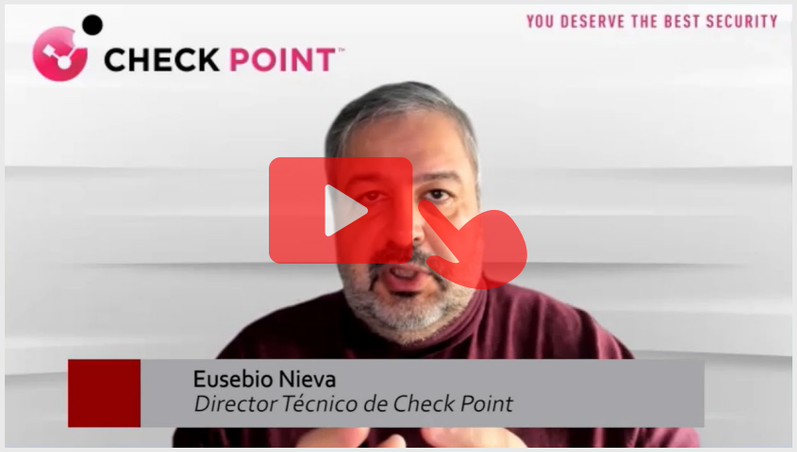
Finalizaba aportando Sergio Martínez otro elemento al debate: la privacidad contra la ciberseguridad, "que va a tener más relevancia próximamente. Hay una realidad que también afecta a las infraestructuras, como el cifrado de los DNS. Es algo que está encima de la mesa y que será un tema recurrente en el futuro". ■

MÁS INFORMACIÓN

Check Point Maestro y la necesidad de seguridad para las redes hiperescalares

Si te ha gustado este artículo, compártelo

Tecnologías habilitadoras de un puesto de trabajo conectado, en movilidad e híbrido



“Muchas empresas se plantean SASE o ZTNA como servicio para evitar complejidades”, Eusebio Nieva, Director Técnico de Check Point

“El puesto de trabajo hibrido cambia el escenario para el empleado y para el personal de TI”, Miguel Carrero, VP Security Service Providers & Strategic Accounts de WatchGuard

“El tráfico encriptado es una autopista para el cibercrimen”, Sergio Martínez, Country Manager de SonicWall

“ESET pone el foco en el usuario y en la usabilidad y eficacia de las soluciones”, David Sánchez, Director Comercial de ESET

WatchGuard Endpoint Security Solutions

Proteja sus dispositivos con confianza

Las soluciones nativas en la nube de WatchGuard Endpoint Security protegen a las empresas de cualquier tipo de ciberataques presentes y futuros mediante las soluciones Endpoint Protection Platform (EPP) y Endpoint Detection and Response (EDR). Nuestra plataforma WatchGuard Endpoint Security ofrece una protección completa de EPP y EDR, así como servicios de búsqueda de amenazas y aplicaciones de confianza cero, suministrados a través de un único agente ligero y gestionados desde una única plataforma basada en la nube.

WATCHGUARD EPP

Endpoint Protection Platform

WATCHGUARD EDR

Endpoint Detection and Response

WATCHGUARD EPDR

Endpoint Protection Detection and Response

Threat Hunting Service

Zero-Trust Application Service

+34 917 932 531

spain@watchguard.com

www.watchguard.com

itTRENDS

OPINIÓN

Las tecnologías emergentes abren un nuevo paradigma para el sector de la construcción

Sergio Hernández Moreno,
presidente de Smartech Cluster y regional manager Smart Infrastructures de Cataluña en SIEMENS

En la actualidad no podemos imaginar un mundo sin datos. Un mundo donde no exista el teléfono móvil, esa herramienta que casi parece una extensión más de nuestro cuerpo y con la que, sin ser del todo conscientes, llevamos a cabo un gran número de interacciones al día y compartimos gran cantidad de datos.

La tecnología se ha introducido en nuestras vidas de una forma cotidiana provocando que las hasta hace poco grandes desconocidas, como el IoT y la IA, formen parte de nuestro día a día sin necesidad de tener profundos conocimientos sobre las mismas.

En una descripción muy llana, estas tecnologías emergentes consiguen que los objetos hablen, es decir, transmitan datos. Solo tenemos que fijarnos en todas las transacciones digitales que hacemos habitualmente y que pertenecen al mundo del Internet de las Cosas (IoT). El hecho de que los datos vayan creciendo de un modo exponencial también implica que su tratamiento, para un uso adecuado de los mismos, deba tener un crecimiento exponencial. Es aquí donde tecnologías de IA (Inteligencia Artificial) toman un importante protagonismo gracias a los algoritmos extraen el jugo de toda esa maraña de datos, que sin estos mecanismos sería indescifrable.

Pero ¿qué pasaría si la tecnología que nos parece tan tangible y de uso diario se alinease dando lugar a grandes conjuntos de datos que interaccionan entre sí? Sin duda, llevaría a otra escala la tecnología y su usabilidad. Pues bien, hoy las nuevas tecnologías brindan la posibilidad de llevar el negocio de la construcción a un siguiente nivel. Sí, esto no es futurible, sino que la tecnología lleva años preparada para ello y, junto al usuario cada día más digital, cambiará el paradigma de la construcción, con una edificación previsible, a medida y personalizada en función de cada usuario.

La Brújula Digital para la Década Digital de la UE nos propone cuatro pilares: capacidades; infraestructuras digitales, seguras y sostenibles; transformación digital de las empresas; y digitalización de los servicios públicos. Estos cuatro focos alineados harán posible dar un paso adelante y transformar un sector tan pasivo como la construcción. No hablo de nada que parezca ciencia ficción, de hecho, en la industria se lleva tiempo utilizando la tecnología para mejorar los procesos de producción o diseño de una fábrica, permitiendo la mejora de la competitividad de las empresas.

Por tanto, ahora es el momento de que el sector de la construcción de ese salto, un salto que debe implicar a toda la cadena de valor. Estoy hablando de aspectos tales como la simulación de los efectos del crecimiento de la población, el incremento del consumo de recursos energéticos o la concentración en los núcleos urbanos. Todos ellos grandes retos que apuntan al año 2050. En poco más de 25 años, esta será nuestra realidad y, para poder hacer frente a la misma, la digitalización será una de las claves.

Entretanto, es factible simularla y gestionarla mediante modelos digitales de los edificios y las ciudades que nos permiten adelantarnos al efecto y generar soluciones ante todos estos retos. Como muestra, tenemos los primeros ejemplos de proyectos de innovación sobre Gemelo Digital en edificios con resultados muy prometedores. A través de ellos vemos claramente cómo la simulación permite, en lugares ya construidos, tomar decisiones de mejor continua para el consumo energético y la sostenibilidad de los emplazamientos con totales garantías.

Si bien la tecnología es una realidad, ¿por qué no se aplica hoy en día en todos los edificios? Para poder contestar a esta pregunta, debo volver a los cuatro pilares de la Brújula Digital. Necesitamos personal con mayor capacitación y ello no conlleva necesariamente nuevo personal, sino más bien al contrario, personal con

La tecnología lleva años preparada y, junto al usuario cada día más digital, cambiará el paradigma de la edificación

la actitud necesaria para mejorar su capacitación. A diferencia de antaño, son habilidades que se pueden adquirir en un tiempo muy reducido y ser un gran contribuyente a la implementación de estos sistemas.

Sin duda, la capacitación es un gran habilitador que facilita la transformación digital de las empresas. Sin embargo, es una cuestión que hasta el momento pasa desapercibida para una gran mayoría de pymes, lo que impedirá que sigan el ritmo de otras que sí se suban al carro y que consigan mejorar su competitividad de manera notable.

Como podemos ver, todo tiene una gran relación entre sí. Sin capacitación del personal no obtendremos la transformación digital necesaria que dé lugar a esas infraestructuras digitales deseadas y que la tecnología actual nos permitiría disponer.

No queremos perder de vista el cuarto foco de la Brújula, la digitalización de la infraestructura pública es primordial. El ejemplo que nos dan las empresas públicas facilita la implicación del resto de actores. Es más, ya hay normativa para digitalizar los edificios públicos, pero para ir un paso más allá debemos focalizarnos en los servicios públicos, es decir, mirar fuera de los edificios y poder digitalizar todo servicio externo.

Pensando en una matriz que nos dé la oportunidad de dimensionar las infraestructuras, los servicios, la movilidad e incluso la energía con términos como el “Grid Edge” alcanzaremos un paradigma digital completo de nuestro entorno. Solo cuando consigamos obtener la digitalización de todos estos procesos con tecnologías como las ya comentadas, que propicien tener una semántica global de entendimiento entre los diferentes sistemas, podremos hablar del concepto de Conectividad Global, Smart City, Country o World. Se trata de entornos donde todos los elementos se puedan comunicar entre sí y, de ese modo, conseguir superar cualquier desafío que se nos pueda plantear en el futuro.

En resumen, me gustaría concluir otorgando a la tecnología un efecto de facilitador para conseguir la mejora de la sociedad en general. Sin tecnología y su correcta aplicación no podremos hacer frente a los grandes retos que tenemos actualmente encima de la mesa, tampoco a los futuros que seguramente se nos planteen en los próximos años o décadas. ■

Si te ha gustado este artículo, compártelo

SOLUCIONES DE **VIDEOCOLABORACIÓN**

Las soluciones avanzadas de videocolaboración de Logitech permiten a los equipos mantenerse en contacto, trabajen desde donde trabajen.

aruba
a Hewlett Packard
Enterprise company

LLEVE LA SEGURIDAD AL EDGE

Proteja su entorno de trabajo híbrido

La ciberguerra se hace realidad

La ciberguerra que desde hace años se viene vaticinando ha llegado. La guerra desatada en Ucrania también se lucha en las redes y está por ver qué impacto tiene en el mundo real. La ciberinteligencia cobra hoy todo su sentido; saber lo que ocurre en el internet más profundo permitirá hacer frente a lo que ciberdelincuentes de todo el mundo están dispuestos a hacer a favor de uno y otro bando.

Hace semanas que los ciberataques contra Ucrania se suceden. Los objetivos no son sólo el sistemas bancario, los organismos públicos o los periódicos y empresas privadas del país, sino los propios ciudadanos, a quienes se engaña con mensajes falsos.

La avalancha de ataques ha llevado a un conflicto digital más amplio. Los gobiernos occidentales se preparan mientras advierten a las empresas que estén alerta a las actividades sospechosas de Rusia, a quien se acusa desde hace años de realizar ciberataques y campañas de desinformación en un esfuerzo por impactar en las economías occidentales y socavar la democracia.

Los ataques contra la infraestructura crítica de Ucrania comenzaron antes de la invasión militar. A mediados de enero el gobierno ucraniano informó de un ataque contra los sitios web del Ministerio de Relaciones Exteriores, el gabinete de ministros y los consejos de defensa del país. Un mes después, los funcionarios de ciberseguridad de Ucrania también anunciaron un ataque DDoS, o denegación de servicios distribuido, contra dos de los bancos más grandes del país, PrivatBank y Oschadbank. Y fue sólo el comienzo.

El intento de ataque a través de una nueva variedad de malware denominada HermeticWiper que impedía que las computadoras se reiniciaran, dejó solo varios cientos de máquinas afectadas y su

Cybersecurity Ventures espera que los costos globales del cibercrimen crezcan un 15 % por año durante los próximos cinco años, alcanzando los $10,5 billones de dólares anuales para 2025, frente a los $3 billones de dólares de 2015. Esto representa la mayor transferencia de riqueza económica en la historia, pone en riesgo los incentivos para innovación e inversión, es exponencialmente mayor que el daño infligido por los desastres naturales en un año, y será más rentable que el comercio global de todas las principales drogas ilegales combinadas.

alcance geográfico más allá de Ucrania se limitó a Letonia y Lituania.

Ha habido escaramuzas cibernéticas en otras partes del conflicto. El gobierno ruso impuso restricciones parciales a Facebook después de que los funcionarios acusaran a la red social de censurar los medios respaldados por el estado en la plataforma, lo que llevó a Facebook a prohibir los anuncios de los medios estatales rusos. La plataforma YouTube de Google también prohibió los anuncios en los medios estatales. Otro titán

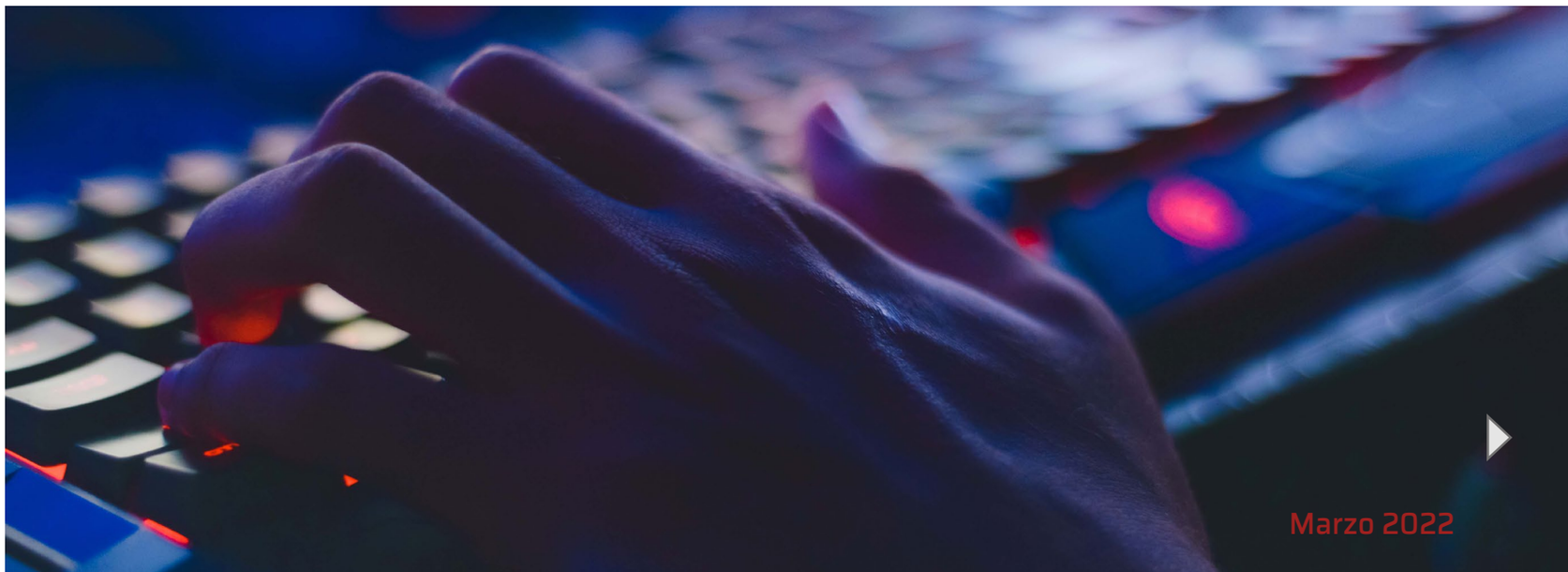
NotPetya, dirigido inicialmente contra instituciones gubernamentales, financieras y energéticas de Ucrania, terminó causando daños colaterales a empresas globales

RUSIA PERFECCIONA SU CIBERGUERRA EN UCRANIA **CLICAR PARA VER EL VÍDEO**

tecnológico estadounidense, Elon Musk, está brindando acceso a Internet satelital a Ucrania a través de sus satélites Starlink, mientras que el gobierno ucraniano está buscando abiertamente donaciones internacionales en criptomoneda y, según se informa, ha recibido millones de dólares en respuesta.

Rusia, tanto oficialmente como a través de ciberdelincuentes que cumplen sus órdenes, tiene una larga historia de uso de armas cibernéticas contra los que consideran sus enemigos, incluido Estados Unidos. El ejemplo más reciente es el ataque de SolarWinds, descubierto por primera vez a fines de 2020, y una serie de ataques de ransomware de alto perfil, incluido el ataque del año pasado en el oleoducto Colonial Pipeline. El primero, que condujo a la infiltración de varias agencias gubernamentales estadounidenses junto con un centenar de empresas, se atribuyó al servicio de inteligencia de Rusia. Este último, que desconectó un oleoducto que transporta la mitad de la gasolina de la costa este durante varios días, se atribuyó a organizaciones criminales con sede en Rusia, que probablemente operaban

Junto con Anonymous, otro grupo hacktivista que apunta a Rusia es AgainstTheWest



Conti, un grupo conocido por sus ataques organizados de ransomware, anunció que se ponía de parte de Rusia

con el conocimiento y la aprobación del gobierno ruso.

Como es lógico, Putin ha negado que Rusia haya tenido parte en ninguno de los incidentes, pero la administración de Biden hizo referencia al incidente contra SolarWinds como una de las razones de las sanciones económicas contra Rusia en abril pasado. Lo cierto es que, en la guerra convencional la atribución suele ser sencilla, pero el ciberespacio es muy complejo y puede llevar mucho tiempo y ser costoso atribuir un ciberataque.

Por su parte, y según recoge Recode, Ucrania ha estado durante años bajo una amenaza casi constante de ciberataques procedentes de Rusia. La red eléctrica del país fue atacada en 2015 y 2016 y, según algunos informes, todavía podría ser vulnerable. El malware llamado NotPetya se desató en el sector financiero de Ucrania en 2017 y terminó extendiéndose a millones de ordenadores en todo el mundo.

Para ser justos, Estados Unidos también ha sido sorprendido usando armas cibernéticas en algunas ocasiones. Se cree que, en coordinación con Israel, está detrás de Stuxnet, un virus que atentó contra el programa nuclear de Irán, aunque ninguno de los países lo admitió nunca.

Ciberguerra en Datos

Según datos recogidos por Check Point Research (CPR), los ciberataques dirigidos contra el Gobierno y el sector militar de Ucrania se incrementaron en un 196% en los tres primeros días de combate.

Los ciberataques a organizaciones rusas aumentaron un 4%, en comparación con el mismo periodo de la semana anterior. En Ucrania, la cantidad global de ciberataques por compañía aumentó un 0,2%, mientras que otras regiones del mundo experimentaron una disminución de las ciberamenazas por empresa.

Casi 260.000 personas se han unido al Ejército de TI de piratas informáticos voluntarios creado por iniciativa del ministro digital de Ucrania, Mykhailo Fedorov

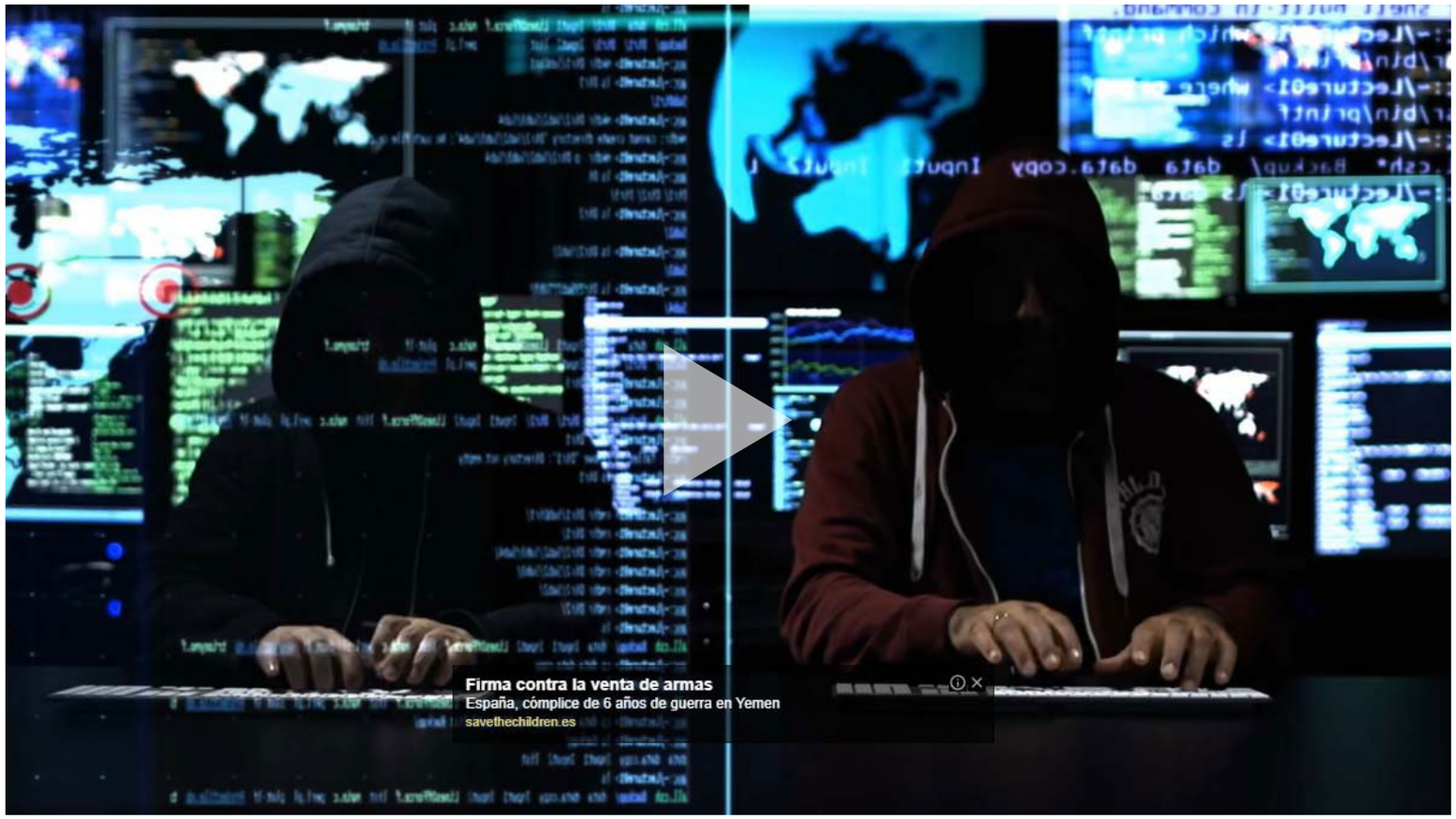
"El conflicto entre Rusia y Ucrania está polarizando el ciberespacio. Los hacktivistas, los ciberdelincuentes, los 'white hat hackers' o incluso las empresas tecnológicas están eligiendo un bando claro, animados a actuar en favor de sus preferencias", alerta Lotem Finkelstein, director de inteligencia de amenazas e investigación de Check Point Software Technologies.

Los investigadores han recogido un aumento significativo de siete veces en los correos de phishing

it whitepapers

ESTRATEGIA DE RUSIA EN EL CIBERESPACIO

Este informe busca aclarar el papel del ciberespacio en el pensamiento estratégico ruso. Analizará las operaciones cibernéticas como un subconjunto de la "confrontación de información" de Rusia y explorará cómo se pone en práctica esta filosofía. El informe examinará tanto las medidas ofensivas, como la participación en la guerra de la información, como las medidas defensivas, como los esfuerzos de Rusia para proteger su propio espacio de información de la influencia extranjera



¿GUERRA CIBERNÉTICA GLOBAL EN UCRANIA?

CLICAR PARA VER EL VÍDEO

en idiomas eslavos del este. Además, un tercio de estos correos electrónicos dirigidos a destinatarios rusos se enviaron desde direcciones ucranianas, reales o falsas.

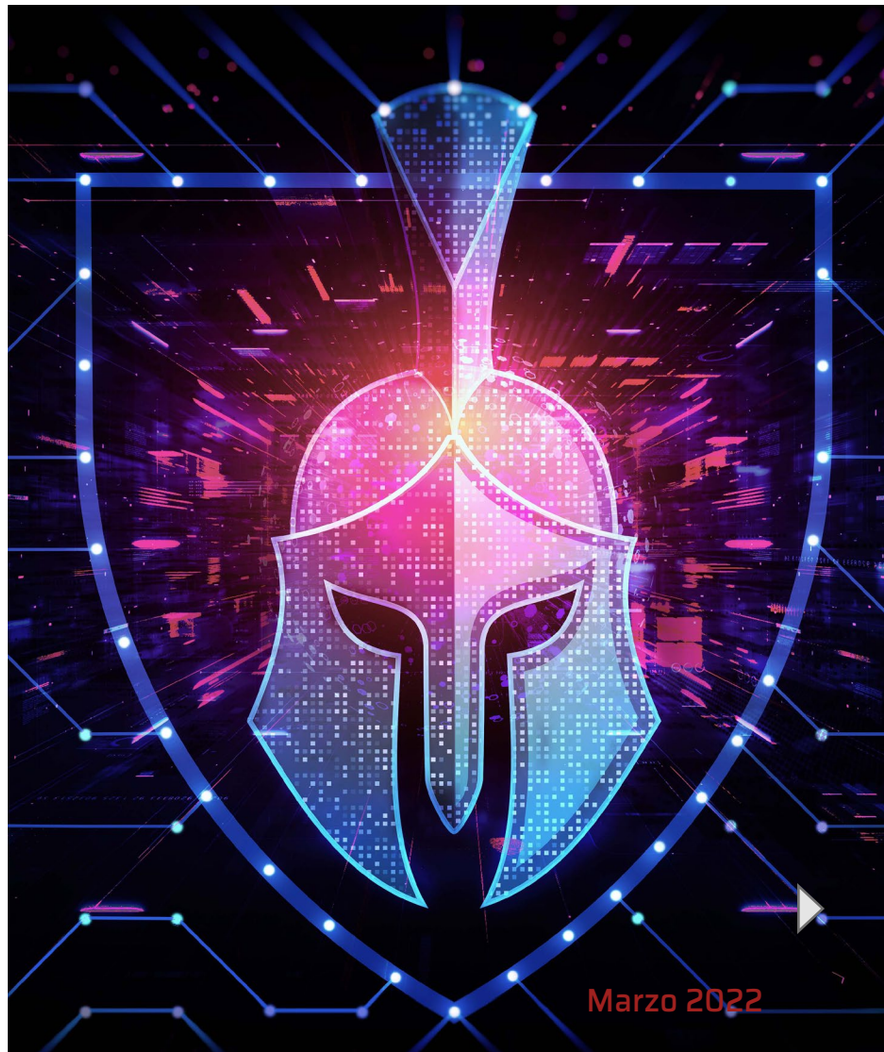
CPR también ha detectado mensajes de correo electrónico fraudulentos que se aprovechan de la situación con el objetivo de obtener un beneficio económico, atrayendo a los destinatarios para que efectúen donaciones a falsos fondos de apoyo a Ucrania.

España en alerta

En plena invasión rusa de Ucrania, el Centro de Operaciones de Ciberseguridad de la Administración General del Estado difundía un correo de advertencia a todos los funcionarios y pedía que durante el primer fin de semana de conflicto los ordenadores y equipos del personal de los distintos ministerios permaneciera apagado.

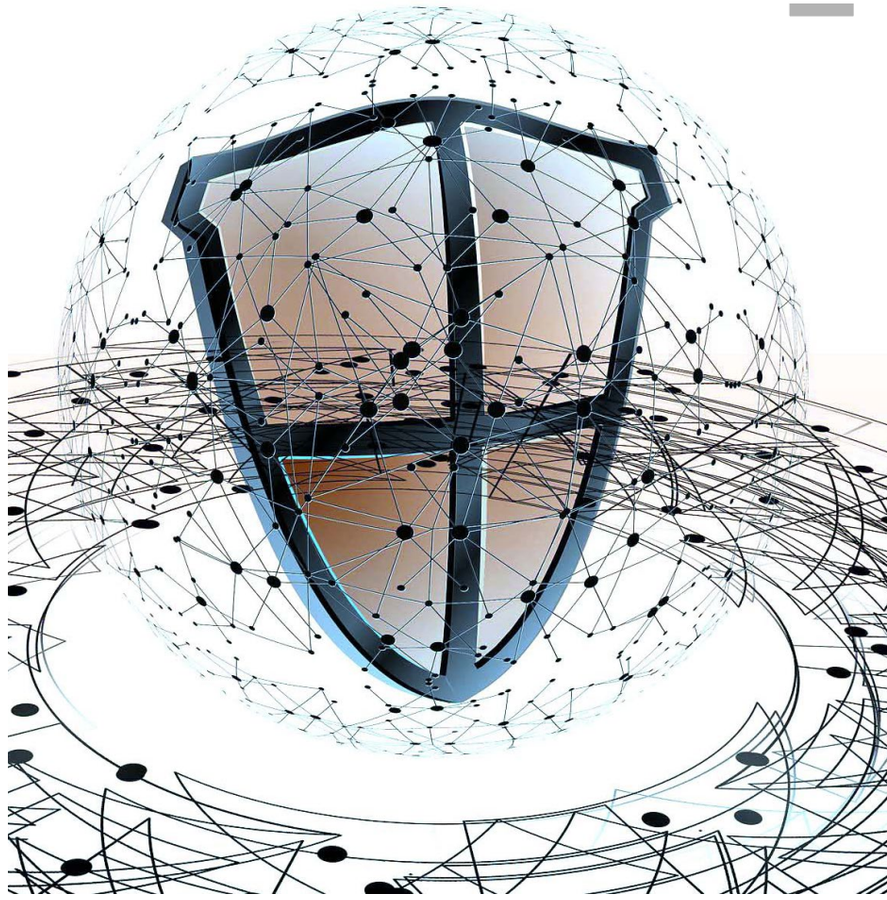
Las AAPP temen que las sanciones acordadas por la Unión Europea, entre las que se

Existe una fuerte campaña de malware proveniente de grupos de ciberdelincuentes rusos y dirigida a los principales grupos de comunicación españoles



encuentran la desconexión de los bancos rusos del sistema de pagos bancarios Swift, la congelación de la mitad de las reservas del Banco Central de Rusia, la prohibición a los oligarcas rusos de utilizar sus activos financieros, el cierre del espacio aéreo de numerosos países occidentales (entre ellos España) a aviones rusos o la prohibición de la emisión de noticias de medios de comunicación estatales rusos como Rusia Today o Sputnik, puedan tener respuesta de Rusia en forma de ciberataques.

Nadie quiere repetir la experiencia del ciberataque que dejó noqueado al SEPE durante meses el año pasado, lo que ha llevado a algunas de las



En sectores estratégicos como la banca también se extreman precauciones y se aumenta el nivel de alerta

NotPety, el malware creado para atacar Ucrania que se extendió por medio mundo

En junio de 2017 se iniciaba lo que posteriormente sería calificado como el ciberataque más destructivo y costoso de la historia. El ransomware NotPetya, dirigido inicialmente contra instituciones gubernamentales, financieras y energéticas de Ucrania, terminó causando daños colaterales a empresas globales con oficinas en y daños por valor de miles de millones de dólares en Europa, Asia y las Américas.

Según los expertos, el ataque "deliberado, malicioso y destructivo" no estaba diseñado para ganar dinero sino para propagarse rápidamente y causar daños. El malware, se aseguró entonces, se disfrazó de ransomware. Ya en su momento Ucrania sugirió que Rusia estaba detrás del ataque, que se produjo en la víspera del día de la constitución de Ucrania, que celebra la separación del país de la Unión Soviética. Rusia anexó Crimea de Ucrania en 2015 y los separatistas prorrusos continúan luchando contra las tropas gubernamentales en el este del país.

Investigaciones posteriores demostraron que NotPetya fue un ciberataque ruso patrocinado por el estado.

Administraciones Públicas españolas a adoptar medidas. En este sentido, organismos como la Seguridad Social, el Consejo de Seguridad Nuclear o el Instituto Nacional de Estadística han instado a sus empleados para que apaguen diariamente sus equipos remotos y se realizarán actualizaciones de seguridad por la noche, entre otras. En el caso del Ministerio de Presidencia, se han generado nuevas contraseñas para su personal, según publica ABC.

En sectores estratégicos como la banca también se extreman precauciones y se aumenta el nivel de alerta para tratar de protegerse contra una ciberamenaza, especialmente las entidades de mayor tamaño y más internacionalizadas a nivel europeo.

Medios de comunicación afectados

Según datos de Iberlayer, un fabricante español de tecnología de ciberseguridad para la protección del correo electrónico, existe una fuerte campaña de malware proveniente de grupos de ciberdelincuentes rusos y dirigida a los principales grupos de comunicación españoles, tanto de prensa escrita como de radio y televisión.

"Con la invasión de Rusia a Ucrania, estamos siendo testigos de la primera guerra híbrida. El ciberespacio se ha convertido en un escenario de batalla tan peligroso como los habituales en los conflictos armados", asegura Pedro David Marco, CEO y Fundador de Iberlayer.

El correo electrónico es uno de los principales vectores de ataque, y según Iberlayer, durante la última semana de febrero el envío de correos electrónicos peligrosos por parte de grupos rusos a los principales medios de comunicación españoles se incrementó de media un 3000%, alcanzando picos en algunos casos de más de 4000% desde el lunes 1 de marzo.

La compañía asegura que desde el pasado 23 de febrero, tan solo un día antes de la invasión rusa a Ucrania, grupos de ciberdelincuentes rusos, que con anterioridad emitían sus correos peligrosos desde direcciones IP rusas, no sólo están focalizando sus esfuerzos sobre los medios de comunicación, sino que además han ido abandonando progresivamente el uso de direcciones IP de ese país y comenzado a utilizar IPs de terceros para el envío de campañas de malware.

Cibersoldados

Casi 260.000 personas se han unido al Ejército de TI de piratas informáticos voluntarios, creado por iniciativa del ministro digital de Ucrania, Mykhailo Fedorov. Informan desde AFP que el grupo, al que se puede acceder a través del servicio de mensajería encriptada Telegram, tiene una lista de objetivos potenciales en Rusia, empresas e instituciones.

Los ciberataques dirigidos contra el Gobierno y el sector militar de Ucrania se incrementaron en un 196% en los tres primeros días de combate

HermeticWiper y Cyclops Blink, dos ciberaramas rusas

El 23 de febrero, el equipo Threat Hunter de Symantec e investigadores de la empresa de ciberseguridad ESET anunciaron el descubrimiento de un nuevo malware llamado **HermeticWiper,** que recibió su nombre del certificado digital falso utilizado para firmar el archivo, que se emite bajo el nombre de una empresa llamada Hermetica Digital.

El malware está diseñado para borrar discos duros o el almacenamiento del sistema de los sistemas que infecta. HermeticWiper funciona corrompiendo primero el Registro de arranque maestro (MBR - Master Boot Record) de cada unidad física. El objetivo parece ser las computadoras anfitrionas en redes críticas. El malware no intenta robar o exfiltrar datos, sino que simplemente los destruye. En tiempos de crisis, el malware podría crear caos al eliminar los datos de importación almacenados en las computadoras personales del personal clave.

Las agencias de ciberseguridad de Estados Unidos y el Reino Unido, publicaron un informe conjunto sobre una nueva variedad de malware llamada **Cyclops Blink.** En ese informe se indicó que el grupo APT Sandworm (también conocido como Voodoo Bear o BlackEnergy) era el responsable de un nuevo malware que se usará para comprometer dispositivos de red de forma remota, principalmente enrutadores de oficinas pequeñas/oficinas domésticas (SOHO) y dispositivos de almacenamiento conectado a la red (NAS). El grupo, según SOCradar, es parte del Centro Principal de Tecnologías Especiales o GTsST de GRU (agencia de inteligencia militar extranjera) de Rusia.

La interrupción de la electricidad en Ucrania en 2015, Industroyer en 2016, NotPetya en 2017, los Juegos Olímpicos y Paralímpicos de Invierno en 2018 o los ciberataques contra Georgia en 2019 se atribuyeron a Sandworm. El nuevo malware, Cyclops Blink, parece reemplazar el malware VPNFilter expuesto en 2018.

Por el momento las acciones parecen estar limitadas a ataques de denegación de servicio (DOS), donde se envían múltiples solicitudes a un sitio web de manera coordinada para saturarlo y derribarlo. Las acciones de desfiguración, en las que el sitio objetivo muestra una página pirateada, también se han observado brevemente en sitios rusos.

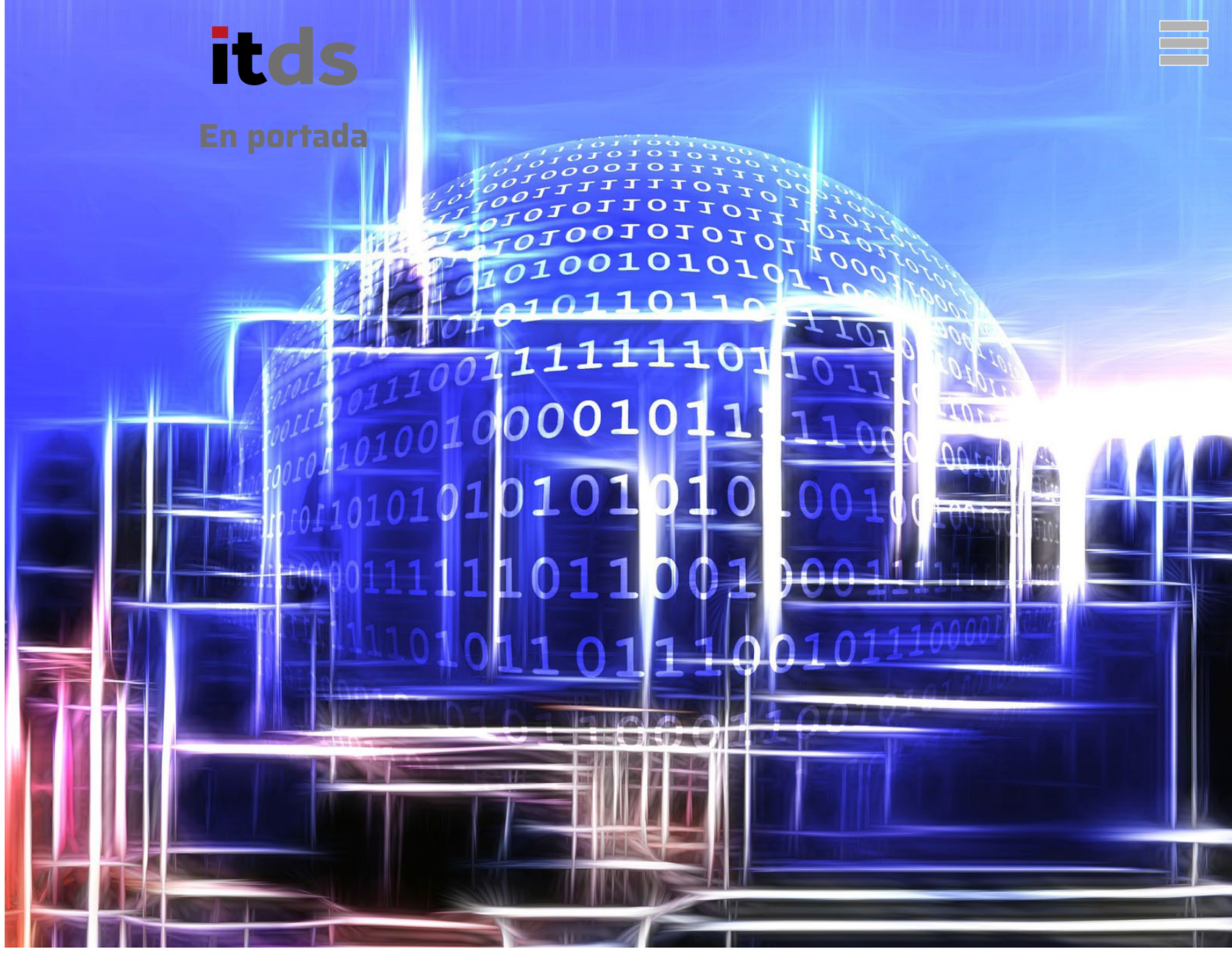
También se podría haber pedido a estos cibersoldados voluntario que intenten identificar las vulnerabilidades de ciertos sitios rusos y enviar esa información a especialistas más experimentados capaces de llevar a cabo acciones intrusivas más sofisticadas, como el robo o la destrucción de datos, según explica Clement Domingo, co- fundador del grupo “Hackers Sin Fronteras”.

Hackers al combate

El 25 de febrero, el grupo de hackers Anonymous declaró la ciberguerra contra el gobierno ruso. Desde entonces, el grupo se ha atribuido el mérito de una serie de ataques DDoS que han inutilizado muchos sitios rusos, incluidos varios sitios web gubernamentales y el sitio web de Russia Today, el medio de comunicación afín al régimen de Vladimir Putin.

Anonymous también dijo que había pirateado la base de datos del Ministerio de Defensa, así como algunos canales de televisión estatales rusos en los que ha publicado contenido a favor de Ucrania, incluidas canciones patrióticas e imágenes de la invasión.

Ucrania ha estado durante años bajo una amenaza casi constante de ciberataques procedentes de Rusia



Según un informe de AFP, Anonymous también dejó mensajes en los sitios web rusos pidiendo a los usuarios rusos que pusieran fin a la guerra.

Anonymous no es el único grupo de hackers que ha mostrado abiertamente de qué lado está. Según recoge SOCradar.io muchos actores de ciberamenazas declararon en qué bando estaban.

Conti, un grupo conocido por sus ataques organizados de ransomware, anunció que se ponía de parte de Rusia, aunque en una segunda declaración exhibió una actitud más suave asegurando que apoyaban la guerra.

El grupo CoomingProject, que ha estado vendiendo/compartiendo los datos que ha obtenido de instituciones críticas desde 2021 en foros de hackers de habla rusa, también se encontraba entre los grupos de hackers que se pusieron del lado de Rusia. El Proyecto Cooming ha anunciado que responderá si el gobierno ruso apunta a un ciberataque.

Formado por componentes de diferentes nacionalidades, no solo de Ucrania y Rusia, sino también de China o Estados Unidos, LockBit anunció que no era parte de la guerra.

Junto con Anonymous, otro grupo hacktivista que apunta a Rusia es AgainstTheWest. En la declaración hecha por el grupo, se afirmó que los sistemas de varias instituciones gubernamentales rusas fueron infectados con ransomware y todos los datos fueron incautados.

Enlaces de interés...

- Los ciberataques contra el Gobierno y el sector militar ucranianos crecen un 196%
- La Seguridad Social o el INE extreman las precauciones ante el aumento del riesgo de ciberataques
- La invasión rusa de Ucrania aumenta el riesgo de ciberataques a nivel mundial
- Anonymous declara la ciberguerra a Rusia
- Ucrania es golpeada por ataques DDoS y por un malware destructor
- Ucrania protagoniza el primer ciberataque del año a un Estado

Los Red Bandits, conocidos por sus ataques de violación de datos, así como los grupos Cyber-Ghost y Sandworm, conocidos por sus ataques DDoS, compartieron en los canales de piratas informáticos que eran partidarios rusos. Se sabe que el grupo Raidforum Admins, que saltó a la palestra con las cibersanciones contra Rusia, está en las filas de Ucrania.

Algunos grupos que llevaron a cabo ataques DDoS en nombre de Ucrania son: IT Army of Ukraine, BlackHawk, y Anonymous Liberland & PWN Bar. Por otra parte, se entiende que el grupo de ransomware llamado Belarussian Cyber Partisans es partidario de la “Ucrania libre”, en la medida en que se le sigue en los canales de Twitter.

Por otro lado, el grupo de extorsión Lapsu$ afirmó haber violado a Nvidia, uno de los mayores fabricantes de tecnología del mundo. Las sanciones estadounidenses y occidentales en represalia por la invasión rusa de Ucrania cortaron el suministro de los principales grupos estadounidenses como Intel, AMD y Nvidia en el ejército de Rusia y su industria tecnológica. Después de la decisión de sanción, los grupos de piratas informáticos de origen ruso supuestamente compartieron datos sobre hashes de los empleados de Nvidia en un canal de Telegram monitoreado por SOCRadar.

Compartir en RRSS

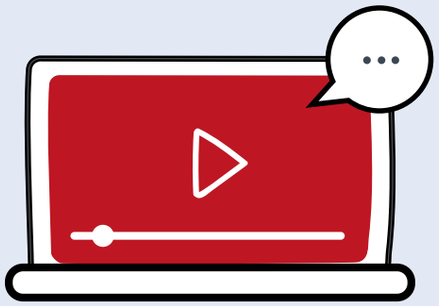
El nuevo paradigma de seguridad para entornos SD-WAN

La desaparición del perímetro tradicional, la adopción de entornos híbridos y multicloud, y el acceso a los recursos empresariales desde cualquier lugar, está acrecentando la convergencia entre la red y la seguridad. En este encuentro conocerás por qué se tiene que adoptar una estrategia SD-WAN, cómo se tiene que gestionar, qué aporta al concepto SASE o cuál es el siguiente paso.

Opera tu IT de forma inteligente y mirando al futuro: conoce OPTIC de Micro Focus

El éxito del negocio en un mundo digital depende de la habilidad de la organización de IT para transformarse al mismo tiempo que el negocio, ofreciendo servicios con agilidad y manteniendo el rendimiento. Pero no es tarea fácil, se requiere un nuevo enfoque.

¡Consulta nuestros webinars!



#ITWEBINARS

La transformación del trabajo: el empleado conectado

ON DEMAND

La naturaleza del trabajo ha cambiado rápidamente. COVID-19 ha tenido, y continuará desempeñando, un papel fundamental en esta transformación del entorno laboral. La mayor parte de las compañías, para mantener a salvo a sus empleados, está adoptando un modelo híbrido o remoto, de manera definitiva. El empleado conectado y productivo requiere, por tanto, de un nuevo entorno de trabajo que le proporcione la mejor experiencia. ¿Cómo construirlo? Únete a este Encuentros IT Trends.

Prioridades tecnológicas para los CIO en 2022

En los últimos dos años el progreso tecnológico se ha disparado. De un lado, la industria avanza en sus propuestas y del otro, la empresa se ha visto abocada a acelerar sus planes de adopción. La transformación digital es una evolución constante y pone sobre la mesa de los decisores de TI múltiples frentes. ¿Cuáles serán sus prioridades en este año?

MAICA AGUILAR CARNEROS

MIEMBRO DEL CONSEJO WOMEN4CYBER SPAIN

Estudió Ingeniería Informática tras terminar la Ingeniería Técnica en Informática de Gestión, en la Universidad Carlos III de Madrid. Navega entre el mundo técnico y jurídico por sus conocimientos de ciberseguridad y privacidad. Lleva más de 14 años vinculada al sector de la ciberseguridad. Actualmente es gerente de Ciberseguridad en Ferrovial, donde entre otras funciones, se encuentran en su ámbito de responsabilidad el Compliance IT, la Gestión de Identidades y la Cultura de ciberseguridad. Es miembro del Comité de Protección de datos de Ferrovial y del Comité del Data Privacy Institute del ISMS Forum. Forma parte del Consejo de Women4Cyber Spain, el capítulo nacional vinculado a la Fundación Women4Cyber de la European Cyber Security Organization. Mentora en distintas iniciativas para promover ciberseguridad y diversidad; docente en masters y certificaciones de Privacidad, Seguridad y Data.

Ciberseguridad desde una perspectiva diferente

Solemos leer artículos donde se pone sobre la mesa la importancia de la Ciberseguridad, donde se habla de las variadas amenazas que se incrementan día a día, debido a la evolución digital y tecnológica que estamos viviendo y que están cambiando las reglas del juego a velocidad de vértigo; artículos donde con números y porcentajes se evidencia el aumento de las amenazas, de ciberincidentes y ciberdelincuencia; donde se habla de esa parte oscura de esta realidad dinámica y del tsunami tecnológico que somos afortunados de estar viviendo: La revolución digital. Hoy vamos a hablar de ciberseguridad desde una perspectiva diferente.

Mi historia

Mi infancia fue en un mundo muy diferente al de mis hijos. Un mundo en el que a mi madre no le permitieron estudiar porque en las familias humildes al que había que dar estudios no era al más capacitado, sino al hombre, para que pudiese mantener una familia en el futuro. Un mundo en el que mis padres se esforzaron porque yo tuviese oportunidades y pudiese llegar a donde quisiera. ¡Qué suerte tuve!

Era un momento en el que nuestra sociedad mantenía ciertas carencias y sesgos debido a patrones heredados que dificultaban la diversidad, el crecimiento y la evolución. Siempre he pensado que fui afortunada en nacer dónde y cuándo nací, en esta gran ciudad que es Madrid a mediados de los 70 ¿Qué habría sido de mí si hubiese nacido unas décadas antes o en un pueblo o en otro país? ¿Tú lo has pensado alguna vez?

Pude estudiar una carrera. Estudié lo que quise, Ingeniería Informática y aquí estoy hoy, en esta revolución digital, dedicada a que estemos un poco más seguros en el entorno profesional y personal. Soy una mujer normal.

A veces, cuando me preguntan a qué me dedico me da un poco de vergüenza decir que a Ciberseguridad. No es raro percibir en los ojos de esas personas ajenas a este sector un poco de decepción. Sí, soy una persona normal, una persona que no encaja con la imagen general que se tiene de los profesionales que nos dedicamos a esto.

Al igual que cuando era niña y quería pasar desapercibida, a veces me siento tentada de inventarme otra profesión para dejar que la sociedad siga pensando que vestimos de negro, llevamos gorro, siempre hablamos a través del ordenador y somos un poco asociales. No lo hago, he aprendido que, aunque es más fácil situarte en un perfil bajo, el principal cambio tiene que venir de nosotros mismos. Tenemos que levantar la cabeza y dar un paso al frente, atrevernos y exponernos. Estamos aquí, somos much@s y no nos tiene que dar miedo ser visibles. El camino que hemos emprendido va a guiar el paso de los siguientes y tenemos que mostrar nuestra bonita profesión.

Estamos aquí, somos much@s y no nos tiene que dar miedo ser visibles

Si estás leyendo este artículo es muy probable que vengas del mundo tecnológico, y me gustaría pedirte un favor, me gustaría pedirte que colabores, me gustaría pedirte que participes de forma activa por una buena causa, que con tu conocimiento y tus habilidades nos ayudes a devolver a esta sociedad lo que nos ha dado, y ya de paso a mejorarla un poquito. Únete a nuestra causa.

Trabajamos para visibilizar el talento femenino que existe actualmente en el sector, para que sirva como referente para las nuevas generaciones

Piensa qué puedes hacer desde tu posición para que nuestros hijos disfruten de un mundo más seguro, inclusivo, diverso, y justo. Un mundo digital en el que se sepan mover, hacer un uso responsable, en el que todos tengamos igualdad de oportunidades y la ética esté presente.

Las nuevas generaciones son nuestro futuro y tienen que estar preparados para usar la tecnología con seguridad, conocer los riesgos y actuar ante ellos.

¿Las personas como capa de protección ante los ataques?

No cabe duda de que, en el proceso de la transformación digital, la ciberseguridad es un pilar fundamental y tenemos que formarnos para asimilar las oportunidades y retos que conlleva.

La seguridad no sólo va de tecnología, no sólo va de procesos, también va de personas. Las personas son clave cuando hablamos de ciberseguridad. Sin embargo, en muchos casos se olvida que la educación en ciberseguridad brinda protección contra el comportamiento humano en escenarios de riesgo, necesitamos “firewall humanos”.

Aproximadamente en un 90% los ciberataques intervienen como vector de entrada la personas. Dicho de otra forma: cómo el eslabón más débil de la cadena de protección somos los personas, los ciberdelincuentes focalizan sus técnicas de engaño hacia nosotros.

La ciberseguridad ha dado ya un paso al frente, existen distintas actuaciones público-privadas a nivel internacional, europeo y nacional, orientadas no sólo a que los productos y servicios que utilizamos tengan un nivel de seguridad adecuado, sino también a que la sociedad identifique los riesgos digitales existentes en nuestro día a día y sepa cómo enfrentarse a ellos. Tenemos que tejer esa red de “firewall humanos”.

Podemos hablar de la importante labor que el INCIBE (Instituto Nacional de Ciberseguridad de España) está realizando con sus campañas, formaciones e iniciativas entre las que se encuentran la de Cibercooperantes o la puesta en marcha del teléfono 017. Este servicio 017, abre un canal directo en el que los ciudadanos pueden informarse, formarse y trasladar sus problemas de ciberseguridad por diversas vías: Web, WhatsApp, YouTube, Telegram, etc.

Mencionar también el Foro Nacional de Ciber Seguridad, como un espacio de colaboración público-privada impulsado por el Consejo de Seguridad

En el proceso de la transformación digital, la ciberseguridad es un pilar fundamental y tenemos que formarnos para asimilar las oportunidades y retos que conlleva

Nacional y en el que actualmente se está desarrollando el Libro Blanco sobre cultura de ciberseguridad en España.

La Nueva Estrategia de Ciberseguridad de la Unión Europea, aprobada en diciembre de 2020, también considera en el Plan de Acción de Educación Digital el aumentar la concienciación sobre la ciberseguridad entre los ciudadanos, poniendo foco en las nuevas generaciones. En este sentido ENISA (Agencia de la Unión Europea para la Ciberseguridad), que tiene encomendada la misión de velar por un alto nivel común de ciberseguridad en toda Europa, durante el mes de Octubre ENISA promueve el mes de la Ciberseguridad en Europa ofreciendo recomendaciones de ciberseguridad con objeto de generar confianza en los servicios digitales y ayudar a los ciudadanos a proteger sus datos personales, financieros y profesionales.

Desde Women4Cyber

Desde Women4Cyber Spain también contribuimos con acciones formativas y de concienciación a crear una cultura digital y de ciberseguridad en la sociedad que favorezca la alfabetización digital promoviendo talleres, cursos, ponencias y todo tipo de actividades que ayuden a las personas a adquirir competencias digitales y a crear conciencia de los riesgos existentes en el uso de la tecnología.

Enlaces de interés...

- W4C Spain
- Programa de Mentoring

Adicionalmente, trabajamos para visibilizar el talento femenino que existe actualmente en el sector, para que sirva como referente para las nuevas generaciones, acercando y humanizando nuestra profesión a la vez que reduciendo la imagen de "frikismo" que socialmente se le ha atribuido.

Women4Cyber Spain mediante su programa de mentoring apoya a personas que se encuentra al inicio de su carrera profesional, facilitamos orientación profesional y el acceso a redes profesionales, así como desarrollamos iniciativas para fomentar las carreras tecnológicas entre las niñas y adolescentes conectándolas con el mundo de la tecnología y de la ciberseguridad.

Women4Cyber Spain es el capítulo español de la Fundación Europea sin ánimo de lucro W4C (ECSO), cuyo objetivo es promover, impulsar y apoyar la participación de las mujeres en el ámbito de la ciberseguridad y la tecnología en general. Nuestra misión es fomentar e impulsar las sinergias público-privadas, privadas-privadas y con la sociedad civil de manera de crear entre todos un mundo digital más diverso, seguro, colaborativo e inclusivo. Recuerda, que nuestra asociación está dirigida a todos los públicos porque el cambio social necesario lo conseguiremos entre todos.

it User
TECH & BUSINESS

Cada mes en la revista, cada día en la web.

La era DeFi

Como indica el informe de Minsait sobre tendencias en medios de pago, el impulso del que se ha beneficiado esta industria durante los meses más duros de la pandemia merecerá la pena si se consolidan estructuralmente los cambios acecidos, tanto en la conducta de los consumidores como en la entrada en escena de nuevos jugadores y de la mejora de soluciones para dar respuesta a las necesidades emergentes de los usuarios.

JOSÉ MANUEL NAVARRO

CMO MOMO GROUP

José Manuel Navarro Llena es experto en Marketing, Durante más de treinta años ha dedicado su vida profesional al sector financiero donde ha desempeñado funciones como técnico de procesos y, fundamentalmente, como directivo de las áreas de publicidad, imagen corporativa, calidad y marketing. Desde hace diez años, basándose en su formación como biólogo, ha investigado en la disciplina del neuromarketing aplicado, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas. Es Socio fundador de la agencia de viajes alternativos Otros Caminos, y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España SEFIDE EDE de la que en la actualidad es director de Marketing. Autor de “El Principito y la Gestión Empresarial” y “The Marketing, stupid”, además de colaborador semanal desde 2006 en el suplemento de economía Expectativas del diario Ideal (Grupo Vocento).

Compartir en RRSS

Si bien el crecimiento del comercio electrónico se ha moderado en los últimos meses y el uso del dinero efectivo sigue manteniendo un margen mínimo que no avala las predicciones de su desaparición, otros parámetros se siguen comportando como se esperaba que ocurriera para el período "post-covid". Nos referimos a que:

- **La banca tradicional sigue siendo el proveedor principal en el sistema financiero,** si bien los nuevos operadores le van ganando cada día posiciones al atraer a un importante número de usuarios y de nuevos bancarizados que buscan modelos de relación más innovadores y soluciones más personalizadas.
- **La diversificación de los medios de pago digitales crece,** aunque sin mermar en exceso a los tradicionales; billeteras, agregadores de cuentas, app de pago entre particulares (P2P) y transferencias inmediatas alcanzan ya a más de un tercio de la población y, sin embargo, no terminan de desplazar a las tarjetas (crédito y débito) del pódium de las compras en comercio físico y electrónico.
- **Asociaciones y colaboraciones entre actores del sector Fintech,** y entre éstas y bancos tradicionales para compartir datos y soluciones más

A pesar de que los volúmenes de criptodivisas aún son pequeños, su crecimiento y adopción por, cada día, más usuarios, recomienda una urgente regulación

Los retos del sistema DeFi serán, primero, mejorar su velocidad actual de procesamiento y ampliar la oferta básica de contratos financieros ("smart contract") de préstamo e inversión a servicios básicos de ahorro y de medio de pago universal

innovadoras, están enriqueciendo el ecosistema, aportándole más valor y generando nuevas oportunidades más eficientes y escalables.

▪ **La necesidad de establecer procesos más seguros y convenientes** en las transacciones sin contacto y de autoservicio (mediante procedimientos de autenticación reforzada y biométrica) ha obligado a los proveedores de servicios financieros y de pago a simplificar las operaciones para mantener una experiencia de usuario satisfactoria, pasando de ser un modelo de operatoria obligada por las circunstancias a uno confiable y demandado por los usuarios para sentirse más seguros frente a posibles fraudes. La innovación en este terreno no ha dejado de crecer poniendo al cliente en el centro de todos los desarrollos para lograr soluciones más intuitivas, humanas y personalizadas.

▪ **La rápida transformación digital del conjunto del sector financiero** ha permitido a muchas entidades generar más ingresos (informe Infosys) de los previstos, no solo por la automatización de muchos procesos sino, también, por la búsqueda de mayor retorno de las inversiones realizadas mediante la aplicación de analíticas avanzadas para un mejor conocimiento del cliente. En un entorno donde los precios dejan márgenes de intermediación muy justos y la oferta de soluciones gratuitas por los nuevos “player” no permite establecer tarifas para muchos epígrafes que antes suponían importantes ingresos, les ha obligado a cambiar las políticas que afectaban a los recursos fuera de balance y a crear un nuevo sistema de servicios personalizados bajo demanda más aceptado por los clientes.

itds

Tribuna

El crecimiento del comercio electrónico se ha moderado en los últimos meses y el uso del dinero efectivo sigue manteniendo un margen mínimo que no avala las predicciones de su desaparición

No obstante, la tendencia en el sector es que las disrupciones audaces de las Fintech se aceleren mediante la incorporación de transformaciones más desafiantes que apuntan a un modelo financiero desintermediado. Si bien es cierto que se ha avanzado en la regulación de las nuevas empresas financiero-tecnológicas, encaminada a proporcionar unas reglas de juego comunes para todo el sector y a proteger a sus clientes con fórmulas que permiten una mayor transparencia y libertad de elección y de gestión del dinero, la tecnología basada en blockchain está propiciando que, cada vez, sean más las personas atraídas por las aplicaciones financieras descentralizadas (DeFi), no reguladas ni respaldadas por organismos centrales supervisores.

La irrupción de las criptomonedas generó en muchos ciudadanos el espejismo de la independencia y el control autónomo sobre su dinero, pero la deriva que ha tomado la “criptoeconomía” se ha alejado de este concepto y ha abrazado rápidamente el modelo especulativo de un mercado de activos con un elevado componente de riesgo y volatilidad, muy atractivo para para inversores avezados y con exceso de tesorería. Aunque los datos no son fáciles de obtener, se estima que unos 300 millones de personas poseen alguna de las más de diez mil criptomonedas circulando en el mercado global (informe TripleA), almacenadas en billeteras digitales de custodia centralizada o descentralizada (Exchanges CEX o DEX). Igualmente, el número de operaciones realizadas con criptodivisas es bastante complejo de calcular ya que los fondos no se suelen mover para transacciones de pago y, en la gran mayoría de las ocasiones, se limitan a ser órdenes de compra o de venta. Aún así, se estima que se realizan unas 280.000 transacciones al día (muy lejos de los casi mil millones que se realizan con VISA y MasterCard).

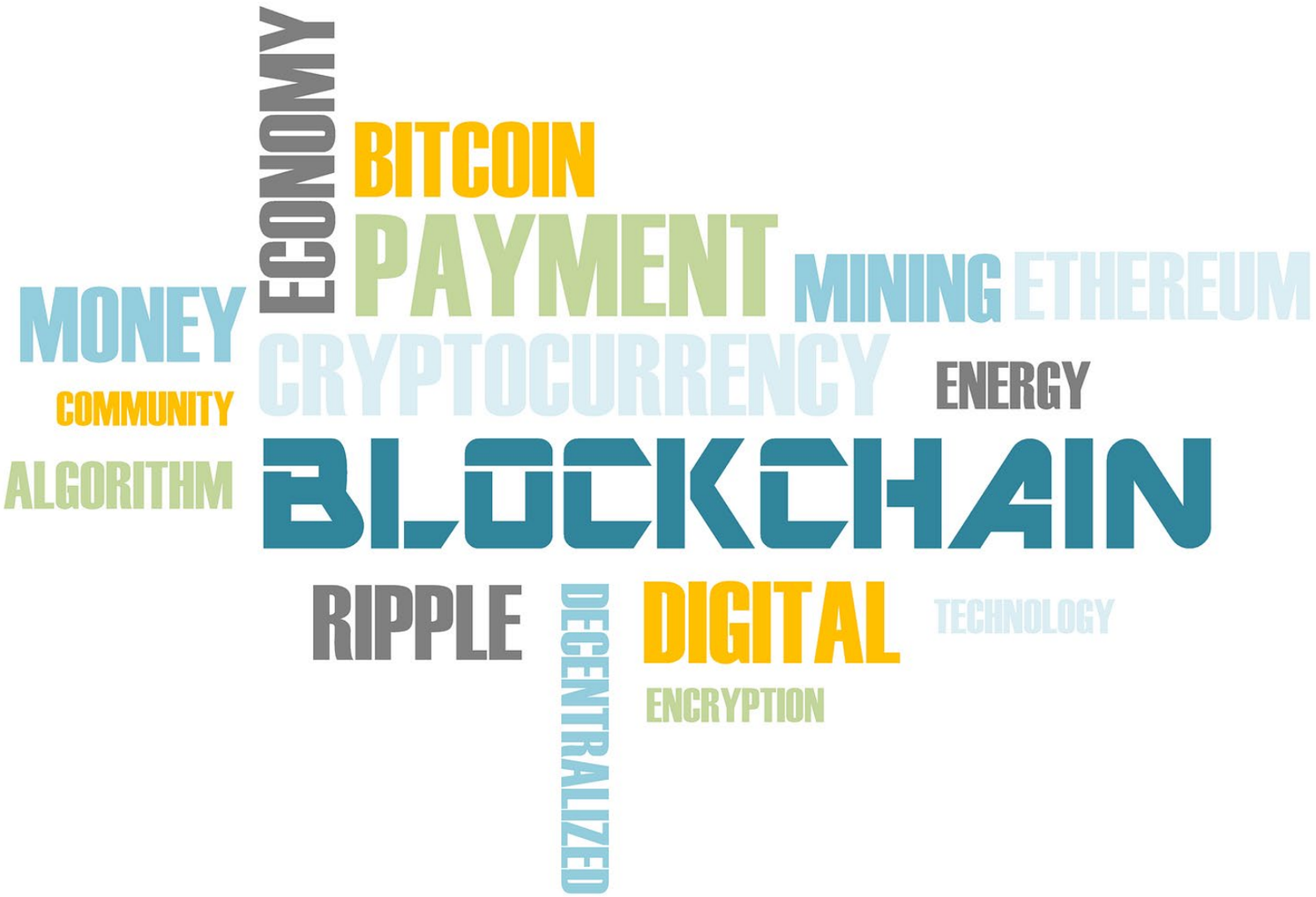
A pesar de que los volúmenes de criptodivisas aún son pequeños (Bitcoin procesó 489.000 millones de dólares por trimestre en 2021 frente a los 5 billones de dólares de VISA y MasterCard), su crecimiento y adopción por, cada día, más usuarios recomienda una urgente regulación, como expone el BPI, para evitar el excesivo apalancamiento de este mercado descentralizado, así como sus continuos desajustes de liquidez y elevada volatilidad de su valoración, siempre dependiente de la confianza del conjunto de usuarios e incapaz de

Son legítimas las preocupaciones de reguladores y responsables políticos sobre la dimensión que están tomando los servicios DeFi, pero también son conscientes del importante potencial transformador del sector financiero

desvincularse de los parámetros económicos clásicos, como se ha visto por su respuesta a las fluctuaciones en la inflación y a las políticas de precios de los bancos centrales. En este escenario, se hace imprescindible proteger a los inversores desde tres vías: frente al fraude y a las actividades ilegales, y dotando de garantías de estabilidad al sistema.

En el caso de Europa, se está trabajando en la regulación mediante el proyecto de reglamento sobre los mercados de criptoactivos (“MiCA”), iniciativa para introducir un marco armonizado y completo para la emisión, aplicación y prestación de servicios en criptoactivos. De aprobarse esta normativa, se abrirá la puerta a que se pueda realizar cualquier tipo de negocio con estos criptoactivos, lo cual normalizará la situación de los proveedores de servicios de criptomonedas (CASP) y formalizará su uso como medio de pago. Aunque se prevé que la implementación del MiCA tendrá lugar en 2024, algunos pasos ya se han dado como han sido la publicación de la circular de la CNMV acerca de la publicidad sobre criptoactivos y la apertura del registro en los bancos de centrales de empresas Exchange (para cambio y custodia).

Son legítimas las preocupaciones de reguladores y responsables políticos sobre la dimensión que están tomando los servicios DeFi, pero también son conscientes del importante potencial transformador del sector financiero. Por ello, la actuación con cautela de los legisladores implica también cierto acompañamiento de propuestas como las



Enlaces de interés...

- W Informe Minsait sobre tendencias en medios de pago
- W Acelerando la Transformación Digital
- I Criptomonedas alrededor del mundo
- I BPI
- W Circular de la CNMV acerca de la publicidad sobre criptoactivos

presentadas en el Foro Económico Mundial para dar sentido a estas tendencias y elaborar una orientación adecuada de las políticas regulatorias para mantener el equilibrio entre la voluntad de los inversores de mantenerse al margen de los mercados tradicionales y la voluntad de los supervisores de proteger la estabilidad financiera global. Si ese equilibrio no se consigue, se corre el riesgo de que muchos inversores se salgan del DeFi, lo cual supondrá graves caídas del valor de los criptoactivos, algo que algunas voces auguran podría ser el derrumbe de la "criptoburbuja".

Los retos del sistema DeFi serán, primero, mejorar su velocidad actual de procesamiento y ampliar la oferta básica de contratos financieros ("smart contract") de préstamo e inversión a servicios básicos de ahorro y de medio de pago universal, mediante el respaldo que ofrece blockchain de un modelo más transparente, seguro y fuera de control de intermediarios. Y segundo, promover la suficiente formación de los usuarios para poder acceder de forma libre, consciente y preparada para gestionar sus posiciones con autonomía y sin riesgos. La regulación ayudará al alcanzar el primer reto, pero el segundo será más complejo de lograr en un alto porcentaje de la población, a no ser que todos los actores implicados se impliquen en la educación financiera necesaria de sus usuarios para garantizar la consolidación de este sistema financiero descentralizado.