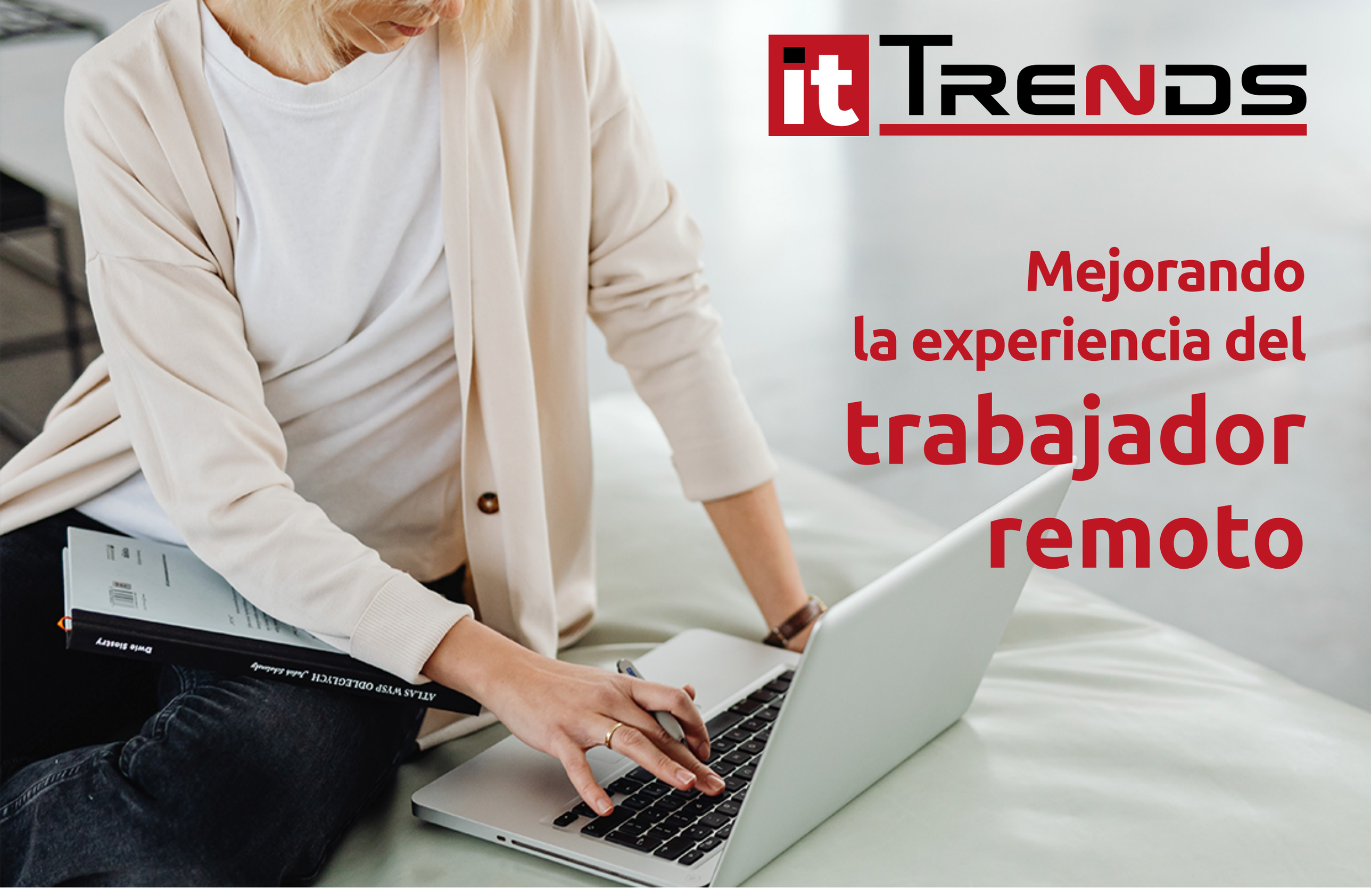


it TRENDS

Mejorando la experiencia del trabajador remoto

GRENKE SONICWALL SOPHOS WatchGuard NFON Cloud Telephone System hp citrix

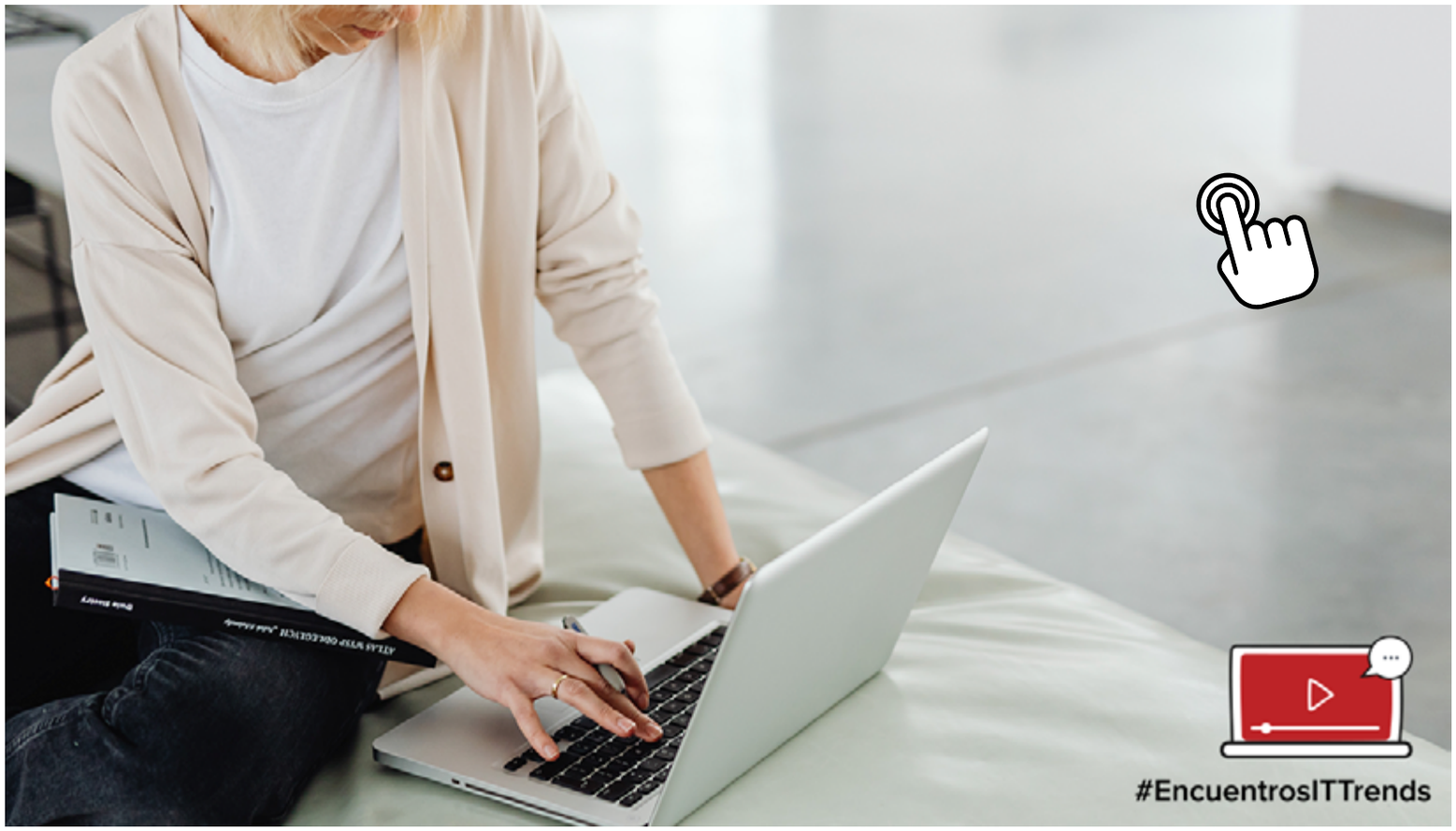
#ENCUENTROSITTRENDS

Mejorando la experiencia del trabajador remoto

Para 2021, tres de cada diez empleados trabajarán desde sus casas. El teletrabajo se ha impuesto como una modalidad habitual de trabajo en todo tipo de organizaciones para aportar la flexibilidad que los empleados demandan, pero también para garantizar la continuidad de los negocios en caso de incidentes. Esté donde esté, el trabajador necesita acceder a todos los recursos empresariales, pero desde su casa, muchas veces con su propio equipo y casi siempre con su conexión a internet, lo que requiere aplicar tecnologías y modelos de seguridad específicos.

Trabajar en remoto también ha impuesto otra dinámica en las reuniones, ahora online y virtuales, necesarias para mantener la marcha de la empresas y los vínculos con la misma.

En IT Trends hemos reunido a diversos expertos para abordar los retos del teletrabajo y cómo avanzar en la productividad y el mejor desempeño de los empleados ahora que lo habitual es trabajar fuera de la oficina, en una sesión titulada Mejorando la experiencia del trabajador remoto, que constó de dos mesas de debate: la primera de ellas, con profesionales del mundo académico, técnico y de Recursos Humanos, y la segunda con especialistas en tecnologías de comunicaciones, seguridad, dispositivos o conexiones que involucran el trabajo remoto. ■



#ENCUENTROSITTRENDS

Nuevas modalidades de trabajo: el empleado remoto

Sonia Fernández Palma, consultora educativa y divulgadora en Ciberseguridad y Alfabetización Digital y miembro de Women4Cyber; Antonio Ramos, Vocal de la Junta Directiva de ISACA Madrid y Rafael Cubero Saiz, Head of People de Tecnatom Group, conversan sobre el impacto del teletrabajo en las empresas.

NUEVAS MODALIDADES DE TRABAJO: EL EMPLEADO REMOTO

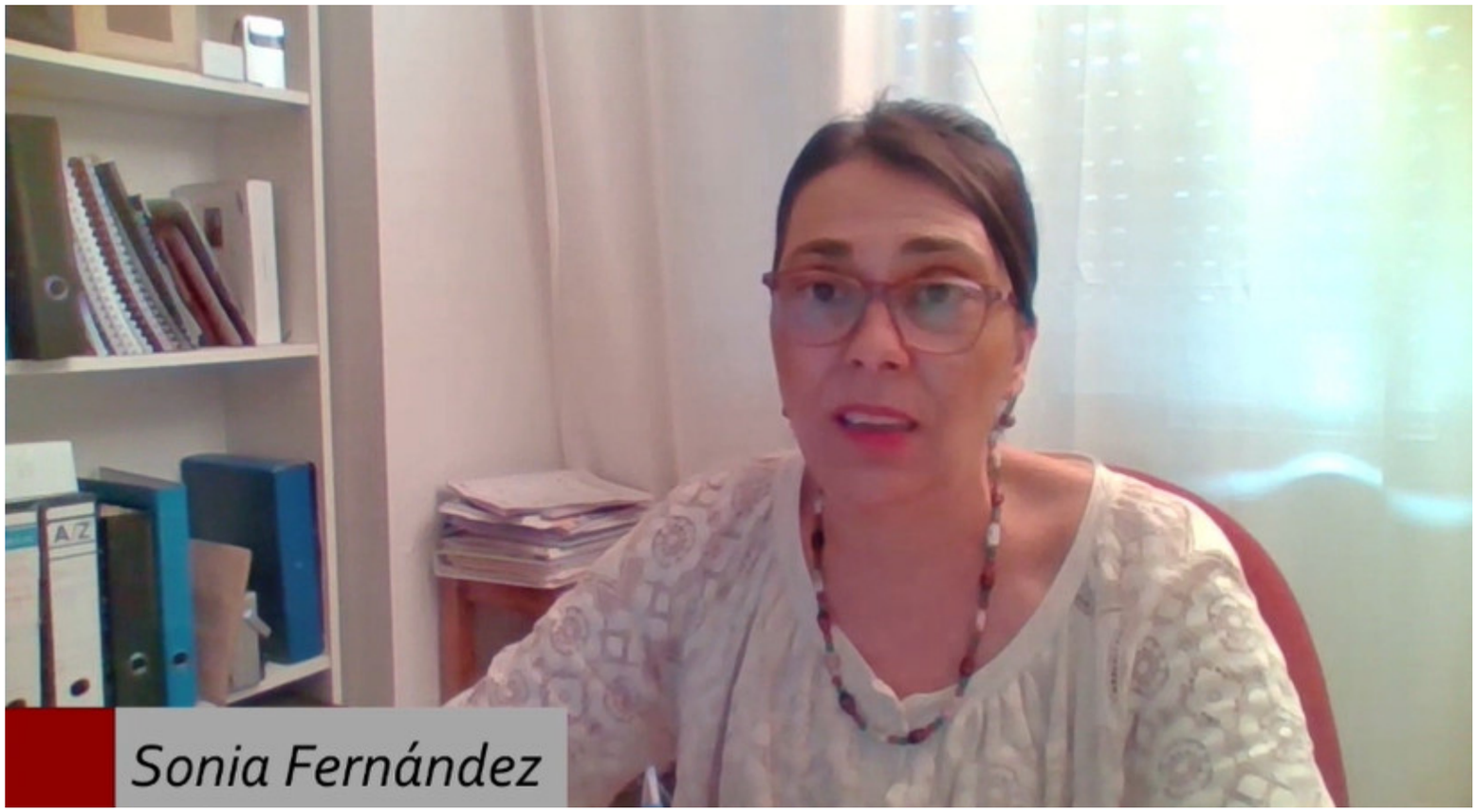
Durante el Encuentro IT Trends titulado Mejorando la experiencia del trabajador remoto, tuvo lugar un primer debate cuyo objetivo fue examinar el teletrabajo y su impacto tanto en los empleados como en las empresas y departamentos de recursos humanos. Para ello se contó con la participación de So-

nia Fernández Palma, consultora educativa y divulgadora en Ciberseguridad y Alfabetización Digital y miembro de Women4Cyber; Antonio Ramos, Vocal de la Junta Directiva de ISACA Madrid; y Rafael Cubero Saiz, Head of People de Tecnatom Group.

Para Sonia Fernández Palma "lo que hemos vivido durante estos últimos meses ha sido y sigue siendo una situación excepcional que requería, sobre todo en el principio, de una actitud extraordinaria, tanto por parte de empresas como de personas de los trabajadores".

La respuesta de las organizaciones empresariales frente al cambio de modelo de negocio ha sido mixta, aseguró Antonio Ramos, quien añadió que muchas empresas afrontaron esta situación "con mucha premura, con mucha improvisación y corriendo muchos riesgos de seguridad". En todo caso, "el que más y el que menos ha sacado un gran aprendizaje. Creo que a partir de ahora podemos afrontar estas situaciones con mucha más experiencia, con mucho más conocimiento y sabiendo un poco mejor a qué nos enfrentamos".

En Tecnatom Group, "la situación se vivió como algo positivo porque lo que los empleados percibieron es que les estábamos cuidando", dijo Rafael Cubero, explicando que hubo un trabajo importante en el área de comunicación para que las relaciones entre las personas y con la empresa no se viesen perjudicadas. La empresa se apoyó en una red social empresarial creando grupos "para poder estar más unidos y no tener sentimientos de soledad", así como otras actividades, campañas y rutinas para mantener activas las relaciones entre empleados y con la empresa". Añadió que la clave fue una coordinación entre las áreas de IT, el área de recursos humanos y el área de servicio médico.



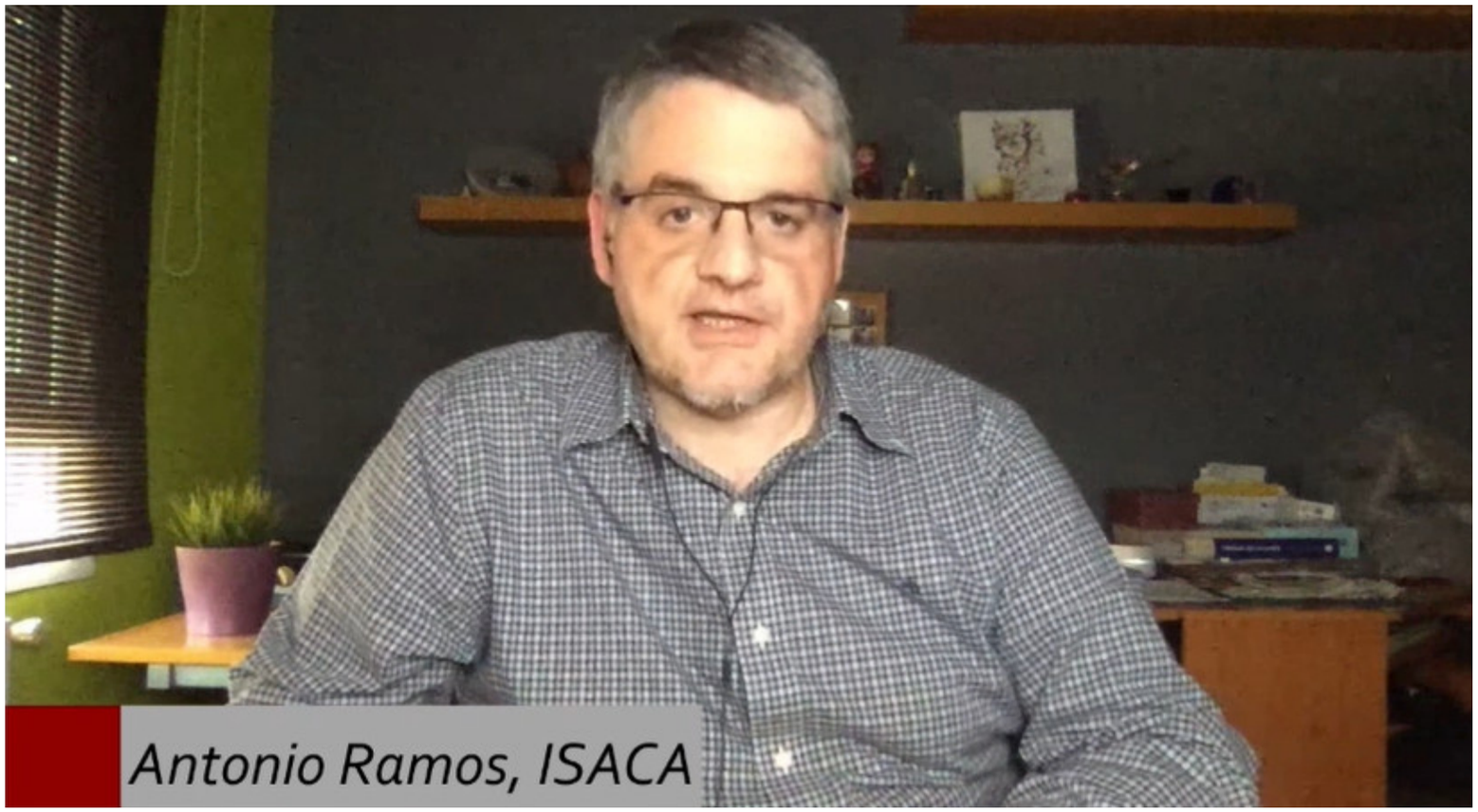
"Para mí, el gran secreto del teletrabajo es la formación"

SONIA FERNÁNDEZ PALMA, CONSULTORA EDUCATIVA Y DIVULGADORA EN CIBERSEGURIDAD Y ALFABETIZACIÓN DIGITAL Y MIEMBRO DE WOMEN4CYBER SPAIN

Asegurando que el principal activo de una empresa son las personas, y que es a las personas a las que hay que cuidar, dijo Sonia Fernández, que no sólo hay que darles herramientas a los empleados, sino formarles para saber utilizarlas. “Para mí el gran secreto es la formación”, aseguró esta consultora mencionando de manera específica la formación en habilidades digitales, muy especialmente en materia de seguridad, así como las habilidades sociales porque “no podemos pensar que como tenemos una pantalla delante, eso es una barrera”.

Además de las ventajas que aporta, como permitir la continuación del negocio, ¿qué retos está planteando este nuevo modo de trabajo? Para Antonio Ramos los retos son muchos “porque trabajar en este entorno digital hace que tengamos que cambiar a la forma en la que veníamos trabajando”, desde temas organizativos a temas técnicos, gestión del conocimiento y de seguridad.

“Lo principal es el negocio y ese es el punto de partida desde donde arrancamos”, dijo Rafael Cubero cuando se le plantea cómo se ha unido el área tecnología, negocio y recursos humanos en tiempos de pandemia. Explicó que algunos perfiles no podían dejar de ir a la oficina, pero que “trabajamos en crear el entorno más seguro posible”, mientras que a todas las personas que podían hacer el trabajo remoto se les dieron todas las posibilidades para hacerlo. En todo caso, en Tecnatom Group no se partía de cero, ya que se contaba con un sistema de trabajo a distancia que “ayudó a que la gente ya supiese a qué se enfrentaban”. Además, el departamento de sistemas tuvo varias tareas a realizar, desde asegurarse que todo el mundo tuviese un portátil para poderse llevar a casa, o una pantalla, reforzar las VPNs o “tareas de formación de todo el portfolio de herramientas de comunicación colaborativas que


Antonio Ramos, ISACA

“Trabajar en este entorno digital hace que tengamos que cambiar la forma en la que veníamos trabajando”

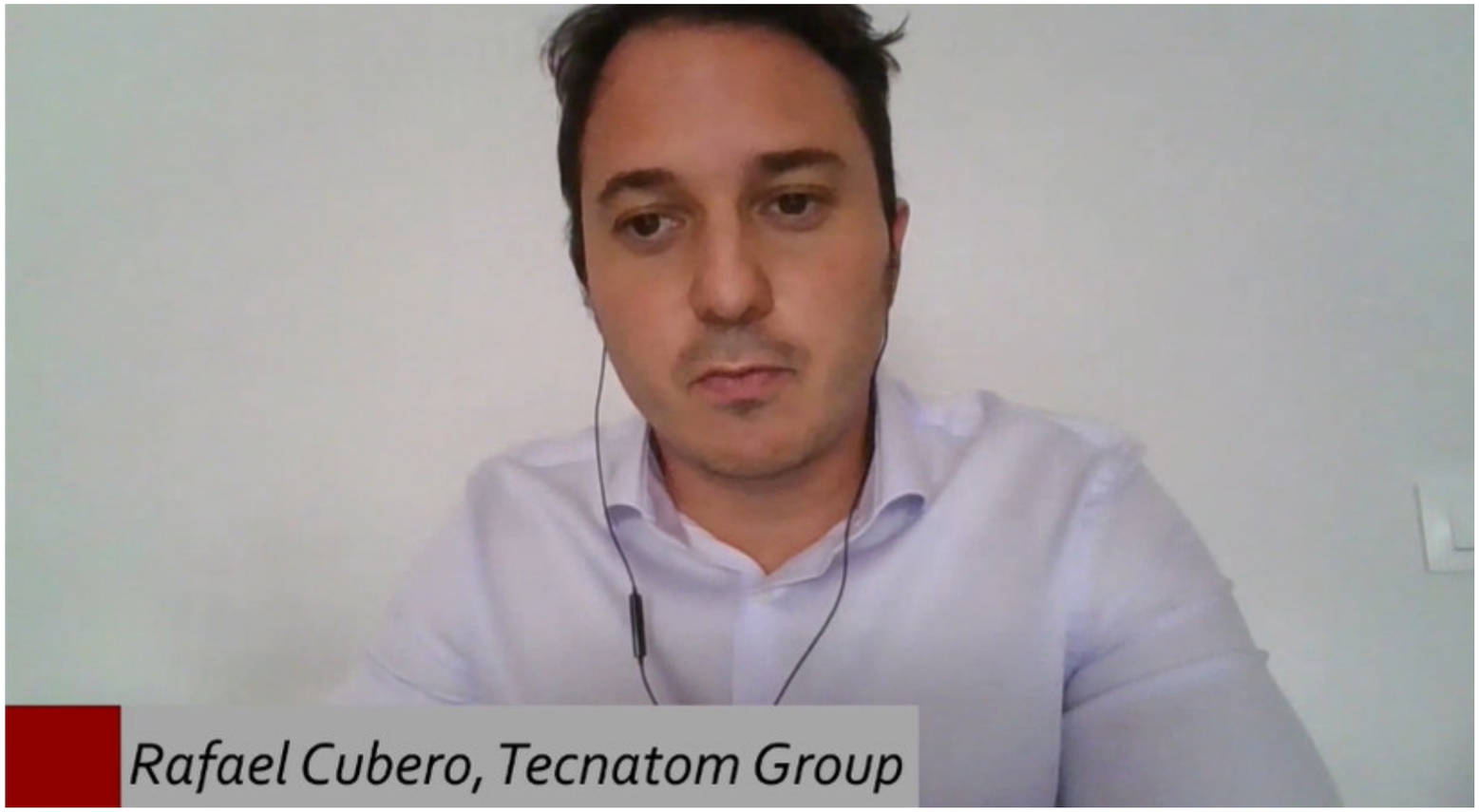
ANTONIO RAMOS, VOCAL DE LA JUNTA DIRECTIVA, ISACA MADRID

tenemos a nuestra disposición y que mucha gente no conocía".

Sobre cómo mejorar la experiencia del teletrabajo, apuntó Sonia Fernández que es importante que el teletrabajo tenga unas normas claras, "que se sepa a qué debemos atenernos". Añadió esta consultora y miembro de la asociación Women4Cyber Spain que es importante aceptar "que ya no vivimos en el mundo en el que vivíamos, sino que vivimos en otro con unas posibilidades infinitas y unos beneficios muy grandes, pero también con algunos inconvenientes y muchos retos por delante".

Respecto al modelo híbrido de trabajo dijo Antonio Ramos que hacer convivir el modelo tradicional asistencial con el remoto es un reto desde el punto de vista tecnológico. Aseguró que no está definida una situación en la que "tengo que ser capaz de hacer convivir un mundo en el que parte del tiempo se va a estar en la oficina y parte del tiempo fuera", algo que impacta a la hora de dimensionar tanto el tamaño de una oficina, las conexiones web, etc.

Para Rafael Cubero, una de las lecciones aprendidas de la explosión del teletrabajo es que el trabajo a distancia se va a quedar y "se ha convertido en un factor más de la propuesta de valor que todas las empresas ofrecen a sus empleados y que va a reforzar el sentimiento de pertenencia a las empresas que apuestan por ello". En cuanto a los planes de futuro en Tecnatom Group, estos pasan por establecer las reglas del trabajo a distancia, así como finalizar "un modelo conexión digital que favorezca la conciliación, pero con cuidado de que no se inmiscuya demasiado en nuestra vida personal". Apuntó también Rafael Cubero que se trabaja en la formación de todas herramien tas colaborativas, la reorganización de espacios en sede para crear unos espacios más amplios y más colaborativos o una mayor inversión en TI. ■


Rafael Cubero, Tecnatom Group

"El teletrabajo se ha convertido en un factor más de la propuesta de valor de las empresas"

RAFAEL CUBERO SAIZ, HEAD OF PEOPLE, TECNATOM GROUP

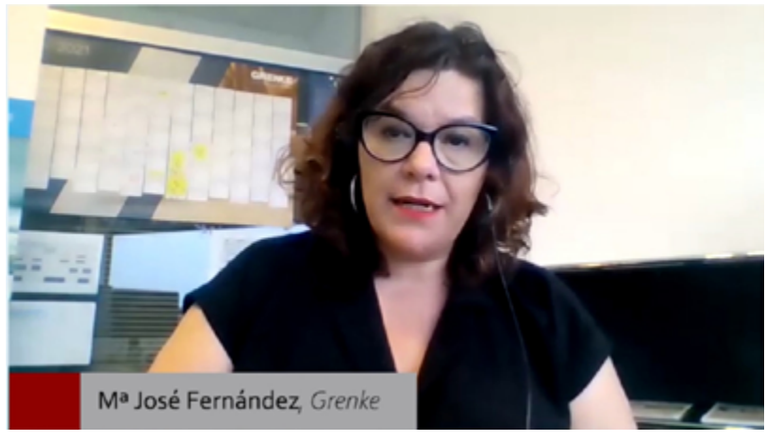
#ENCUENTROSITTRENDS

Cómo mejorar la experiencia del trabajador remoto gracias a la tecnología

Más de la mitad de los trabajadores apoya el teletrabajo. Es más, según una encuesta de la compañía de consultoría de gestión Korn Ferry, un 64% reconoce ser más productivo trabajando desde casa, además de valorar otros aspectos como el ahorro de tiempo en los desplazamientos y una mejor conciliación familiar y laboral.

Trabajar en remoto también ha impuesto otra dinámica en las reuniones, ahora online y virtuales, necesarias para mantener la marcha de las empresas y los vínculos con la misma, todos ellos temas tratados en el #EncuentroITTrends Mejorando la experiencia del trabajador remoto, en el que participaron Melchor Sanz, Direc-

Melchor Sanz (HP Inc.); Iván Rodríguez Santos (Citrix); Mª José Fernández (Granke); Agustín Sánchez Fonseca (NFON); Sergio Martínez (SonicWall); Iván Mateos Pascual (Sophos); y Guillermo Fernández (WatchGuard), durante el debate.



“Las pymes han recibido ayudas para hacer frente a esta digitalización y al teletrabajo”

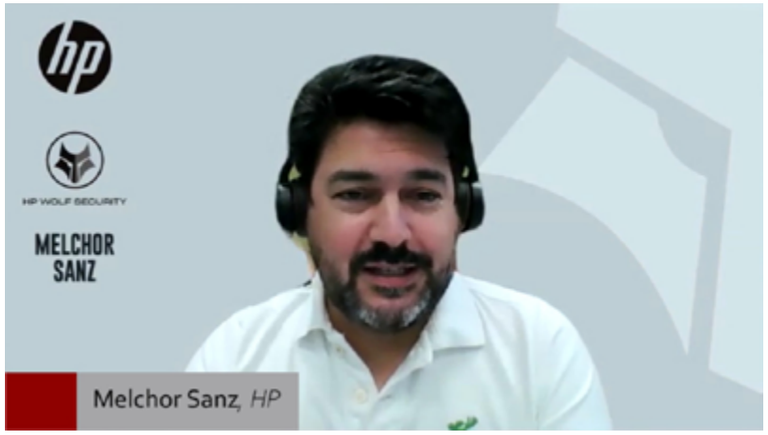
Mª JOSÉ FERNÁNDEZ, BRANCH MANAGER, GRENKE

tor de Tecnología y Preventa de HP Inc.; Iván Rodriguez Santos, Lead Sales Engineer de Citrix Iberia; Mª José Fernández, Branch Manager de Grenke; Agustín Sánchez Fonseca, Responsable de desarrollo de negocio de NFON Iberia; Sergio Martínez, Iberia Regional Manager de SonicWall; Iván Mateos Pascual, Sales Engineer de Sophos; y Guillermo Fernández, Iberia Sales Engineer Manager de WatchGuard.

Lo primero que quedó claro durante el segundo encuentro de este evento online es que los empleados no estábamos preparados para teletrabajar. Lo aseguraba Melchor Sanz, Director de Tecnología y Preventa de HP Inc., afirmando que “estábamos preparados para teletrabajar un ratito, pero no ocho o nueve horas”. Mencionó el directivo que es la tecnología la que puede ayudar a que las empresas sean más eficientes y que los trabajadores estén trabajando de una manera más confortable desde cualquier ubicación, y que todo ello se haga sin que existan mayores riesgos de seguridad.

Más de un año después de la pandemia, cuando damos por hecho que el puesto de trabajo ya va a ser híbrido, ¿cómo será el puesto de trabajo del futuro? Para Iván Rodríguez Santos, Lead Sales Engineer de Citrix Iberia, la clave está en aplicaciones que sean capaces de conectar usuarios y datos a través de cualquier tipo de dispositivo y a través de cualquier ubicación. El éxito, asegura, llega “cuando somos capaces de brindar esta experiencia de usuario de forma consistente”.

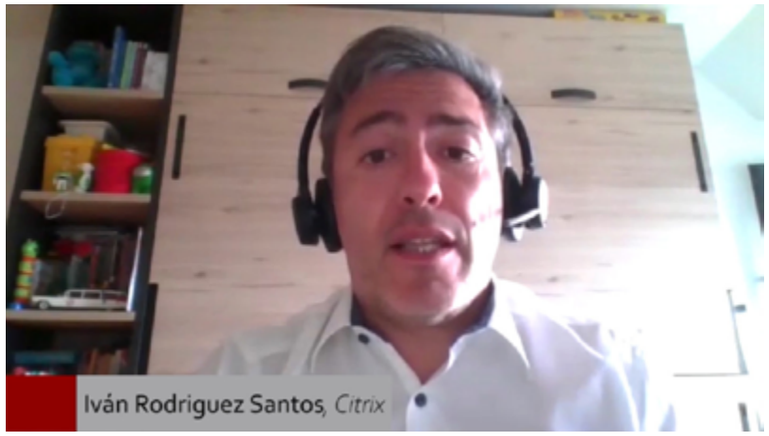
Hablar de teletrabajo es hablar de digitalización, un proceso que, según Mª José Fernández, Branch Manager de Grenke, ya estaba en ciernes cuando llegó la pandemia. La crisis sanitaria llevó a las empresas a acelerar sus planes hasta el punto de que en estos meses se ha avanzado lo que se hubieran tardado diez años.



“No vale cualquier dispositivo para acceder a cualquier entorno”

MELCHOR SANZ, DIRECTOR DE TECNOLOGÍA Y PREVENTA, HP INC.

En lo que respecta a las herramientas de comunicación, que en realidad existen desde hace mucho tiempo, planteó Agustín Sánchez Fonseca, responsable de desarrollo de negocio de NFON Iberia, que no se les está sacando el máximo provecho por una cuestión cultural y por una falta de proceso a nivel de empresas; “al trabajador se le dan unas herramientas, pero hay que dotarles de objetivos y de procesos”. Aseguró también que, si antes se estaban infrautilizando, se ha pasado al extremo contrario y se utiliza



“La clave está en aplicaciones capaces de conectar usuarios y datos a través de cualquier tipo de dispositivo y ubicación”

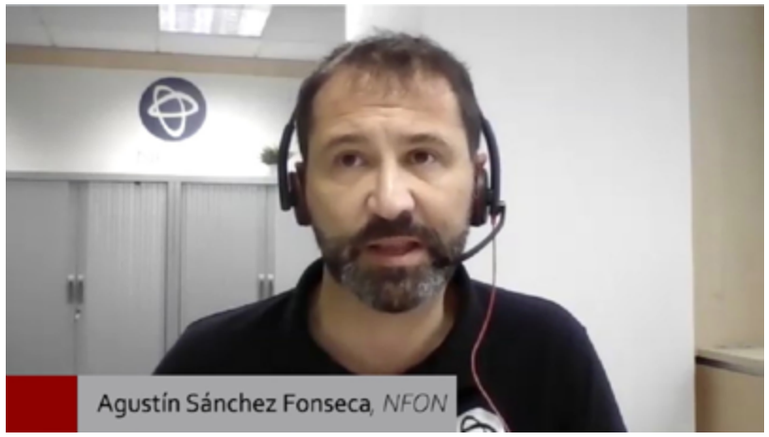
IVÁN RODRIGUEZ SANTOS, LEAD SALES ENGINEER, CITRIX IBERIA

la videoconferencia para todo o el móvil demasiado cuando “no vale para un uso corporativo, ya que ni permite asegurar o dar la máxima calidad de atención, ni asegura la máxima disponibilidad”.

La digitalización acelerada y la falta de preparación para el teletrabajo han tenido un impacto en la seguridad de las empresas. El teletrabajo, explicó Sergio Martínez, director general de SonicWall Iberia, implica que accedemos a aplicaciones corporativas y a datos desde cualquier sitio, que el perímetro de seguridad ha desaparecido y que la superficie de exposición se ha incrementado. Ahora, aseguró el directivo “se hace necesaria una nueva seguridad”, que debe tener en cuenta cinco ideas sencillas: defensa por capas, visibilidad, ser capaces de detectar lo desconocido, realizar un acceso remoto seguro, y todo ello con un TCO y un coste disruptivo.

Desde Sophos Iberia, Iván Mateos, sales engineer de la compañía, apuntó que para que una solución funcione, para que algo se adapte y se pueda utilizar, tiene que ser fácil, tiene que ser “descomplicado”: “los usuarios tienen que poder trabajar desde casa como lo hacían desde la oficina y sin cargarles de responsabilidad”. Aseguró que muchas veces se tiende a echarle la culpa al usuario de lo que pasa y que, si bien el usuario tiene que saber hacer muchas cosas, hay otras muchas que no tiene por qué saber. “La solución es que no se tenga que preocupar por nada gracias a un ecosistema de ciberseguridad donde todo hable con todo y sea sencillo de administrar”.

¿Cómo podemos facilitarle la vida al empleado con un equilibrio entre la seguridad y su experiencia? Tiene claro Guillermo Fernández, Iberia Sales Engineer Manager de WatchGuard, que hay que encontrar la manera de ayudarles con herramientas que automaticen la parte de toda la problemática de seguridad sin abrumarles a alertas y a decisiones. Puso como ejemplo de equilibrio lo relativo a la gestión de contraseñas, que aseguró “sigue siendo un mal endémico que arrastramos de desde hace muchos años”.



“El principal inconveniente para no disfrutar de esta democratización de la tecnología es la cultura y el inmovilismo”

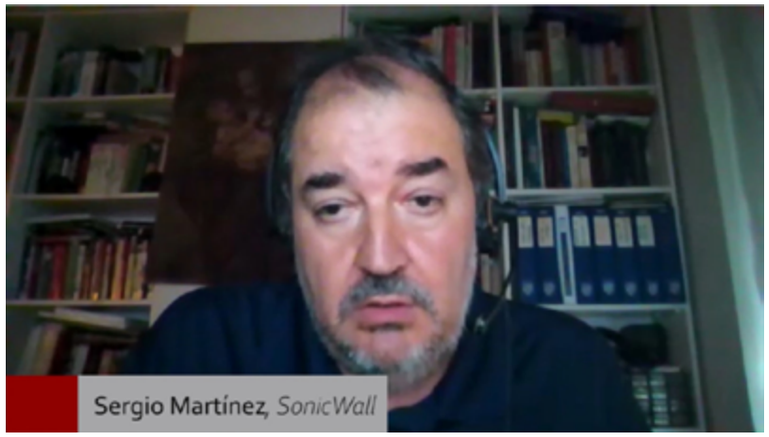
AGUSTÍN SÁNCHEZ FONSECA, RESPONSABLE DE DESARROLLO DE NEGOCIO, NFON IBERIA

Para Melchor Sanz, mejorar la experiencia del trabajador remoto pasa por “descomplicar”, y eso significa no sólo simplificar el acceso a la información, a una aplicación o a la red, sino hacerle la vida más fácil al empleado desde que pulsa el botón de su dispositivo. Añadió que “no vale cualquier dispositivo para acceder a cualquier entorno” y propuso una gestión moderna de los dispositivos que va desde la capa más física de seguridad a la capa de sistema operativo o la capa de aislamiento.

Asegurando que el trabajo remoto es sólo un marketing porque “al fin y al cabo todos los usuarios deberían trabajar allí donde estén”, mencionó Iván Rodríguez los servicios Workspace que permiten que el usuario acceda desde un único punto, allí donde esté, homogeneizando el acceso e incrementando la seguridad.

Lo habitual cuando se piensa en teletrabajo es asociarlo a grandes empresas, a multinacionales con empleados repartidos por todo el mundo. ¿Qué ocurre en el mundo pyme? Dijo Mª José Fernández que son las grandes compañías las que tienen más medios, y que las pymes se están digitalizando mucho más. Explicó que han recibido ayudas para hacer frente a esta digitalización a través de fondos ICO, ayudas que han llegado de Europa y propuestas como la de Grenke, que “permitimos que las empresas y las pymes puedan obtener todo el equipamiento de hardware, software, conexiones a Internet… y en general todo lo que necesiten para poder realizar el teletrabajo, agilizando todos los procesos y que los trabajadores estén cómodos y tranquilos”.

En este proceso de teletrabajo, ¿se ha conseguido unificar la experiencia del puesto de trabajo en la oficina y en casa? Dijo Agustín Sánchez Fonseca que el acceso a los datos desde la oficina ya estaba muy disgregado y que al irnos a casa no sólo ha generado un reto en cuanto a unificar la experiencia en casa y en la oficina como un único modelo de uso, “sino que tienes gente con perfiles diferentes, tienes millenials y tienes gente que se niega a dejar de usar el teléfono de sobremesa”. Explica que existe la oportunidad de unificar todas las comunicaciones en el menor número posible de dispositivos, y aun así po-



“Roto el perímetro, la única solución es poner diferentes medidas de seguridad”

SERGIO MARTÍNEZ, IBERIA REGIONAL MANAGER, SONICWALL

der tener esta herramienta en todos los dispositivos posibles, que es la manera de dar flexibilidad.

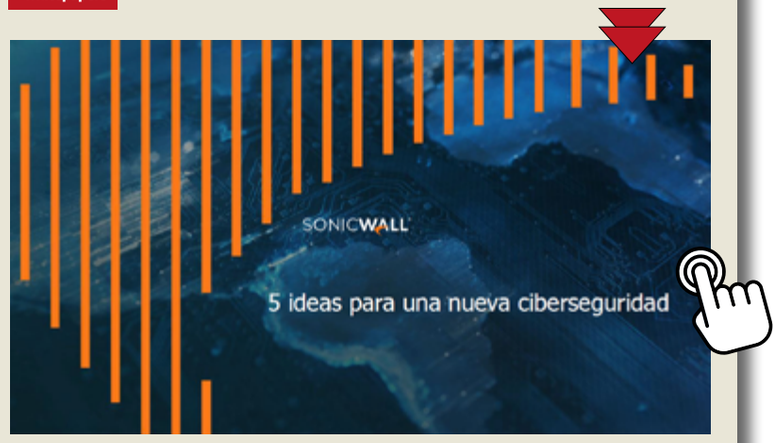
Roto el perímetro, “la única solución es poner diferentes medidas de seguridad”, dijo Sergio Martínez, añadiendo que la verdadera pandemia “es el robo de identidades para realizar luego ataques y movimientos laterales en las compañías”. Aseguró que los intentos de intrusión se dispararon gracias al robo de identidades y que el ransomware sigue siendo un grave problema. “Está muy claro que debemos desplegar más medidas de autenticación, que muchas aplicaciones se han migrado a la nube para facilitar su acceso desde fuera, que los ciberataques son más sofisticados… y que está claro que hay que aplicar y poner en marcha una nueva ciberseguridad basada en capas de extremo a extremo y de este a oeste”.

Para Iván Mateos hay un reto que tenemos que aplicar tanto al mundo de la ciberseguridad como a nuestra vida cotidiana: primero pensar y luego actuar; “si conseguimos hacer eso evitamos trabajar dos veces; evitamos que cada vez que se plantea un nuevo problema tengamos que analizar todo otra vez, revisar todas las soluciones del mercado y además seguir aumentando la complejidad de nuestro Frankestein”. Mencionó la propuesta de un ecosistema de ciberseguridad adaptativo con el que “conseguimos simplificar mucho la ecuación y tener además un nivel de seguridad superior”.

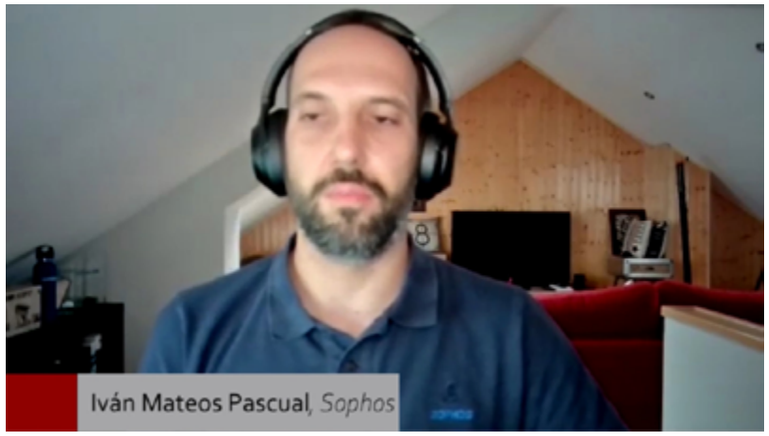
El phishing ha sido uno de los caballos de batalla durante dos meses de la pandemia. En opinión de Guillermo Fernández, este incremento vino derivado “de tener a los empleados trabajando desde casa” y ha puesto de manifiesto la necesidad de llevar la protección que antes estaba en el perímetro a ese puesto de trabajo. “El empleado es la primera barrera de seguridad y los cursos de concienciación son importantes”, aseguró el directivo pare reducir su impacto.

Si la primera barrera de seguridad es el usuario, la segunda es el dispositivo y la tercera el sistema operativo, y le siguen las aplicaciones y las comunicaciones, explicó Melchor Sanz. Dijo el Director de Tecnología y Preventa de HP Inc. que se tiene que garan-

CINCO IDEAS PARA UNA NUEVA CIBERSEGURIDAD



Un año después de la pandemia, cuando el perímetro de seguridad se ha perdido irremediablemente y las ciberamenazas son cada vez más y más sofisticadas se hace necesaria una nueva seguridad, que debe tener en cuenta cinco ideas sencillas: Defensa por capas, visibilidad, ser capaces de detectar lo desconocido, realizar un acceso remoto seguro, y todo ello con un TCO y un coste disruptivo.



“Los empleados tienen que poder trabajar desde casa como lo hacían desde la oficina y sin cargarles de responsabilidad”

IVÁN MATEOS PASCUAL, SALES ENGINEER, SOPHOS

tizar que cada una de esas capas sea segura por sí misma desde el diseño, pero que entre ellas se hablen para tener un sistema de control homogéneo.

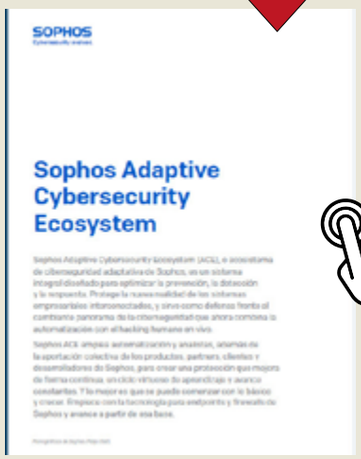
Los más rápido y fácil para los clientes que ya estuvieran utilizando sistemas y VPN antes de la pandemia fue ampliarlos “sin pararse a pensar”, apuntó Iván Rodríguez añadiendo que las VPN suelen ser complicadas de gestionar y que existen otras opciones, como el acceso remoto al PC de Citrix, que permite “acceder a mi escritorio con las mismas aplicaciones, mismo interfaz, mismo look&feel y con el protocolo nativo de Citrix para poder acceder a sus aplicaciones de la manera más segura y trabajar como en la oficina”.

Este nuevo modelo de trabajo en el que nos hemos visto inmersos por una parte nos ha alejado de los compañeros a los que veíamos prácticamente todos los días, pero también nos ha acercado, gracias a esas múltiples videoconferencias, a gente con la que antes no teníamos apenas relación. ¿Cómo han impactado esas dos tendencias en el trabajador remoto? “Al principio fue un shock”, aseguró Mª José Fernández, añadiendo que ahora se ha instaurado un modelo híbrido en el que “vamos sumando las relaciones personales y las relaciones digitales que ahora ya son cercanas a mí”.

La tecnología se ha democratizado. Por un lado, la pyme tiene acceso a herramientas tecnológicas para igualarse en muchos aspectos a grandes empresas, y también las grandes empresas tienen acceso a herramientas más ligeras o menos costosas y más sencillas de utilizar. Para Agustín Sánchez Fonseca, “el principal inconveniente para no disfrutar de estas ventajas y de esta democratización de la tecnología es la cultura, el inmovilismo y cierta resistencia por parte de algunos fabricantes y operadores con modelos perversos que retienen, por lo menos en el ámbito de las comunicaciones, a las pymes y a las no tan pymes”.

Siguiendo con el concepto “descomplicar”, dijo Sergio Martínez que modelos como Zero Trust, que se han visto reforzados por la pandemia “lo que intentan es utilizar tecnologías que lo hagan más fácil, pero sin fiarse ni confiar en nadie, ni siquiera en los accesos pri-

SOPHOS ADAPTIVE CYBERSECURITY ECOSYSTEM



Sophos Adaptive Cybersecurity Ecosystem (ACE), o ecosistema de ciberseguridad adaptativa de Sophos, es un sistema integral diseñado para optimizar la prevención, la detección y la respuesta. Protege la nueva realidad de los sistemas empresariales interconectados, y sirve como defensa frente al cambiante panorama de la ciberseguridad que ahora combina la automatización con el hacking humano en vivo.

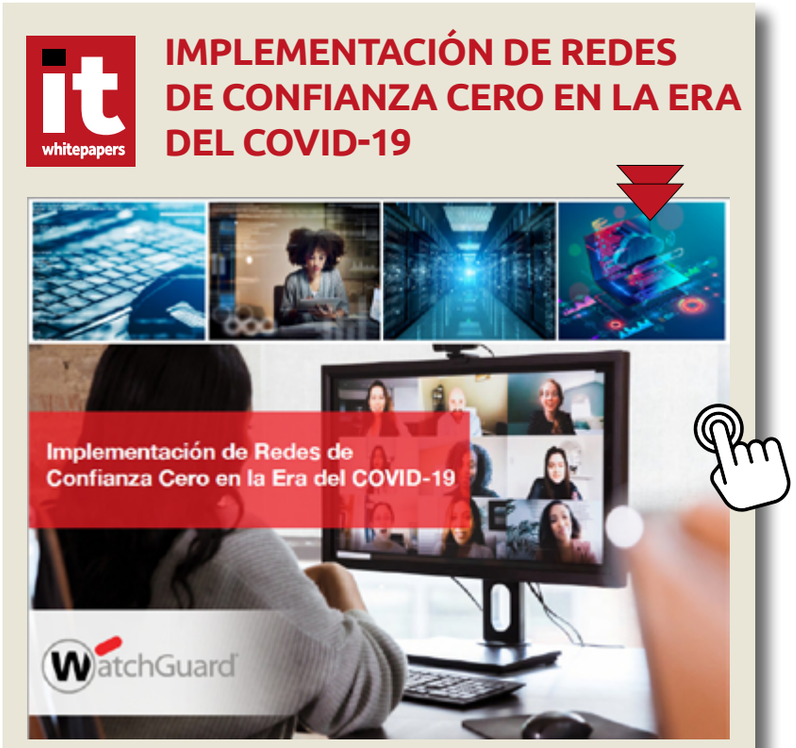
“Esperar que sea el empleado quien de forma proactiva y continuamente esté actualizando todo el software no es realista”

GUILLERMO FERNÁNDEZ, IBERIA SALES ENGINEER MANAGER, WATCHGUARD

vilegiados con los que hay que tener mucho cuidado”. Aseguró además que el futuro de la seguridad de la red está en el cloud, que la nube pública crecerá esta año un 35% y que las VPN serán sustituidas por tecnologías Zero Trust en casi un 60%.

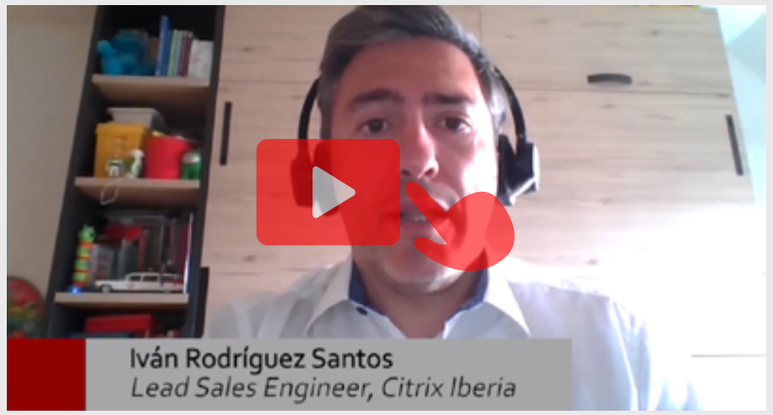
“El trabajador remoto ha sufrido muchas amenazas y ha sido punto de mira durante este último año por ese aislamiento, y eso ha supuesto no solo un aumento del phishing, sino llamadas de falsos servicios técnicos o casos de ransomware que se han propagado desde la VPN a toda la red en más de una empresa”, puntualizó Iván Mateos. La solución, para el experto de Sophos, es contar con un ecosistema de seguridad que incluso disponga de un servicio de gestión de amenazas para que, si todo falla, si consiguen entrar, se pueda actuar en minutos.

Por último, preguntamos a Guillermo Fernández cómo cree que deben gestionarse las vulnerabilidades de los sistemas operativos y aplicaciones de terceros ahora que ni los empleados ni sus equipos están en la oficina. Empezó recordando que en un 80% de los ataques se están explotando vulnerabilidades que ya han ido corregidas previamente y que su experiencia es que los clientes “no son conscientes de cómo está la situación de todo su parque, y más en este entorno tan distribuido como tenemos ahora”. Esperar que sea el empleado quien de forma proactiva y continuamente esté actualizando todo el software no es realista, concluyó este experto, proponiendo que haya una capa por encima que lo automatice, que sea muy sencillo, que los empleados no tengan que hacer nada y que para el administrador no suponga una sobrecarga. ■



La respuesta al coronavirus no tiene precedentes y este experimento del “trabajo desde casa” lleva a muchas empresas a un territorio decididamente desconocido. Con la mayor parte de los usuarios finales trabajando ahora de forma remota, los enfoques de seguridad de confianza cero pueden ayudar a mantener la continuidad y la seguridad.

Mejorando la experiencia del trabajador remoto: propuestas tecnológicas

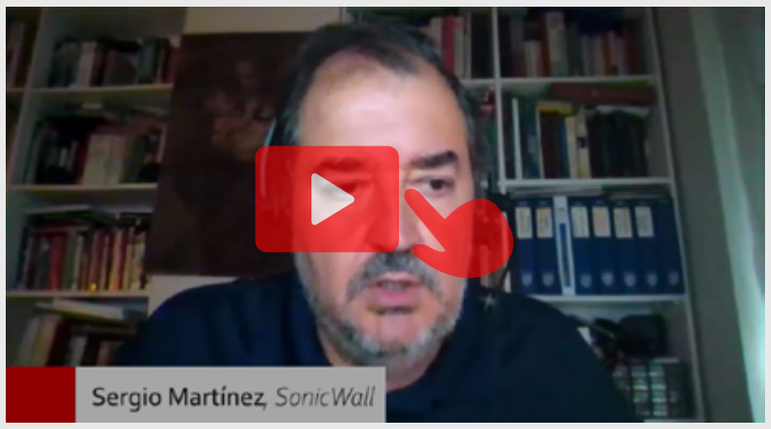


“Lo importante es poder dar la misma experiencia al usuario esté donde esté” (Citrix)

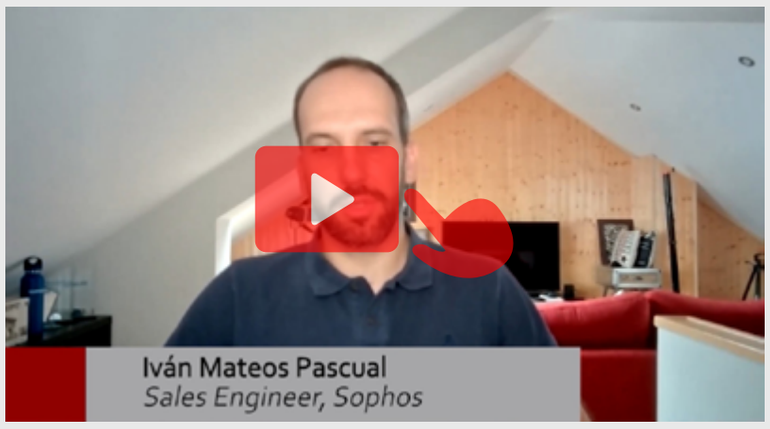
“La cultura de la empresa y del empleado son claves en el nuevo modelo de trabajo remoto” (Grenke)

“Para el trabajo híbrido no vale cualquier dispositivo” (HP Inc.)

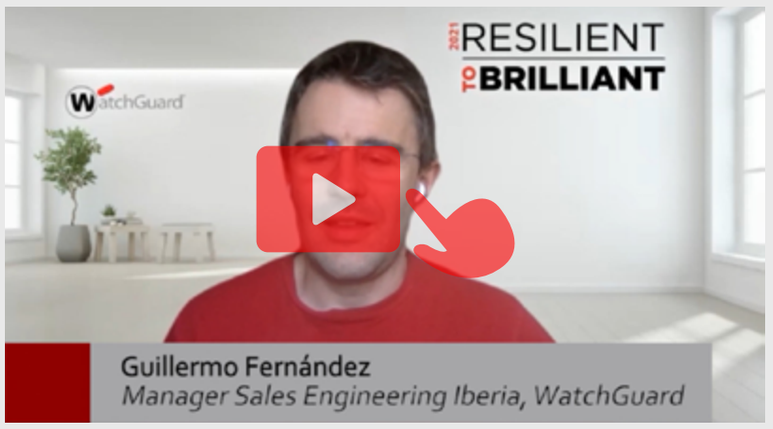
“La oferta de centralita y contact center básico de NFON cubre las necesidades del teletrabajo” (NFON)



“Cinco ideas para una nueva ciberseguridad” (SonicWall)



“Hay que dejar de pensar en soluciones Frankestein para empezar a hablar de ecosistemas” (Sophos)



“El teletrabajo nos hace más frágiles a los ataques de phishing” (WatchGuard)