TECH FORUM 2021

CYBER SECURITY WORLD MADRID

SITUACIÓN Y PERSPPECTIVA DEL SECTOR DE LA CIBERSEGURIDAD EN ESPAÑA

1- INTRODUCCIÓN TECH FORUM: CYBER SECURITY WORLD MADRID

Vivimos en un mundo en el que millones de dispositivos están interconectados, en los que los datos, tanto públicos como privados, son objeto de un posible ciberataque. Un riesgo que, a raíz de la pandemia del coronavirus, se ha expuesto a unos niveles sin precedente. La seguridad digital es ahora, más que nunca, una prioridad.

El sector de la ciberseguridad moverá este año en España un volumen de negocio cercano a los 1.320 millones de euros, lo que supone un 8,1% más que en 2020, según un estudio de IDC.

En el mes de junio de 2021 se realizó una encuesta a profesionales del sector para conocer de primera mano los retos actuales en materia de ciberseguridad corporativa, los planes que se han puesto en marcha en el último año como consecuencia del COVID-19 y las tendencias más inminentes del mercado. Al finalizar la encuesta, los participantes se reunieron en el *Tech Forum de Cyber Security World Madrid* para debatir sobre los resultados y sacar conclusiones.

El objetivo de este white paper es recoger y analizar las conclusiones del forum para poder plasmar la situación real de la ciberseguridad corporativa en España y descubrir las inquietudes de los directivos y empresarios del sector.

2- PROPÓSITO DEL TECH FORUM

Durante la pandemia del COVID-19 se ha podido comprobar la criticidad de las infraestructuras digitales en materia de ciberseguridad. La incertidumbre derivada del coronavirus y el incremento, sin precedentes, del teletrabajo ha supuesto un reto para todo tipo de empresas, principalmente entre las pymes, a las que se dirigen más del 70% de los ciberataques. Por ello, las compañías, sin importar tamaño ni core business, apuestan cada vez más por proteger los sistemas más vulnerables.

El reto de hacer de la ciberseguridad una piedra angular en la estrategia de toda empresa es acuciante y por ello, es imprescindible crear espacios de debate que funcionen como punto de encuentro entre las diferentes empresas del sector y ayuden a definir los desafíos actuales en materia de ciberseguridad corporativa.

El *Tech Forum de Cyber Security World Madrid,* co-presentado junto a representación de Women4Cyber Spain*,* ha sido la antesala a Cyber Security World Madrid, un evento omnicanal para directivos y expertos en el que se abordarán diferentes cuestiones relacionadas con la ciberseguridad corporativa desde una óptica profesional con casos de éxito y estudios. La cita será los días 27 y 28 de octubre en IFEMA, y contará con espacios destinado a expositores, networking y auditorios en los que se ofrecerán conferencias de numerosos líderes del mercado.

3- LA MUESTRA

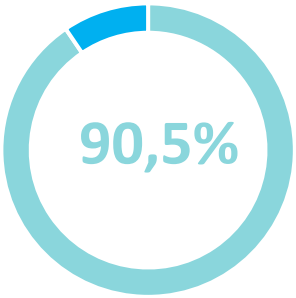
Este estudio se ha realizado con profesionales de ciberseguridad corporativa en España de dos perfiles diferenciados. Un primer grupo compuesto por representantes de empresas que son usuarias de soluciones de ciberseguridad y un segundo grupo, compuesto por profesionales

pertenecientes a las compañías proveedoras de servicios y tecnología de ciberseguridad. Los participantes tanto a través de la encuesta como en el foro presencial han sido:

- Director Comercial en Aruba
- Country Manager Spain & Portugal en Check Point Software Technologies
- Regional Director en Crowdstrike
- EMEA Account Manager en Darktrace
- Country Manager Digital en Entrust
- Cyber Security Business en Evolutio
- Director Comercial en Guardicore
- CISO en Indra
- Director Comercial en Netskope
- Regional Sales director en SentinelOne
- Director Comercial en SonicWall
- Director South EMEA en Sophos
- Country Manager Iberia en WatchGuard
- CISO en AXA
- Miembro de la junta directiva de Women4Cyber Spain
- Presidenta de Women4Cyber Spain
- Director General de Innovación y Emprendimiento en el Ayuntamiento de Madrid
- Responsable TIC Empresas en la Cámara de Comercio-TIC Negocios
- Managing Director en Céfiros
- Responsable global de gestión de amenazas en Iberdrola
- Global CISO en Iberdrola
- Jefe del servicio de análisis de la ciberseguridad y la cibercriminalidad en Oficina de Coordinación Cibernética. Ministerio del Interior
- CISO en Sanitas
- CISO en Santillana
- CISO en Globalia
- Director General de la Oficina Digital en el Ayuntamiento de Madrid

4- CONCLUSIONES GENERALES

4.1 Consecuencias de la pandemia en el sector de la ciberseguridad corporativa



Más del 90% de los encuestados ha respondido que la crisis sanitaria ha acelerado los planes de ciberseguridad corporativa propia o la de sus clientes.

Además, los participantes han comentado que a raíz de la pandemia se ha producido un efecto contradictorio. Para muchas empresas la pandemia ha supuesto un parón general de la actividad y por ende un parón de las medidas de ciberseguridad. Para otras, la obligación de trasladar a los trabajadores a sus casas y continuar produciendo las ha llevado a poner en marcha estrategias de ciberseguridad de forma rápida, tomando riesgos que en otras situaciones hubieran sido impensables, pero pudiendo avanzar mucho en muy poco tiempo.

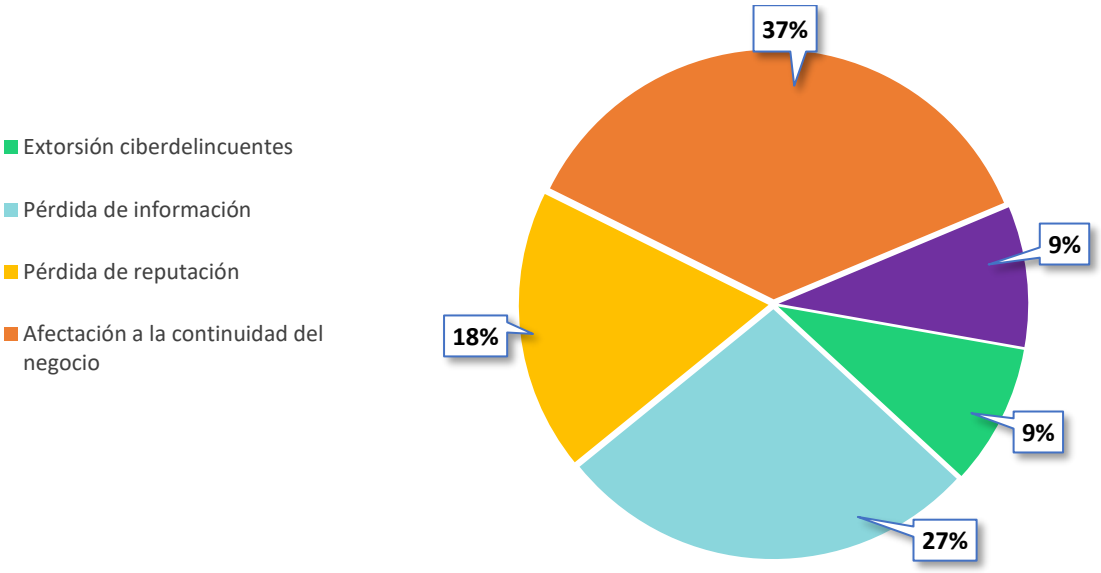
"Para nosotros la pandemia ha sido un tractor bastante fuerte porque hay clientes que han parado su producción, pero otros han cambiado su manera de trabajar teniendo que llevar a todos sus emplados a trabajar en sus casas y no había casi nadie preparado para esos volúmenes de empleados trabajando desde casa."

"Mi opinión es que el que haya improvisado ha fallado. Lo que nos ha permitido esta pandemia es poner en valor lo que teníamos previamente."

Queda claro que de una forma u otra la pandemia ha puesto en valor la necesidad de implementar medidas de ciberseguridad efectivas. Entre las estrategias más implementadas en los últimos meses, los encuestados mencionan: la importancia del perímetro deslocalizado, el avance en el modelo Zero Trust, la formación, la concienciación y el cloud proxy.

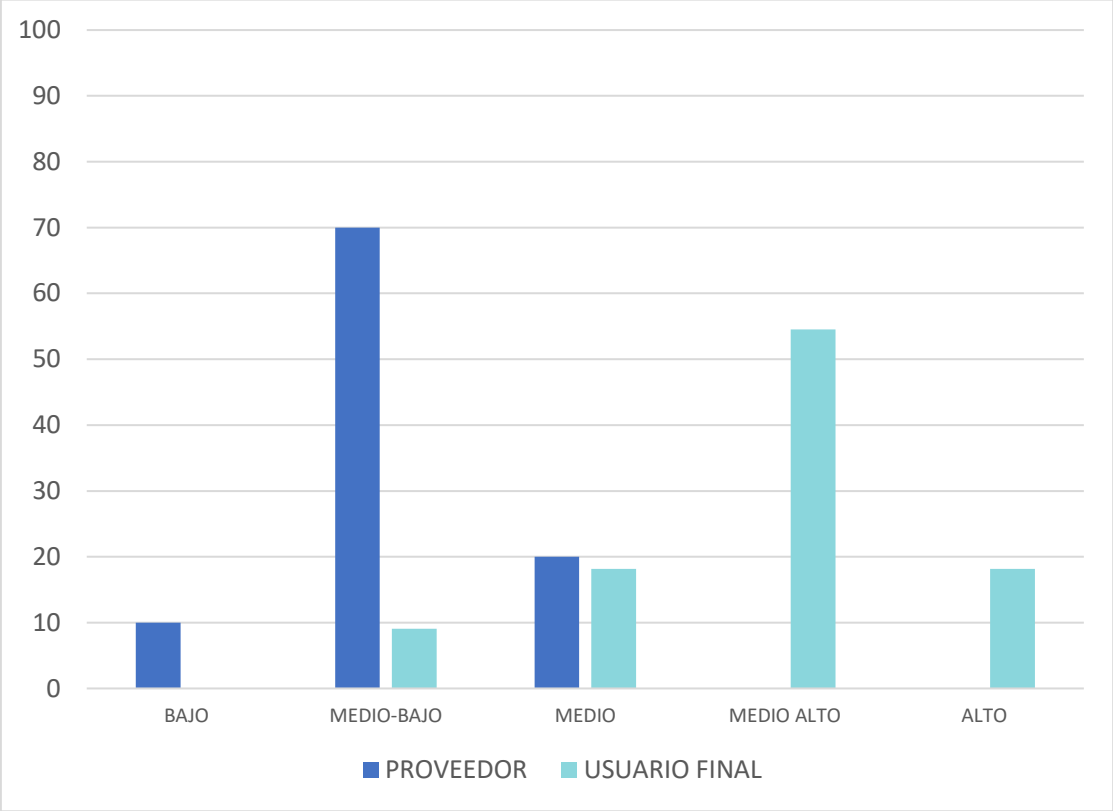
4.2 Ciberataques y nivel de protección de los equipos remotos

Sin lugar a duda, las cuestiones que más preocupan a los directivos de cara a un ciberataque corporativo son la afectación a la continuidad del negocio y la pérdida de información.



Según han comentado, el *driver* para aumentar la inversión en seguridad es el miedo al incidente que les haga perder información o les obligue a parar el negocio. Al tomar conciencia de que esto es una posibilidad, la inversión en seguridad aumenta y la protección de los equipos también.

Respecto a este último tema, es significativa la diferencia de criterios que existe entre los profesionales del sector en relación con la percepción que tienen del nivel protección de los equipos remotos de las empresas españolas.

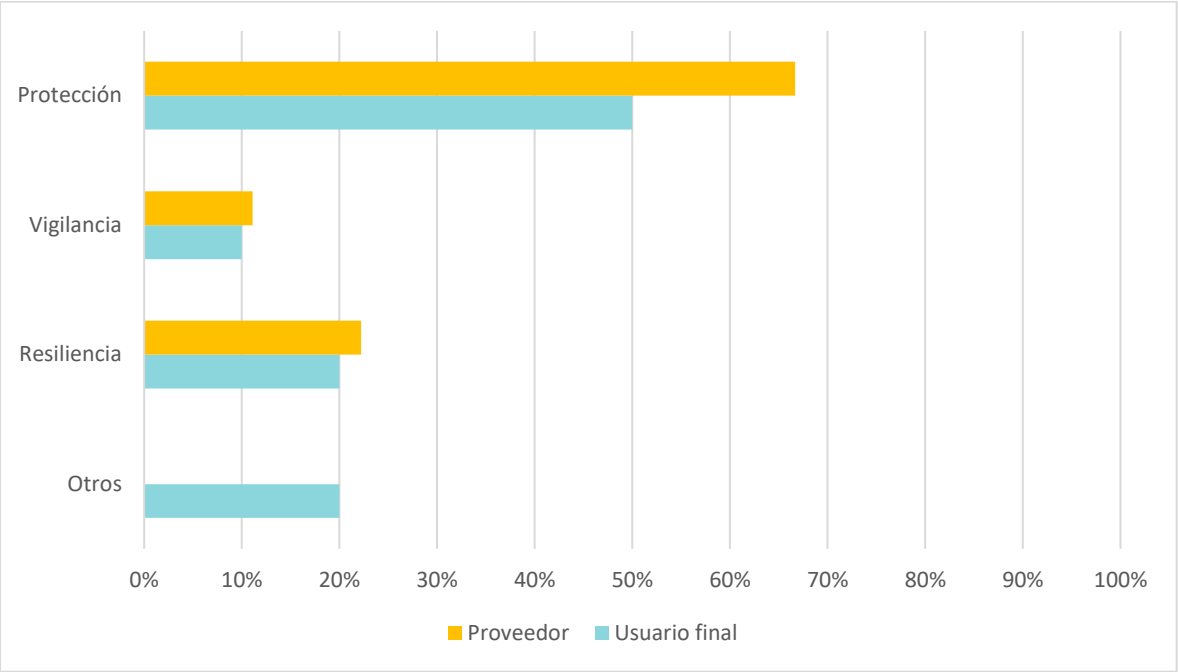


"La brecha entre la percepción que tenemos de cómo de seguro estamos a cómo realmente estamos ha existido toda la vida. Empezamos a hablar ahora de que el perímetro se ha extendido, porque todo el mundo es muy conciente de lo que estamos viviendo pero no hay nada nuevo. Seguimos evolucionando y la seguridad sigue evolucionando, el problema que seguimos teniendo es que las empresas no consideran que el tema de la seguridad sea un tema prioritario hasta que no se demuestra lo contrario y un día no pueden abrir la fábrica."

Durante el debate han señalado que la percepción de las empresas puede deberse a que los presupuestos destinados a la ciberseguridad han aumentado de forma muy significativa en los últimos años.

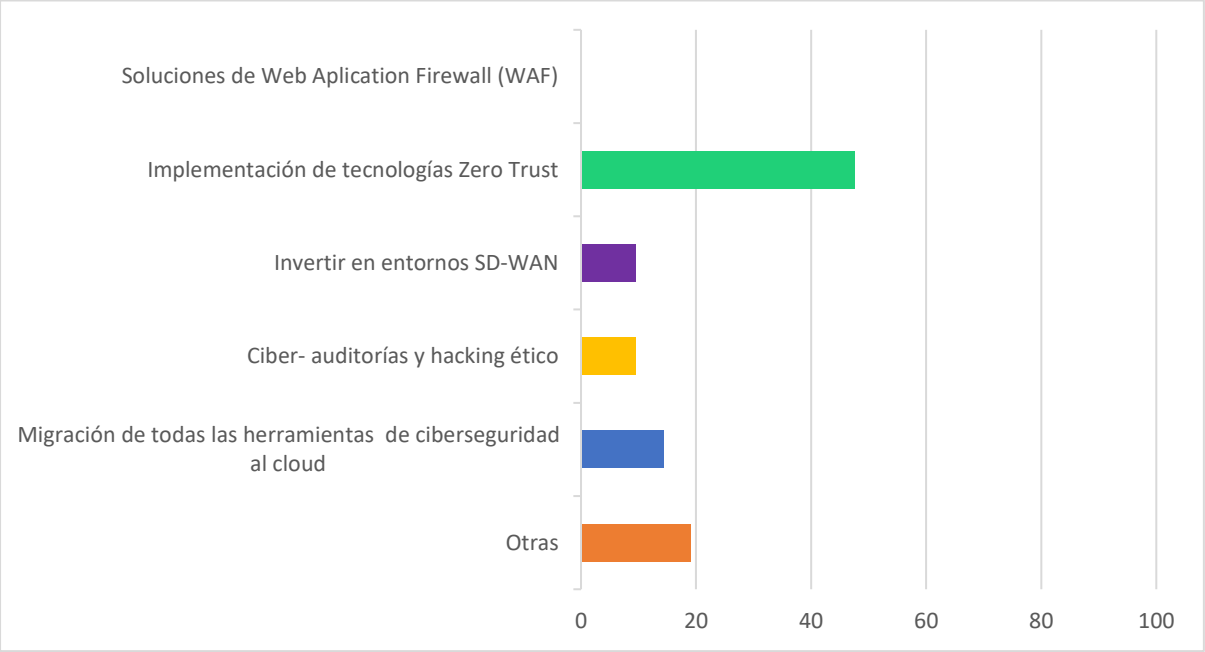
4.3 Cibercultura en las empresas

Los aspectos de ciberseguridad en los que más se invierte hoy en día son: en primer lugar, la protección, en segundo la resiliencia y en tercero la vigilancia.



"El problema con las estrategias reactivas es que en muchos casos provocan que las empresas vayan por detrás de las amenazas, quedando expuestas a pérdidas económicas, reputacionales o de oportunidades de negocio."

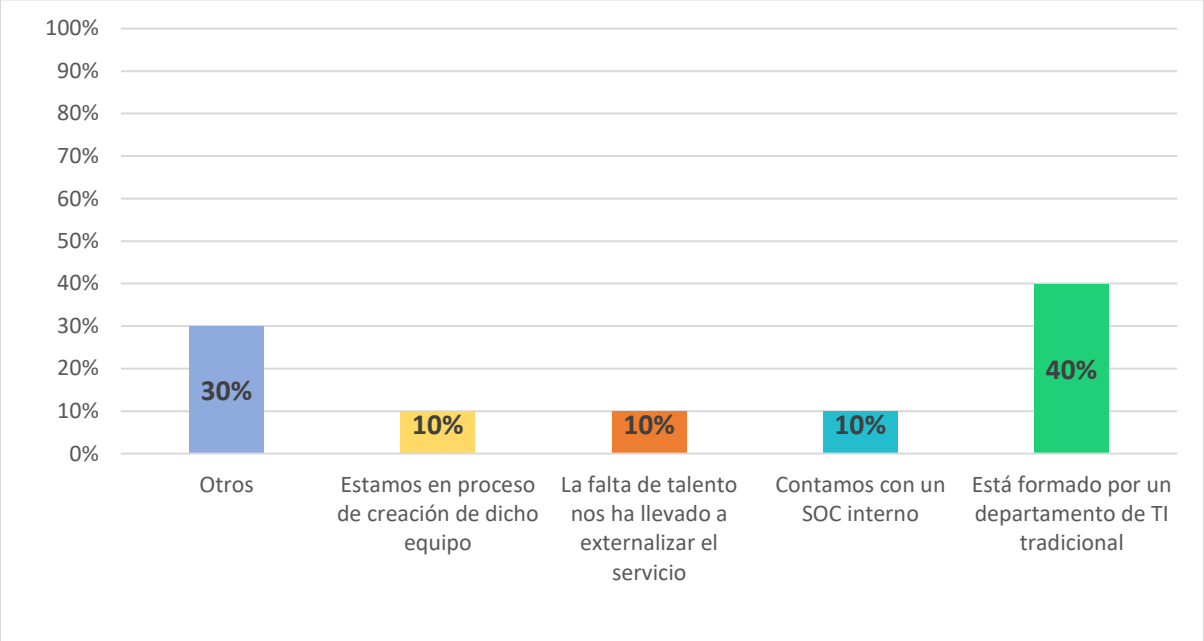
Respecto a las estrategias de ciberseguridad que creen que destacarán a partir de ahora, el 48% de los encuestados opina que la implementación de tecnologías Zero Trust será la opción favorita.



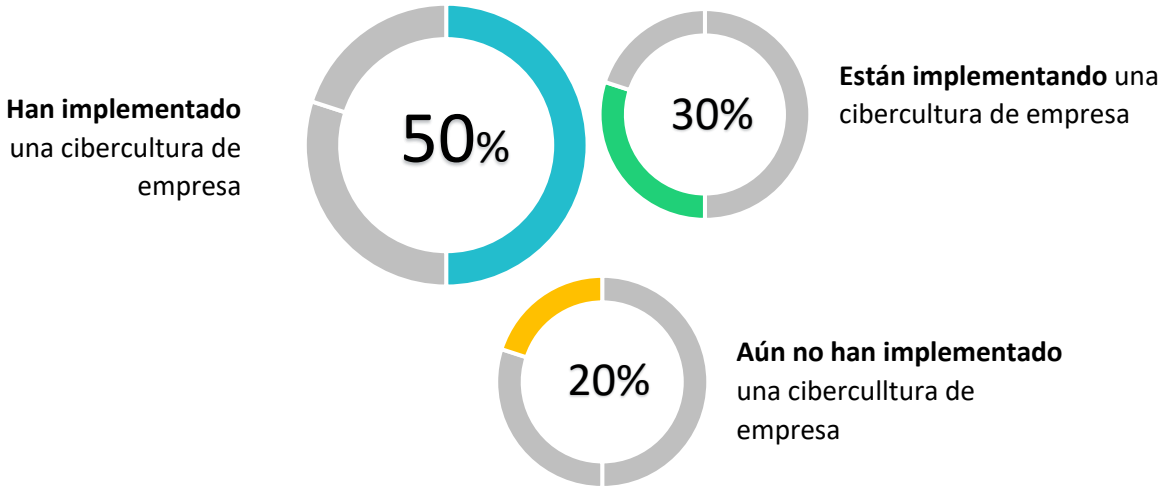
Sin embargo, con el resto de las tecnologías el posicionamiento no está claro, ya que las empresas proveedoras consideran que la migración de todas las herramientas de ciberseguridad al cloud será la segunda una estrategia prioritaria mientras que las empresas usuarias finales apuestan por las inversiones en entornos SD-WAN, las ciber auditorías y el hacking ético.

4.4 Cibercultura en las empresas

Según ha indicado casi la mitad de los encuestados, la mayoría de los equipos corporativos centrados en la ciberseguridad están formados por departamentos de TI tradicional.



No obstante, algunas empresas han compartido otro tipo de sistemas de organización más avanzados formados por diferentes líneas de defensa. En estos casos, los especialistas de ciberseguridad se integran en las diferentes áreas de negocio pudiendo trabajar la estrategia de forma integrada con el modelo de negocio de la empresa. Ejemplos que cada vez serán más habituales ya que si bien solo un 50% de los directivos asegura haber implementado una cibercultura de empresa, hay otro 30 % que asegura que están en proceso de implementarla.



"Es fundamental que haya responsables de ciberseguridad integrados en todos los puntos de toma de decisión de la empresa, figuras independientes pero integradas dentro de los equipos."

Por último, se ha debatido sobre las temáticas que más preocupan al sector de cara al futuro. Los temas principales fueron:

La captación y retención del talento fue la cuestión más repetida por los profesionales durante el debate, que han asegurado que la rotación dentro del sector es muy alta y que resulta muy difícil retener el talento. En esta línea surgen dos posturas enfrentadas:

- Una que defiende que la creación de programas de talento es una inversión interesante para las empresas porque el ROI siempre es positivo.
- Otra que defiende que este tipo de programas suponen un gasto para la compañía que no llegará a rentabilizar.