Educación e innovación.

Tendencias tecnológicas para los nuevos retos

Patrocinadores:

Alcatel·Lucent Enterprise

ESET

Global Knowledge™ a skillsoft company

SOPHOS Cybersecurity evolved.

WatchGuard

Educación e Innovación

Tendencias tecnológicas para los nuevos retos

La crisis de la Covid-19 ha supuesto una revolución para la amplia mayoría de los sectores, con especial incidencia en la educación y la formación. Este cambio de paradigma ha provocado un verdadero cambio en el perfil profesional que buscan los empleadores, que ahora se apoya más que nunca en otro tipo de habilidades más allá de la capacitación. Las instituciones educativas también han necesitado abordar su propio proceso de transformación digital, con un ojo puesto en las posibilidades que pueden proporcionar tecnologías disruptivas como la Realidad Virtual (RA) o el Internet de las Cosas (IoT).

El primer trimestre de 2020 ha marcado un antes y un después en la economía global. La pandemia derivada de la Covid-19 ha provocado una revolución en los procesos empresariales de prácticamente todos los sectores, que se han visto en la necesidad de acelerar su transformación digital a pasos agigantados para poder seguir siendo relevantes en un mundo cada vez más interconectado, tanto a nivel interno como de cara a sus clientes y/o usuarios.

El sector educativo es uno de los que más se ha visto afectado por esta pandemia, ya que los confinamientos y la recomendación de mantener una distancia interpersonal adecuada hicieron que la presencialidad en la formación se viera interrumpida en un primer momento. Según el informe Panorama de la Educación (Education at a Glance) 2020 de la OECD, China fue el primer país que abordó el cierre de las instituciones educativas en febrero de 2020. A finales de marzo del mismo año este cierre se había instaurado en algún grado en los 38 países miembros y los 8 asociados de la OECD.

En España, el freno a la educación y formación presencial se produjo entre el 11 y el 13 de marzo, ratificado por el Real Decreto 463/2020, de 14 de marzo, que declaró el estado de alarma para la gestión de la crisis sanitaria. Esto provocó que el sector tuviera que enfrentar una transformación digital a gran escala de manera forzosa, ya que todas las actividades que antes se realizaban en un entorno físico debían pasar a efectuarse de manera online, estuvieran o no preparados instituciones y estudiantes.

NUEVOS PERFILES PARA UN NUEVO ENTORNO GLOBAL

Al igual que empresas y demás organismos han necesitado reinventar todos sus procesos, este cambio de paradigma ha puesto de relieve la necesidad de una evolución en el sector educativo para preparar mejor a estudiantes y profesionales, de cara a formar a los mejores perfiles en esta nueva realidad empresarial.

En este sentido, el perfil del formador toma un papel importante, ya que ha necesitado redefinirse, huyendo del rol tradicional hacia nuevas técnicas formativas que obedezcan las necesidades actuales. Según una encuesta de UNICEF España para conocer la respuesta de la comunidad educativa frente a la pandemia de la COVID-19, más de la mitad de los docentes creía importante abordar la formación docente para mejorar la calidad de la educación a distancia, mientras que un 21,7% lo consideraba urgente.

Este entorno global en constante cambio requiere resistencia y adaptabilidad. Un informe

de McKinsey Global Institute estima que en 2030 la demanda de habilidades tecnológicas entre los profesionales aumentará en un 52%, las habilidades sociales y emocionales un 22% y las habilidades cognitivas en un 7%. Por su parte, el informe Workforce Ecosystems de MITSloan Management Review en colaboración con Deloitte señalaba que más del 90% de los managers encuestados creía necesario el acceso a nuevas capacidades, conjuntos de habilidades y competencias de cara al futuro. De ellos, el 35% apostaba por impulsar capacidades en los campos digital, de datos, cloud, seguridad y soft skills.

Los datos señalan que esta era del teletrabajo ha cambiado por completo las características que los reclutadores buscan entre los nuevos empleados, cobrando cada vez más importancia las habilidades blandas o 'soft skills' frente a la capacitación profesional. La escuela de negocios IEBS señala 10 de estas habilidades como imprescindibles, donde que destacan la resiliencia, el pensamiento crítico, el compromiso, la flexibilidad, el trabajo en equipo, la mentalidad de crecimiento, el aprendizaje constante e independiente, la creatividad, la toma de decisiones en base a datos y las habilidades digitales.

TECNOLOGÍA Y CERTIFICACIONES PARA LA NUEVA NORMALIDAD

La nueva realidad ha supuesto un avance en la transformación digital del sector que se ha visto en la necesidad de apostar por la tecnología para impartir formación a través de métodos que no se habían instaurado en gran medida con anterioridad a la pandemia. El reto al que se enfrentan las instituciones educativas es el de capacitar a sus alumnos para que sean capaces de competir en un nuevo entorno laboral.

El sector educativo es uno de los que más se ha visto afectado por esta pandemia, ya que los confinamientos y la recomendación de mantener una distancia interpersonal adecuada hicieron que la presencialidad en la formación se viera interrumpida en un primer momento

El Informe del Estudiante Conectado de Salesforce pone de manifiesto que esta nueva normalidad debe apostar por un entorno mixto, como demuestra que el 43% de los estudiantes y el 54% de los profesionales está a favor de los cursos híbridos. Según el mismo estudio, más de seis de cada diez miembros del personal afirmó que la pandemia obligó a su institución a reevaluar los modelos de servicio y apoyo del personal, así como a invertir en capacitación que permitiera al

profesorado y al resto del personal desempeñar su trabajo de forma virtual. Por otro lado, el 52% estima que su institución invertirá en más tecnología para el aula y más de una cuarta parte afirmó que su institución ha incorporado un puesto de supervisión de la experiencia digital de estudiantes y personal.

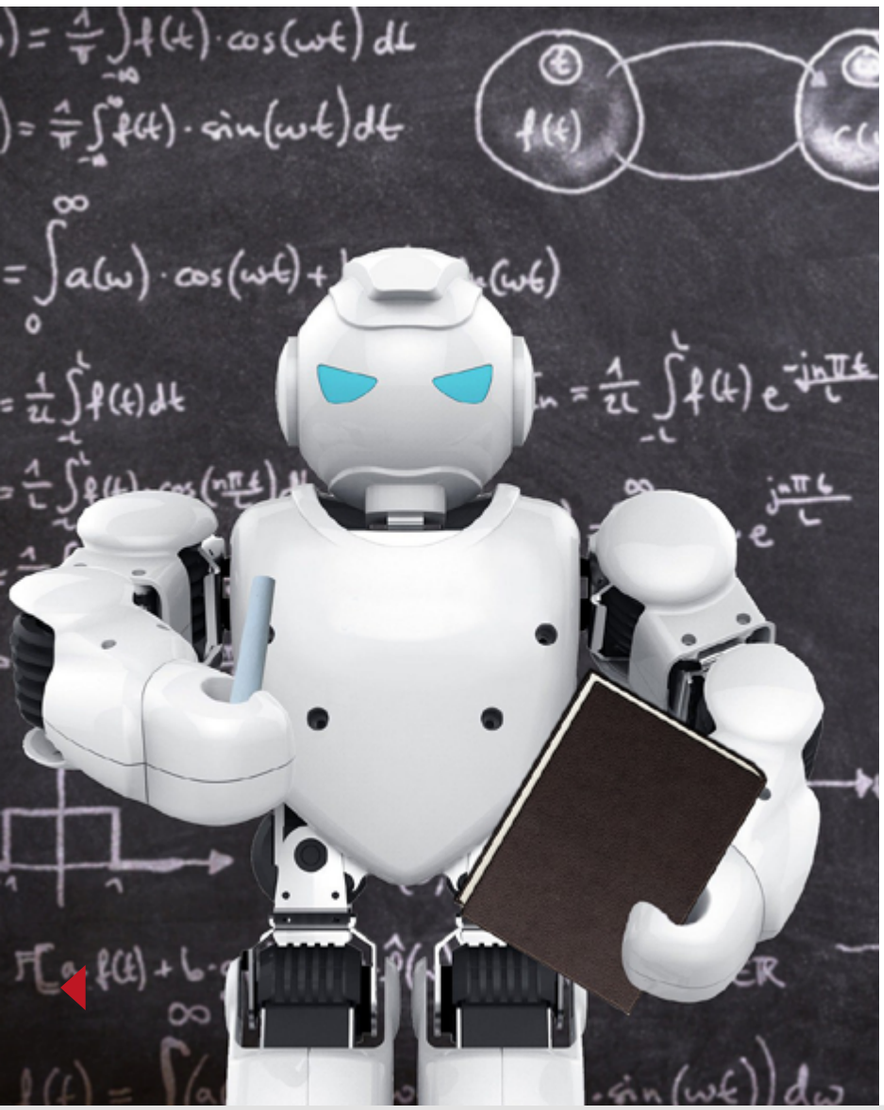
A nivel profesional, el panorama señala que los procesos de selección apostarán por certificaciones y conocimientos prácticos frente a la posesión de títulos a la hora de buscar talento. En este sentido, las competencias tecnológicas toman mayor importancia, ya que las empresas necesitan de personal formado en esta materia para poder sustentar la transformación digital en la que se ven inmersas. De hecho, según el informe The Future of Jobs del World Economic Forum, la capacidad de las empresas a nivel global para aprovechar el potencial de crecimiento que ofrece la adopción de las nuevas tecnologías se ve obstaculizada por la escasez de competencias, por lo que están apostando por potenciar la formación de sus trabajadores. Según este estudio, las empresas están proporcionando oportunidades de formación para la reconversión y el perfeccionamiento profesional al 62% de su plantilla, mientras que para 2025 esperan ampliar esa oferta en un 11%. A pesar de ello, son los propios profesionales los que deben dar un paso adelante, ya que este mismo informe indica que solo el 42% de los empleados se acoge a los cursos ofrecidos por la empresa.

TENDENCIAS TECNOLÓGICAS PARA EL SECTOR EDUCATIVO

Una vez planteada esta transformación digital, las instituciones educativas tienen que pararse a pensar cuáles son las tecnologías en las que deben apoyarse para afrontar los nuevos retos que se les plantean a todos los niveles.
De nuevo el Informe del Estudiante Conectado de Salesforce señala que son varias las instituciones que ya están aplicando mejoras tecnológicas, pero muy pocas las que están utilizando sistemas integrados para comunicarse con sus estudiantes, por lo que se crean brechas en los servicios y la confianza. Así, según los resultados del estudio, menos de la mitad de las instituciones (47%) está priorizando las inversiones en integración tecnológica, mientras que el 45% está otorgando más importancia a los sistemas de CRM y el 40% está apostando por la tecnología de análisis de datos.

Gartner señala en su estudio Top Technology Trends Impacting Higher Education in 2021 cuatro categorías principales en las que se observan estas tendencias: experiencia del estudiante, sostenibilidad del negocio, escalar los cambios y la Nueva Normalidad.

El perfil del formador toma un papel importante, ya que ha necesitado redefinirse, huyendo del rol tradicional hacia nuevas técnicas formativas que obedezcan las necesidades actuales



A la hora de hablar de la experiencia del estudiante, Gartner apuesta por experiencias virtuales, ya que señalan que el 72% de los estudiantes expresó su preocupación por no poder ir al campus en 2020. Los eventos virtuales fueron, sin embargo, bien valorados por el 84% de los encuestados. De esta forma, vuelve a ponerse de relieve la importancia del modelo educacional híbrido y del aprendizaje inmersivo, apostando también por tecnologías como la realidad virtual por ejemplo a la hora de conocer las instalaciones de una institución mediante la puesta en marcha de tours virtuales. Un CRM que englobe a todos los departamentos de la institución también cobra importancia en este apartado, ya que permitirá seguir y optimizar todo el ciclo educativo del estudiante de forma centralizada, dando la oportunidad al centro de ofrecerle una mejor experiencia.

La ciberseguridad es uno de los campos más importantes y de las asignaturas pendientes a la hora de hablar del futuro tecnológico del sector y su sostenibilidad. Check Point Research señala que el sector de la educación/investigación es el que se está viendo más afectado en este sentido. De hecho, en los últimos meses las instituciones educativas españolas han recibido una media de 2.998 ataques semanales por centro, lo que se traduce en un 11% más que en el semestre anterior. El Informe de Ciberamenazas 2021 de SonicWall indica que el 63% de los centros educativos no revisan los permisos de forma regular, el 22% no sabe cómo se otorgan los derechos de acceso, el 24% admitió otorgar derechos de acceso directo a cualquier solicitud, y solo el 18% cuenta con un profesional de la ciberseguridad dedicado a tiempo completo entre el personal. Esta brecha entre el nivel de amenazas que se cierne sobre este sector y la falta de preparación de los centros para hacerlas frente es uno de los principales retos que debe abordar cuanto antes el ecosistema educativo.

El cloud computing se revela como la clave para poder escalar todos estos cambios de forma óptima. Al inicio de la pandemia, las universidades y los centros de enseñanza superior se encontraron en una situación de crisis en la que necesitaron una respuesta inmediata y escalable para poder prestar servicios a través de la enseñanza virtual y remota. La nube ofrece a las instituciones una serie de opciones que les permiten trabajar durante la pandemia y desplazó el foco tecnológico hacia objetivos operativos, como el funcionamiento de los centros de datos y la gestión de datos e infraestructura, para ayudar a los centros educativos a cumplir los objetivos más estratégicos en torno a la enseñanza, el aprendizaje y la participación de los estudiantes en el mundo virtual. Además sirve como base para construir la siguiente capa tecnológica para incluir aplicaciones SaaS, Inteligencia Artificial (IA), Business Intelligence (BI) o soluciones IoT.

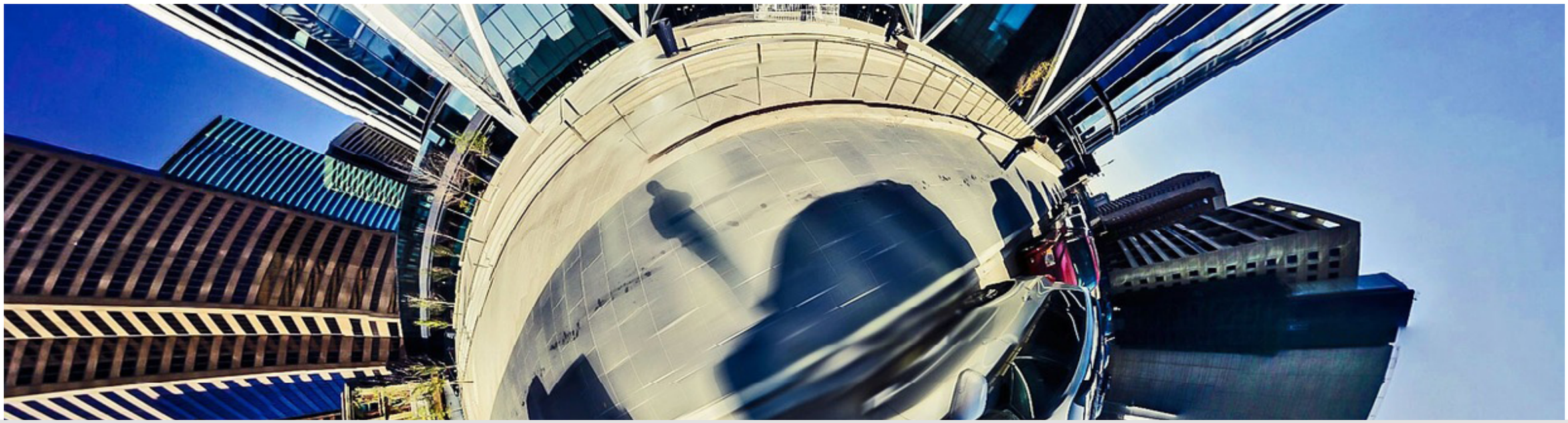
La automatización en las respuestas a los estudiantes viene de la mano de los Chatbots. El informe de Gartner señala que las instituciones educativas suelen renovar entre el 20% y el 25% de su población estudiantil cada año. Estos nuevos estudiantes tienden a hacer las mismas preguntas que generaciones anteriores, algo que se podría abordar gracias a esta tecnología ahorrando a los centros tiempo y dinero.

La Nueva Normalidad va a dar un papel especial a los dispositivos móviles en el sector educativo, así como el desarrollo de aplicaciones que ayuden en el desarrollo formativo del alumno. El sector de las EdTech está creciendo a un gran ritmo, con un valor a nivel global de algo más de 65.000 millones de euros, cifra que podría llegar hasta los 243.000 millones de euros según un estudio de Grand View Research.

El uso de todas estas tecnologías disruptivas en el sector educativo se ve respaldado por instituciones como la UNESCO, con actividades como la Conferencia internacional sobre la Inteligencia Artificial en la Educación o la Semana del Aprendizaje Mediante Dispositivos Móviles, iniciativas con las que el organismo ayuda a los gobiernos y a otras partes interesadas a valerse de las tecnologías para fomentar el aprendizaje.

Además, el Plan de Recuperación, Transformación y Resiliencia que recoge la estrategia del Gobierno de España para canalizar los fondos proporcionados por Europa para reparar los daños provocados por la crisis de la COVID-19, dedica dos componentes a la modernización del sistema educativo y a la Formación profesional (componentes 20 y 21), con acciones destinadas al refuerzo del capital humano de las próximas generaciones, la eliminación de brechas sociales y territoriales, y el acceso a oportunidades laborales dignas y adaptadas a las necesidades del mercado laboral. Este Plan busca, a través de la

Esta era del teletrabajo ha cambiado por completo las características que los reclutadores buscan entre los nuevos empleados, cobrando cada vez más importancia las habilidades blandas o 'soft skills' frente a la capacitación profesional



modernización y digitalización del sistema educativo, avanzar en un modelo educativo personalizado, flexible, que se adapte a las necesidades del alumnado, prevenga el abandono temprano de la educación y promueva la mejora de los resultados educativos. Para alumnos de formación superior, el Plan prepara medidas como la modernización del sistema universitario, el refuerzo de la Universidad Nacional de Educación a Distancia o la mejora de las infraestructuras digitales y equipamientos universitarios.

Está claro que la pandemia de la Covid-19 ha planteado un nuevo escenario en el que el sector educativo ha necesitado encontrar soluciones de manera urgente, acelerando así su transformación digital. Las nuevas tecnologías serán el punto de apoyo para que el sector sea capaz de resolver las necesidades que este novedoso entorno está planteando tanto para el personal propio como para los alumnos, de manera que la Nueva Normalidad suponga un aliciente y se convierta en el empujón definitivo para que las instituciones se olviden del modelo tradicional y puedan dirigirse sin más excusas hacia la educación del futuro. ■

MÁS INFORMACIÓN

- Panorama de la Educación (Education at a Glance) 2020 de la OECD
- Real Decreto 463/2020, de 14 de marzo
- Encuesta de UNICEF España para conocer la respuesta de la comunidad educativa frente a la pandemia de la COVID-19
- Informe de McKinsey Global Institute sobre la demanda de habilidades tecnológicas entre los profesionales
- Informe Workforce Ecosystems de MITSloan Management Review en colaboración con Deloitte
- Informe IEBS School sobre soft skills más demandadas en 2021
- Informe del Estudiante Conectado de Salesforce
- The Future of Jobs del World Economic Forum
- Top Technology Trends Impacting Higher Education in 2021 de Gartner
- Datos de ciberataques en el sector educativo de Check Point Research
- Informe de Ciberamenazas 2021 de SonicWall
- Estudio de Grand View Research sobre el mercado EdTech
- Conferencia internacional sobre la Inteligencia Artificial en la Educación de la UNESCO
- Semana del Aprendizaje Mediante Dispositivos Móviles de la UNESCO
- Plan de Recuperación, Transformación y Resiliencia

Rainbow™

Alcatel·Lucent Enterprise

Rainbow™ Classroom

Recrear la experiencia del aula, a distancia, desde su sistema de gestión de aprendizaje

#Educación

#EnseñanzaColaborativa

Educación e Innovación.

Tendencias tecnológicas para los nuevos retos

El sector educativo ha sido uno de los más afectados por la pandemia. Se ha visto en la necesidad de acelerar su transformación digital a pasos agigantados para poder responder a las necesidades de una realidad inédita. Las nuevas tecnologías y la seguridad de toda su infraestructura cobran ahora más importancia que nunca.

La pandemia derivada de la Covid-19 ha provocado un cambio de paradigma en toda la sociedad. Uno de los sectores que más ha sufrido esta situación ha sido el de la educación y la formación, ya que de la noche a la mañana se ha encontrado con la necesidad de realizar todo un cambio en su actividad, pasando de un modelo casi completamente presencial a sistemas de enseñanza en remoto. En esta realidad, en la que los players del sector han tenido que realizar una transformación digital acelerada, las nuevas tecnologías se han convertido en la clave, así como la necesidad de securizar toda esa nueva infraestructura. Por ello, ¿cuáles son los principales retos a los que se debe enfrentar el sector educativo y de la formación en esta nueva normalidad? Para analizar cómo ha impactado este último año en el sector; la brecha digital de la educación; sus carencias; cuáles son las tecnologías o especializaciones que están experimentando mayor demanda; cómo va a impactar este

EDUCACIÓN E INNOVACIÓN.
Tendencias tecnológicas para los nuevos retos

"Toda esa tecnología que está ahí tiene que ser acometida de una manera rápida, flexible, compatible con el futuro, abierta, es ahí donde pensamos que va a haber una gran demanda"

ENRIQUE SÁNCHEZ, COUNTRY BUSINESS LEADER DE ALCATEL LUCENT ENTERPRISE

nuevo modelo en la tecnología; o hacia dónde se dirige el futuro de la educación y qué tecnologías serán las más necesarias, hemos contado en esta Mesa Redonda IT con la participación de Enrique Sánchez, Country Business Leader de Alcatel Lucent Enterprise; Carlos Tortosa, Director de Grandes Cuentas de ESET; Eduardo Moreno, Country Manager de Global Knowledge; Álvaro Fernández, Account Executive de Sophos; y Ricardo de Ena, Area Sales Manager North Spain de WatchGuard.

EL IMPACTO DE LA PANDEMIA EN LA EDUCACIÓN

El último año ha supuesto toda una revolución para el sector, que se ha visto obligado a iniciar una abrupta digitalización de todos sus procesos para poder seguir realizando su actividad. Como indica Enrique Sánchez, "ha significado un cambio de prioridades. La tecnología estaba ahí, pero la prioridad en el uso ha sido muy distinta". Los modelos híbridos han provocado que el uso de las plataformas sea desde cualquier dispositivo y desde cualquier lugar, lo que ha puesto a prueba las capacidades de las empresas de TI para entregar soluciones adecuadas.

Desde el lado formativo, Eduardo Moreno considera que aún nos encontramos en un proceso de adaptación a un nuevo paradigma que ha venido para quedarse. "Las modalidades de impartir formación van a ser clave y van a cambiar la forma en la que aprendemos. Era un paso que quizá ya venía dándose en los últimos años que la pandemia ha acelerado".

Para Álvaro Fernández, el sector de la educación era el más analógico, por lo que la pandemia realmente ha provocado una situación de contingencia. "Ha sido algo completamente inesperado y el sector educativo no estaba preparado, porque era uno de los sectores que se encontraba en un estado más incipiente de

"A nivel tecnológico lo que más se va a demandar va a seguir siendo la protección del dispositivo y la protección de la información, añadiendo la identificación del usuario y después los servicios necesarios para que todo ese círculo esté bien gestionado"

CARLOS TORTOSA, DIRECTOR DE GRANDES CUENTAS DE ESET

transformación digital". Dado que los centros tuvieron que implantar toda esta tecnología con urgencia, ahora es el momento de pensar en la seguridad de esta infraestructura.

REDUCIENDO LA BRECHA DIGITAL

Aunque sea complicado observar puntos positivos en esta situación, es posible que haya

servido para reducir la brecha digital del sector educativo, aunque quizás no lo suficiente.

Así lo señala Carlos Tortosa, cuando habla de que en muchas ocasiones se siguen utilizando dispositivos personales en los que la seguridad puede verse en entredicho, mientras que otros centros han realizado una fuerte inversión para contar con dispositivos y un sistema adecuado. "Existe una brecha digital muy pequeña en lo que sería un entorno educativo más universitario, por la necesidad de disponer de dispositivos con recursos y en los que el nivel de protección es superior. Después, si bajamos un poco el escalón, en la educación secundaria y primaria, es mucho más complicado. Sobre todo porque la brecha digital viene bastante marcada por una brecha también económica".

Por su parte, Ricardo de Ena opina que poco a poco se irá reduciendo esta brecha digital. "Todo lleva un proceso paulatino, desde que se detecta, hasta que realmente se toman las medidas, hasta que realmente hay una labor de concienciación, que deberíamos entonar un poco el mea culpa, si realmente estamos concienciando todo lo que implica y todas las consecuencias que tiene el cerrar esa brecha". Algo que se ve por ejemplo en la actualidad con la carencia de chips que está viviendo el mercado provocada por este boom en la digitalización.

Enrique Sánchez cree que reducir esta brecha digital es una necesidad del mercado y una oportunidad de negocio. "Ya no se trata de ver cómo

Eduardo Moreno
Country Manager, Global Knowledge

"Las modalidades de impartir formación van a ser clave y van a cambiar la forma en la que aprendemos. Era un paso que quizá ya venía dándose en los últimos años y que la pandemia ha acelerado"

EDUARDO MORENO, COUNTRY MANAGER DE GLOBAL KNOWLEDGE

afrontar la situación actual, sino de cuál va a ser el diseño de lo que vamos a hacer en el futuro". En general esta situación ha ayudado a que el sector madure, las conversaciones tanto con centros educativos como con universidades se han vuelto más efectivas. Es importante conseguir integraciones efectivas de la tecnología. Además, no solo hay que fijarse en la parte del alumno, sino que también es necesario poner foco en el funcionamiento interno de las instituciones

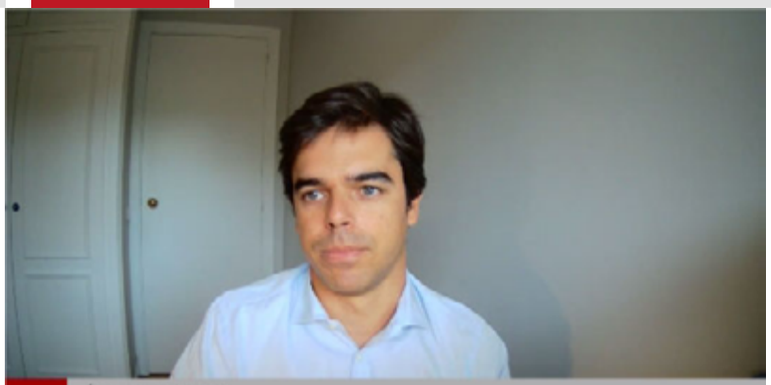
CARENCIAS DE UN SECTOR EN TRANSFORMACIÓN

La pandemia ha destapado algunas carencias tecnológicas en el sector educativo. ¿Cuáles son esos gaps que se han observado a raíz de esta situación?

En la opinión de Eduardo Moreno, universidades y colegios no estaban suficientemente preparados para esto. "Mover toda la formación a modalidades diferentes, como hemos tenido que hacer nosotros, virtualizar absolutamente todo, pasar a microlearnings, a otro tipo de formación más blended, donde se conjugan diferentes metodologías de entrega, requiere una especialización que seguramente ni universidades ni centros escolares tienen". A pesar de que se dispone de la tecnología y de las ganas necesarias para todo este proceso, falta el conocimiento para aplicarla de la forma más conveniente.

Después de haber puesto todo lo que estaba en su mano para conseguir que la rueda siguiera girando, como indica Ricardo de Ena, es el momento de pensar si se han tomado las medidas adecuadas y qué modelo se quiere adoptar. "Esto implica un alto grado de formación a todo ese claustro para hacer frente a esta nueva tecnología, que para ellos es completamente nueva".

Está de acuerdo Enrique Sánchez, que apostilla que esas carencias se han visto tanto en los usua-


Álvaro Fernández
Account Executive, Sophos

“La pandemia ha sido algo completamente inesperado y el sector educativo no estaba preparado, porque era uno de los sectores que se encontraba en un estado más incipiente de transformación digital”

ÁLVARO FERNÁNDEZ, ACCOUNT EXECUTIVE DE SOPHOS

rios como en el propio canal formativo. “Desde el punto de vista de gestión o de implementación ha habido claras áreas de mejora”. A pesar de ello se muestra optimista señalando que el trabajo que se está realizando tiene un ojo puesto en el futuro.

Carlos Tortosa hace hincapié en los gaps observados en la identificación del usuario. “Necesitamos saber realmente que quien está al otro lado de la pantalla es realmente quien dice ser”. También indica que hay otras carencias que se han incrementado, sobre todo a nivel de ciberseguridad.

TECNOLOGÍAS Y ESPECIALIZACIONES MÁS DEMANDADAS

La realidad formativa está cambiando, dirigiéndose hacia nuevos modelos, pero, ¿cuáles son las tecnologías o especializaciones que están experimentando mayor demanda?

Álvaro Fernández lo tiene claro. “Los gestores de contenido y herramientas de videoconferencia han sido las que hemos visto que la demanda se ha incrementado”. La parte negativa es que ese aumento de demanda no se ha visto reflejado desde el punto de vista de la seguridad, algo que se va a plantear ahora.

En esta línea se muestra Carlos Tortosa, indicando que es necesario cubrir necesidades al hablar de autenticación, control parental y concienciación. “Todos tenemos claros cuáles son los riesgos que se corren, tenemos que intentar concienciar a todo el mundo de hasta qué punto todos esos riesgos son reales y qué necesidades tienen para proteger”.

Por su parte, Eduardo Moreno señala que la presencialidad no va a volver a la formación profesional porque realmente no le reporta mayor beneficio al alumno, lo que va a provocar un crecimiento en plataformas y modelos de e-learning. Del mismo modo que tampoco reporta ventajas para las instituciones de formación: “Para los centros educativos es muy complicado mantener centros de educación con muchos metros cuadrados para apenas impartir cursos”.


Ricardo de Ena
Area Sales Manager North Spain, WatchGuard

“Todo lleva un proceso paulatino, desde que se detecta, se toman las medidas, hasta que realmente hay una labor de concienciación; deberíamos entonar un poco el mea culpa, por si realmente estamos concienciando con todo lo que implica y con todas las consecuencias que tiene el cerrar esa brecha”

RICARDO DE ENA, AREA SALES MANAGER NORTH SPAIN DE WATCHGUARD

EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS

Tecnologías como el cloud, la seguridad o la movilidad han impactado mucho en este nuevo modelo educativo hacia el que se dirige el sector, ¿de qué manera van a hacerlo? En opinión de Enrique Sánchez es necesario que las redes sean inteligentes y capaces de adaptarse en todo momento. "Toda esa tecnología que está ahí tiene que ser acometida de una manera rápida, flexible, compatible con el futuro, abierta, es ahí donde pensamos que va a haber una gran demanda".

Ricardo de Ena pone énfasis en la ciberseguridad y comenta que al principio de la pandemia lo más demandado eran conexiones VPN, para que alumnos, profesores y demás personal del centro pudieran acceder a un entorno compartido, seguro y con accesos autenticados. Después la demanda derivó hacia redes wifi seguras con el modelo híbrido. "Ahora vendrán esas auditorías de 'bueno, lo que hemos puesto para pasar la pandemia, ¿nos vale o no nos vale? ¿Nos quedamos con algo o no nos vale?'"

Todo el nuevo paradigma educativo está basado en estas tres tecnologías, según indica Eduardo Moreno resaltando su papel a la hora de impactar en esta nueva realidad educativa. "Ciberseguridad y cloud tienen 0% de desempleo, con lo cual la demanda de estas profesiones va a crecer y crecer, tanto en el sector educativo como en todas las industrias en las que tengan impacto".

De acuerdo se muestra Álvaro Fernández al hablar de la alta tasa de empleabilidad que tienen estas áreas. Pero ahora lo importante es el reto que tienen los colegios de operar esa tecnología que acaban de implementar. "En muchos colegios el propio profesor de Informática es el administrador de sistemas y es la persona que lleva seguridad". De ahí la necesidad de que las soluciones sean fáciles de administrar. ■

MÁS INFORMACIÓN

Mesa redonda IT- Educación

El futuro de la educación

Este nuevo modelo ha venido para quedarse. Esto conduce al planteamiento de una cuestión importante: ¿Hacia dónde se dirige el futuro de la educación y qué tecnologías serán las más necesarias para el sector educativo?

Para Carlos Tortosa el sector se va a dirigir hacia un modelo híbrido, aunque en algunos casos se volverá a la presencialidad, sobre todo al hablar de los más jóvenes y los más mayores. "A nivel tecnológico lo que más se va a demandar va a seguir siendo la protección del dispositivo y la protección de la información, añadiendo la identificación del usuario y después los servicios necesarios para que todo ese círculo esté bien gestionado".

Ante esta pregunta, Álvaro Fernández subraya la necesidad de asentar y consolidar todo lo que se ha hecho durante este año y medio. "Esas tecnologías existen y las tienen que adoptar los centros educativos, tienen que consolidarlas". Desde el punto de vista de la seguridad, tecnologías como VPN, autenticación y servicios que acompañen esa seguridad serán la clave en los próximos años. Además, señala que la transformación digital del sector está comenzando y va a seguir durante los próximos años.

Para finalizar, Ricardo de Ena destaca dos aspectos que para él son fundamentales. Lo primero, que es importante securizar los sistemas sin mermar su rendimiento para que esta transformación digital no sea algo traumático para este sector tradicionalmente analógico. Por otro lado también señala que "volvemos un poco al 2005, cuando empezamos a hablar del bring your own device, que esto en el mercado precisamente de educación se ve al día. Tratar de borrar esa línea que decíamos entonces, esa delgada línea de en qué momento este dispositivo no es corporativo entonces no puedo tomar todas las políticas de ciberseguridad necesarias, pero a la vez necesito que lo traigas porque no te puedo ofrecer ninguno". Por ello incide en conseguir tener la máxima seguridad cumpliendo con la normativa sin que implique un impacto negativo en la conectividad.

MARÍA JOSÉ GARCÍA RODRÍGUEZ, DIRECTORA DE TECNOLOGÍAS
DE LA INFORMACIÓN DE LA UNIVERSIDAD AUTÓNOMA DE MADRID

“La tecnología ha demostrado que es capaz de abrir un abanico de posibilidades que no se habían explorado hasta la fecha”

El sector educativo ya se encontraba en un proceso de innovación disruptiva antes de la pandemia, por lo que, en realidad, la situación vivida solo ha acelerado este proceso.

En su opinión, ¿qué carencias desde el punto de vista tecnológico ha destapado la situación de pandemia que estamos viviendo en las Infraestructuras educativas?

En los días previos al inicio del confinamiento se propusieron muchas ideas para tratar de sobrellevar lo mejor posible el escenario que se nos veía encima, sin saber siquiera cuanto podría durar, porque, en un inicio, se hablaba de unos quince días. El equipo de TI de la UAM optó por pasar a producción los proyectos colaborativos que, hasta ese momento, eran tan solo simples pilotos. La parte tecnológica funcionó incluso mejor de lo esperado, por lo que no puedo destacar grandes carencias. Lo más “costoso” en realidad y en esas circunstancias, fue formar a los usuarios.

¿La situación vivida durante los últimos meses, ¿ha acelerado el proceso de transformación digital en el sector educativo? ¿De qué manera?

Sin duda. La tecnología ha demostrado que es capaz de abrir un abanico de posibilidades que no se habían explorado hasta la fecha, que la tecnología sirve de ayuda. Los métodos docentes previos a la pandemia eran como siempre habían sido las cosas y no se había planteado la posibilidad de cambiarlos, hasta ahora.

"Pasada la premura que requirió poner en marcha soluciones homogéneas, ahora es el momento de entrar al detalle, de poner en marcha una atención personalizada"

¿Cuáles son las principales demandas tecnológicas de los profesionales del sector educativo?
Pasada la premura que requirió poner en marcha soluciones homogéneas, ahora es el momento de entrar al detalle, de poner en marcha una atención personalizada. Porque ni todos los docentes son iguales, ni todas las materias se imparten de la misma forma.

Desde su punto de vista, ¿a qué retos se enfrenta la Educación en España y cuáles son las tecnologías más relevantes que impactan en estos retos?
El sector educativo se encuentra en proceso de cambio, y creo que todavía queda camino para considerarlo maduro. En mi opinión, para que el cambio sea aceptado, la experiencia de las personas ha de ser satisfactoria y para ello precisamos la colaboración de todos de manera coordinada y conjunta.

¿Hasta qué punto el cambio vivido en los modelos educativos ha venido para quedarse y de qué manera las nuevas tecnologías van a ayudar a este cambio y a su adaptación?
Gestionar este cambio que venimos afrontando no es tarea fácil. El área TIC debe ser ágil para dar soluciones a los problemas que se vayan planteando, de manera que los cambios se vayan asentando, y sean aceptados de buen grado.

¿Hacia dónde debe evolucionar la Educación y cuáles son los aspectos más críticos de mejora?
El sector educativo ya se encontraba en un proceso de innovación disruptiva antes de la pandemia, por lo que, en realidad, la situación vivida solo ha acelerado este proceso. Los informes internacionales, tales como Gartner, ya vienen marcando desde hace algunos años como las personas demandarán formación a lo largo de su vida, lo que va a requerir soluciones personalizadas para distintas necesidades. ■

MARÍA JOSÉ GARCÍA RODRÍGUEZ,
Directora de Tecnologías de la Información de la Universidad Autónoma de Madrid

Licenciada en C.C. Físicas por la UCM y Executive Master en Sistemas de Información por el IE, lleva más de 25 años desarrollando su carrera profesional en diferentes empresas y organismos, siempre en el área tecnológica.

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	Endpoint Protection Platform ESET Mail Security ESET Sharepoint Security ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET PROTECT	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Secure SharePoint Server ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
RESPUESTA	DETECCIÓN

CYBERSECURITY EXPERTS ON YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Responder al cambio de la realidad formativa

ENRIQUE SÁNCHEZ,
Country Business Leader España y Portugal, Alcatel-Lucent Enterprise

La pandemia, a la que tenemos todavía que referirnos, ha obligado de golpe a modificar presupuestos y modelos de negocio y a cambiar las prioridades en los presupuestos. Pero la tecnología ha demostrado algo con claridad: las comunicaciones en nube han eliminado el impacto negativo en la actividad de empresas, centros educativos y organismos de cualquier sector, por el teletrabajo, la enseñanza online y la actividad a distancia.

Centrándome ya en el sector de la enseñanza, hemos visto que algo que los responsables educativos llevaban tiempo valorando ha empezado a acelerarse: nuevos modelos educativos híbridos (que combinan lo remoto y lo presencial, incluso al mismo tiempo), mayor peso del acceso a las herramientas formativas desde cualquier lugar, gestión remota o simplificada de los procesos administrativos para los estudiantes. Asimismo, vemos que sigue siendo prioritario disponer de infraestructuras que garanticen el cumplimiento regulatorio y de seguridad, más teniendo en cuenta la explosión de nuevos elementos como la automatización de procesos mediante nuevos elementos como la IA o el IOT o la integración de comunicaciones en aplicaciones educativas.

DISMINUCIÓN DE LA BRECHA DIGITAL

Todo lo anterior ha supuesto, al menos desde el punto de vista de la priorización de objetivos a corto y medio plazo, un decremento de la brecha digital. Sin embargo, vemos que las entidades educativas aún deben percibir que la tecnología responde a sus necesidades concretas, a sus usos o procesos educativos concretos, y eso es misión de los suministradores y fabricantes como nosotros: debemos entender bien esos retos y tenemos que proponer a las organizaciones educativas soluciones que ofrezcan una respuesta clara y simple de valor demostrado.

Veamos un ejemplo: los responsables de IT de las entidades educativas sí saben que las redes les ofrecen la garantía de seguridad y adaptación a los estudiantes, profesores y personal administrativo. Sin embargo, si nos centramos en el proceso educativo en sí, vemos que muchas universidades o centros de enseñanza secundaria se han planteado aproximaciones de formación híbrida (parte presencial y parte remota) con soluciones que no han sido del todo satisfactorias (complejidad en el uso, necesidad de aprendizajes adicionales, despliegues caros como para generalizarlos en todas las aulas, dificultades culturales y de adaptación a nuevos usos, enseñanza deficiente por problemas de calidad de audio o vídeo). Una propuesta integrada en el entorno que actualmente utilizan y que tenga un mínimo coste de adaptación es esencial.

RESPONDER AL CAMBIO DE LA REALIDAD FORMATICA

Vamos hacia modelos nuevos de comunicaciones en la enseñanza. Muchas entidades ya analizan el futuro a medio plazo y los modelos que se adapten a la nueva realidad. Nosotros nos centramos en una aproximación holística, donde vemos las necesidades en aulas y campus y la forma en la que las redes contribuyen a proporcionar los servicios adecuados con las garantías de seguridad y priorización: redes que entienden los servicios y a los usuarios, y que adaptan sus condiciones a personas, dispositivos o entidades inteligentes.

Por otro lado, adquieren especial importancia los LMS (Learning Management Systems), con un uso general, incluso como elemento vertebrador de la formación en el aula, remota o híbrida. En este sentido, la integración de todos los medios audiovisuales y las comunicaciones en esos sistemas permiten más calidad. Deben tener un coste asequible (lo que descarta las complejas y caras salas de vídeo conferencia o telepresencia). Para cerrar el círculo y ofrecer un servicio integral, pensamos que se deben extender estas capacidades de integración en los procesos educativos a las actividades administrativas, con aplicaciones como los sistemas SIS (Student Information System) que ofrecen a los estudiantes una gestión sencilla desde cualquier lugar, integrando, y aquí está la innovación, el contacto en tiempo real con el personal administrativo, para resolver cualquier problema durante la matriculación, la gestión de pagos o la logística.

El modelo de impartición híbrido va a exigir soluciones flexibles de nube e integración de comunicaciones de tiempo real en los procesos y aplicaciones educativas (LMS, SIS, ...). Y la seguridad y el cumplimiento regulatorio obligarán a disponer de redes inteligentes, altamente disponibles, que contemplen perfiles de usuarios, de dispositivos (IoT o acceso a las aplicaciones) y de elementos que automatizan los procesos con inteligencia artificial. ■

ENRIQUE SÁNCHEZ,
COUNTRY BUSINESS LEADER DE ALCATEL LUCENT ENTERPRISE

Entender el sector para ofrecer soluciones a su medida

El sector educativo tiene necesidades muy específicas. El modelo de educación virtualizada y de soluciones colaborativas ha venido para quedarse, siendo necesario evolucionar con él. Por ello es necesario entender bien el sector para ofrecerle soluciones a su medida.

La transformación digital de la educación se enfrenta a tres grandes retos tecnológicos: seguridad, simplificación e integración. Enrique Sánchez, Country Business Leader de Alcatel Lucent Enterprise indica que leer bien lo que necesita el sector, debido a sus particularidades, es importantísimo.

Por ello es necesario que tanto canal como fabricantes hagan un esfuerzo didáctico y de simplificación para entender verdaderamente los procesos que hay detrás. Ser capaces de entregar soluciones verdaderamente transparentes para el cliente, para el usuario, para la gestión y para la integración. La filosofía de Alcatel Lucent Enterprise es la de crear tecnologías que vayan siempre pensadas hacia la verticalización. Por ello han desarrollado una plataforma abierta y específica cloud con una infraestructura que la soporta capaz de aglutinar todas estas necesidades específicas y servicios para este entorno en concreto de la educación.

Los objetivos favoritos en los que actúa el ransomware

JOSEP ALBORS,
Director de investigación y concienciación de ESET España

Las recomendaciones y medidas de seguridad necesarias para evitar y hacer frente a un ataque de ransomware son sobradamente conocidas y solo hace falta tener la voluntad y contar con los recursos necesarios para aplicarlas. Además, es necesario permanecer actualizado en lo que respecta a las técnicas usadas por los delincuentes para ir revisando las soluciones implementadas, de forma que estas sigan resultando efectivas.

A pesar de llevar muchos años conviviendo con esta amenaza, el ransomware sigue siendo algo desconocido o no muy tomada en cuenta por muchos usuarios y empresas. Por ese motivo, tanto los investigadores de ciberseguridad como los medios de comunicación no dejamos de hacernos eco de su evolución para generar concienciación y conseguir que se adopten medidas eficaces frente a esta amenaza.

Tras varios años analizando esta amenaza hemos podido comprobar como el ransomware ha ido afectando a prácticamente cualquier tipo de usuario o empresa de cualquier sector. Sin embargo, a la hora de elegir sus objetivos se ha visto una clara evolución, con los primeros casos afectando principalmente a usuarios particulares, pasando después a centrarse en pymes y afectando actualmente a empresas y organizaciones de cualquier tamaño.

Actualmente podemos observar ciertas tendencias a la hora de elegir objetivos por parte de los delincuentes y, si bien no estar entre estos objetivos principales no salva a ninguna empresa de ser víctima, si que es interesante analizar las preferencias de los criminales para obtener el mayor beneficio de sus acciones.

Según un reciente análisis, la víctima ideal de los actores detrás de la mayoría de casos de ransomware sería una empresa ubicada en Estados Unidos, Canadá, Australia o la Unión Europea y con unos ingresos mínimos de 5 millones de dólares (y preferiblemente mayores de 100 millones). Esto es solo una guía, puesto que todos los días vemos casos de ataques protagonizados por ransomware en otras regiones y hacia empresas de todos los tamaños, pero sirve para hacerse una idea de lo que buscan los delincuentes.

Además, es destacable observar como algunos grupos evitan atacar directamente o a través de sus afiliados a ciertos sectores como la educación, sanidad, gobierno u ONGs. Los motivos son variopintos y van desde la "ética profesional" hasta intentar evitar llamar demasiado la atención de las autoridades. Ataques recientes como el de Colonial Pipeline o Kaseya han demostrado las capacidades de estos grupos delictivos, pero también han provocado una reacción por parte de las autoridades que los ha puesto en el punto de mira, algo que no les conviene.

En lo que respecta a las técnicas preferidas por el ransomware actualmente, este es un tema que se ha tratado en varias ocasiones pero que nunca está de más repasar. Podemos ver como los accesos a través de RDP o VPN siguen siendo los favoritos por los delincuentes, habiéndose creado todo un mercado de compra/venta de accesos a redes corporativas donde ciertos delincuentes consiguen comprometer su seguridad para después vender este acceso a los operadores de ransomware

o sus afiliados para que accedan, roben información y, seguidamente, la cifren.

También se aprovechan todo tipo de vulnerabilidades para hacerse con el control de sistemas clave como los servidores de Exchange. Una vez se ha conseguido comprometer un sistema dentro de la red, lo normal es que se empleen varias herramientas como Mimikatz o Cobalt Strike para realizar movimientos laterales y conseguir acceder y comprometer otros sistemas importantes como los controladores de dominio, algo que facilita el robo de información confidencial y el posterior cifrado de todos los equipos de la red.

Otros métodos usados por los criminales son el uso del correo electrónico para adjuntar ficheros maliciosos o enlaces que inician la cadena de ejecución de este malware. También hemos visto como se realizan llamadas desde call centers para engañar a los usuarios y que estos descarguen malware desde ciertas páginas web e incluso se han llegado a realizar ofertas a posibles empleados descontentos para que infecten ellos mismos la red a cambio de un porcentaje de los beneficios obtenidos en el pago del rescate. ■

CARLOS TORTOSA, DIRECTOR DE GRANDES CUENTAS DE ESET

Concienciación y soluciones de seguridad robustas

Vivimos una realidad en la que la tecnología se ha vuelto imprescindible para el sector de la educación. A pesar de ello, los centros aún no están totalmente preparados ni completamente protegidos. Para conseguir esta seguridad, es muy importante concienciar a alumnos e instituciones, además de contar con las soluciones adecuadas.

El sector educativo comienza un nuevo curso en el que la tecnología va a seguir siendo protagonista, por lo que es importante proteger tanto dispositivos como redes, así como al propio usuario. Carlos Tortosa, Director de Grandes Cuentas de ESET, explica cómo los centros españoles han necesitado apostar por la digitalización y qué pasos hay que dar para mantener segura toda esa infraestructura.
ESET trabaja en una doble vertiente: concienciación y soluciones de seguridad robustas. Para ello, la compañía está acostumbrada desde hace años a ofrecer formaciones adaptadas a cada tipo de público, desde alumnos de 5 o 6 años hasta profesionales o directivos. Por su parte, las soluciones de ESET están específicamente diseñadas para proteger tanto a los dispositivos del usuario (ordenadores, teléfonos…) como al resto de la infraestructura del centro, incluyendo soluciones de control parental destinadas a proteger a los más pequeños.

Revolución digital
a través de la formación digital

EDUARDO MORENO,
Director General Global Knowledge
(a Skillsoft company)

La transformación digital es la única vía para conseguir no solo competitividad, sino la recuperación económica que tanto necesitamos tras estos tiempos de pandemia y sus consecuencias.

El COVID-19 nos ha obligado a todos a entrar de lleno y quizá de manera apresurada en lo que podríamos llamar la primera revolución digital, una evolución de la segunda revolución industrial que comenzó a principios del siglo XX. En pocas industrias no existe ya cierta huella digital, pero el porvenir es enorme. Es tan grande que es inimaginable, pero indudablemente tiene sus riesgos:

La transformación digital no es ni será sencilla, sobre todo para muchas empresas basadas en procesos tradicionales bien analógicos y/o manuales y, desde luego, pasará por un intenso programa de formación y actualización (o reskilling) a todos los niveles y en todas las capas de cada empresa, independientemente del trabajo.

Este no es el único reto que tenemos por delante: a pesar de que tecnologías como Cloud o Ciberseguridad tienen un 0% unemployment, la industria sigue padeciendo una enorme falta de profesionales en la mayoría de las grandes tendencias tecnológicas, amenazando con ello a un desarrollo adecuado de esta revolución y pudiendo provocar diferencias sociales aún mayores debidas al estancamiento de muchas empresas que no encuentran la llave del crecimiento por falta de conocimiento.

Una vez más, la solución a esta amenaza vuelve a estar en manos de la formación, facilitador clave de la revolución digital.

La formación y la educación también se han visto digitalizadas a todos los niveles. Todos lo hemos vivido encerrados en casa, trabajando desde nuestro despacho con un ordenador portátil, educando a los niños con un iPad, o aprendiendo idiomas desde un móvil y no en un aula. ¿Qué hubiera sido de nuestra economía sin las posibilidades que nos ha brindado la tecnología?

No obstante, la formación solo será la solución a la falta de competitividad, a la brecha digital y al desempleo si también consigue transformarse y adaptarse.

Empresas como Global Knowledge o Skillsoft ya ofrecen todo un arsenal de modalidades de entrega de contenidos que facilitan el aprendizaje en cualquier lugar, de cualquier forma y en cualquier momento.

Las empresas sumidas en plena transformación digital necesitan facilidades. No pueden

abandonar su negocio y dedicar todos sus recursos en pro de la era digital. Necesitan flexibilidad, necesitan poder transformar a sus equipos a través de itinerarios que los lleven de “A” a “B” sin que ello impacte en su día a día. Necesitan poder acceder a un contenido formativo en cualquier momento y poder tener un mentor que les guíe cada día. Necesitan poder practicar con las tecnologías a través de laboratorios disponibles 24x7, y siempre accesibles. Necesitan contenidos actualizados en formato digital, y necesitan poder probar sus conocimientos a través de certificaciones on line, sin necesidad de desplazamientos.

Necesitan, sobre todo, que las empresas de formación nos transformemos tanto como ellos necesitan, y que nos adaptemos totalmente a las demandas de esta ola digital. Una ola que nos llevará a la orilla o que nos arrastrará al fondo. Depende de cómo la abordemos... ■

EDUARDO MORENO, COUNTRY MANAGER DE GLOBAL KNOWLEDGE

Ofrecer un servicio formativo especializado basado en las nuevas tecnologías

El impacto que ha tenido la pandemia en el sector educativo ha sido enorme, que ha cambiado completamente el modelo formativo. También ha provocado una aceleración a la hora de adoptar diferentes tecnologías y modalidades de entrega como la formación virtual o el e-learning.

El reto al que se enfrentan los learning partners es el de adaptarse a estas nuevas circunstancias y crear una infraestructura que pueda ofrecer un servicio formativo especializado basándose en las nuevas tecnologías. Para Eduardo Moreno, Country Manager de Global Knowledge, el cloud y la ciberseguridad son las tendencias más importantes a nivel formativo, ya que se trata de profesiones en las que el desempleo es prácticamente inexistente.

La salida a bolsa de Global Knowledge, así como su fusión con Skillsoft, ha supuesto una gran oportunidad para la compañía. Su propuesta se basa en una experiencia de más de 25 años en el mercado, la especialización de sus formaciones, multimodalidad de entrega y un equipo de profesionales comprometido para asesorar sobre cualquier carrera en la que el cliente quiera especializarse. Además, cuentan con una plataforma basada en inteligencia artificial para gestionar en tiempo real la formación y el talento de los equipos.

Seguridad, pieza clave
en el proyecto educativo de los centros

RICARDO DE ENA,
Area Sales Manager
North Spain WatchGuard Technologies

Internet, smartphones, tablets, apps, Wi-Fi, redes sociales, cloud... es un hecho que las TI nos han cambiado la vida y, por extensión, han influido en la docencia, especialmente a raíz de la pandemia del COVID-19 que, como en tantos otros ámbitos, ha marcado un punto de inflexión en el sector educativo, poniendo de relieve aún más la importancia de la educación online, la dependencia de las nuevas tecnologías y, por supuesto, de contar con accesos y conexiones seguras.

Más del 79% de los profesores cree que la tecnología marca una importante diferencia para hacer que el aprendizaje sea más interesante. Pero si se tienen en cuenta los riesgos asociados al mundo cibernético... la respuesta puede no ser tan positiva, pues hay muchas cuestiones de seguridad relacionadas con el aprendizaje a través del uso de las TI y la educación a distancia, que van desde la seguridad intrínseca de la plataforma elegida y las cuestiones relacionadas con la privacidad, hasta el control del acceso de los usuarios y los problemas relacionados con los derechos de autor de los documentos compartidos en esas plataformas. Por último, está la cuestión de la protección de los menores y otras personas que hacen uso de la plataforma elegida.

Aunque como en todo, en el equilibrio está el punto medio. Y es aquí donde no se deben escatimar esfuerzos por promover la seguridad en los entornos educativos y trabajar para concienciar en el uso responsable de las TI entre alumnos y el personal docente.

Los retos a superar son múltiples, ya que administrar los sistemas de TI en cualquier institución educativa no es tarea fácil. Hoy, los centros de enseñanza cuentan con una base de usuarios formada por estudiantes y personal dispersos en amplias instalaciones que se conectan a través de redes cableadas e inalámbricas por distintos tipos de dispositivos. Recordemos que los dispositivos móviles también están transformando la educación y, por tanto, que los centros necesitan ofrecer acceso a los estudiantes a Wi-Fi de alta velocidad para proporcionarles una abundante cantidad de recursos educativos y herramientas de aprendizaje online. En muchas redes, la seguridad Wi-Fi llega tarde, pero en las escuelas las redes cableadas e inalámbricas requieren lo mismo, es decir, la implementación de soluciones de protección sólidas. Al mismo tiempo, se deben mantener controles adecuados para ofrecer una experiencia en Internet segura y apropiada teniendo en cuenta la edad, pues no debemos olvidar que muchos colegios tienen menores bajo su cuidado.

En definitiva, hablamos de entornos complejos, donde las exigencias a las infraestructuras de TI en términos de rendimiento y seguridad son de lo más alto, pues deben tomarse precauciones para evitar potenciales ciberataques o un mal uso de las tecnologías o la información personal, así como de otro tipo de riesgos que minen una gestión educativa óptima y con garantías para el desarrollo de los estudiantes. Avalar un acceso seguro a Internet y los recursos online, es parte de la estrategia de ciberseguridad que toda institución docente ha de incorporar a su proyecto educativo.

Afortunadamente, y como no podía ser menos, la respuesta a estos desafíos se encuentra también en las TI. Tecnologías más sofisticadas que aportan una protección inteligente e integral, así como la visibilidad de defensa en profundidad ne-

cesaria para proteger a los jóvenes estudiantes y al personal docente, pero a su vez, más fáciles de implementar y gestionar, son uno de los pilares sobre los que se asienta la seguridad de los entornos tecnológicos dentro del mundo de la enseñanza actual conectada que requiere un enfoque unificado para la protección de sus arquitecturas de red. Hoy existen tecnologías inteligentes, rápidas y eficaces diseñadas exclusivamente para garantizar y cumplir con los requisitos de seguridad de las conexiones WiFi más exigentes en el terreno de la enseñanza. Soluciones de autenticación multifactor (MFA) que permiten proteger tanto las contraseñas como la identidad de los usuarios que se conectan a la red del centro educativo, así como sus activos. Herramientas de protección de los endpoints con tecnologías Zero-Trust que permiten la supervisión continua de los endpoints, la detección y la clasificación de toda la actividad para revelar y bloquear comportamientos anómalos de los usuarios, las máquinas y los procesos. Y, por supuesto, tecnologías de protección de red que ayudan a mantener la red protegida contra las amenazas más avanzadas y zero-days. ■

RICARDO DE ENA, AREA SALES MANAGER NORTH SPAIN DE WATCHGUARD

La seguridad como servicio para proteger la transformación digital de la educación

La educación se ha caracterizado por ser un sector muy tradicional que siempre ha estado a la cola desde el punto de vista tecnológico. La pandemia ha provocado una digitalización forzada del sector, en el que el modelo híbrido es el que más posibilidades tiene de asentarse.

El sector educativo está afrontando esa transformación en la medida de sus posibilidades, sobre todo lastrado también por la falta de microchips a escala global. Ricardo de Ena, Area Sales Manager North Spain de WatchGuard, señala que esto ha provocado una apuesta por el modelo de Bring your own Device (BYOD), lo que implica un reto para la seguridad tanto de los propios dispositivos como a la hora de conectarse a la red del centro. La propuesta de WatchGuard está focalizada en el Security as a Service, modelo en el que el cliente puede contar con un partner hiperespecializado capaz de controlar todos los puntos relacionados con la ciberseguridad, desde el perímetro hasta los accesos, pasando por la red o el endpoint, todo ello de una forma sencilla y con un coste ajustado. Además, cuentan con una capa de big data y de monitorización que permite tener una visión global de todo lo que está pasando en la organización.

Principales problemas de ciberseguridad en educación

ÁLVARO FERNANDEZ,
Account Executive para Sophos Iberia

Los ciberdelincuentes han estado atareados buscando nuevas formas de aprovechar técnicas como phishing, ransomware, ingeniería social para llevar a cabo ataques en centros educativos. A continuación, presentamos algunos de los puntos más críticos que deben abordarse para proteger a los usuarios y a los datos.

Los estudiantes y los profesores necesitan tener acceso a herramientas de aprendizaje ubicadas principalmente en la nube (aplicaciones para compartir archivos, email, aplicaciones) y a veces necesitan acceder de forma remota a los recursos en la red escolar. Al mismo tiempo, el personal administrativo y de TI que trabaja desde casa también puede necesitar acceso a sistemas y documentos ubicados en la red escolar. Si el acceso remoto no es seguro, los ciberdelincuentes pueden colarse y tomar el control de toda la red. Utilizar una red privada virtual (VPN) que ofrezca acceso remoto seguro a los usuarios y que proteja todos los datos que fluyen dentro y fuera de la VPN al cifrarlos, es fundamental.

Otro punto importante es contar con una sincronización entre firewall y la seguridad de los endpoints, para identificar instantáneamente los endpoints comprometidos, en el caso de haberlos, aislarlos hasta que se limpien y evitar que las infecciones se propaguen lateralmente a otros dispositivos en la red.

CONTROLAR EL ACCESO A DATOS CONFIDENCIALES

Los datos personales de estudiantes, maestros, exalumnos y personal administrativo, junto con datos confidenciales relacionados con la investigación y la propiedad intelectual de un centro educativo pueden enriquecer a un ciberdelincuente al venderlo o pedir un rescate. Es fundamental imponer el acceso en función de la identidad del usuario, lo que permita a los usuarios autorizados acceder solo a lo que necesitan para realizar su trabajo. Para proteger los datos confidenciales, la investigación y otros recursos críticos, permitir el acceso solo a aquellos que están autorizados, con soporte de autenticación de dos factores (2FA) para acceder a áreas clave del sistema, incluidos IPsec y SSL VPN, portales de usuarios y consolas de administración web, es la mejor opción.

PROTECCIÓN CONTRA MALWARE

Es difícil saber si los dispositivos y las aplicaciones utilizados, cuentan con los últimos parches de seguridad y si el antivirus está actualizado. A menos que dichos dispositivos remotos se conecten a través de una VPN, deberá asegurarse de que están seguros antes de que puedan acceder a los recursos de la red educativa.

Es importante implementar capacidades avanzadas de protección web que puedan identificar y bloquear las últimas amenazas web. Esto permite aplicar reglas de filtrado web para mantener a los estudiantes a salvo de casos de ciberacoso, contenido inapropiado, abuso y otras amenazas online. Los controles periféricos le permiten controlar lo que su personal puede y no puede conectar a sus dispositivos corporativos. Esto le ayuda a proteger su red contra amenazas inesperadas.

PROTECCIÓN CONTRA PHISHING

Los ataques de ingeniería social y phishing plantean importantes riesgos de ciberseguridad para las instituciones educativas. Los estudiantes, profesores o miembros del personal

pueden ser engañados para hacer clic en enlaces maliciosos que pueden proporcionar a los ciberdelincuentes acceso a la red de la escuela y sus valiosos recursos. La mejor manera de contrarrestar los ataques de ingeniería social y phishing es a través de la concienciación y capacitación del usuario. Educar y testear a los usuarios con ataques simulados ayuda a facilitar una cultura positiva de concienciación en ciberseguridad y los hace menos propensos a caer en estafas. Es importante que la seguridad del correo electrónico también esté actualizada y que todos los endpoints tengan protección avanzada contra malware, ransomware, exploits y virus conocidos y desconocidos.

Los dispositivos móviles como teléfonos, tabletas y otros se utilizan cada vez más para la enseñanza. Un solo dispositivo desprotegido aumenta el riesgo de comprometer toda la red y los sistemas escolares, especialmente en un momento en que las escuelas han reducido las barreras para acceder a sus redes, específicamente para los estudiantes. Con la mayoría de los dispositivos conectados a Internet, la superficie de ataque aumenta significativamente. Una solución de seguridad efectiva para dispositivos móviles puede ayudar a mantener seguros a los estudiantes y al personal en Internet, evitando descargas de archivos peligrosos y bloqueando el acceso a sitios web inapropiados. ■

ÁLVARO FERNÁNDEZ, ACCOUNT EXECUTIVE DE SOPHOS

Consolidar y mantener seguras las tecnologías implementadas

La pandemia ha golpeado de lleno al sector de la educación, viviendo una situación de contingencia. Aún falta mucho camino por recorrer tanto desde el punto de vista tecnológico como de la seguridad. Ya no vale sólo con tener una protección para el puesto, es necesario implementar otras tecnologías más avanzadas para mantenerse seguros.

El sector educativo ha sido capaz de acelerar su transformación digital como consecuencia de la crisis provocada por el coronavirus, pero es necesario consolidar lo que se ha hecho hasta el momento y mantener seguras esas tecnologías. Álvaro Fernández, Account Executive de Sophos, señala que la pandemia nos ha enseñado a estar más preparados para dar respuesta ante situaciones que no puedes planificar.

La oferta de Sophos se basa en tres pilares: efectividad en costes, autonomía y sencillez. Sus soluciones ayudan a proteger tanto dispositivos como redes, puntos de acceso o infraestructuras Cloud, con todo centralizado en una única plataforma de gestión en la nube que interconecta todas las soluciones de seguridad de la compañía, para que sean capaces de coordinarse entre sí y tomar decisiones de forma automatizada.

Las amenazas en el sector educativo crecen al ritmo de su digitalización

ALFONSO RAMÍREZ,
director general
Kaspersky Iberia

En el último año y medio, y especialmente debido a la pandemia, el sector educativo ha pasado a entrar en la lista de objetivos de los ciberdelincuentes. Hasta entonces, la incidencia de ataques era bastante limitada, pero con la implantación de la teleeducación y la incorporación de un número cada vez mayor de recursos online para utilizar en el aula, el número de amenazas y su variedad ha evolucionado en gran medida.

Aunque la mayoría del alumnado en España ha vuelto a la educación presencial, el proceso de digitalización del sector sigue avanzando. Por un lado, se adoptan nuevas herramientas y posibilidades para el uso pedagógico, incluyendo varias que no habían sido pensadas para cumplir este rol. Un buen ejemplo de ello son las cuentas de TikTok o Instagram que se usan como complemento a la educación. Muchos de estos nuevos instrumentos están mejorando la experiencia de la enseñanza, pero también introduciendo nuevas amenazas. Algunas de las más habituales son:

1. Los Sistemas de Gestión de Aprendizaje (LMS) como Google Classroom o Frog permiten a los profesores hacer un seguimiento del proceso de aprendizaje de los estudiantes, a la vez que registran su progreso y los aspectos que requieren su atención. A medida que aumenta la cantidad y popularidad de los LMS, también crece el número de sitios de phishing asociados con servicios educativos y de videoconferencias. Sus principales objetivos son robar datos personales o difundir spam en la comunidad educativa. Además, los LMS abren la

posibilidad de que surjan amenazas nuevas e inesperadas, como el Zoombombing.

2. El uso de servicios de vídeo como YouTube, Netflix, SchoolTube, KhanAcademy, etc. es cada vez mayor. La tendencia es la creación de más videos educativos que circularán como producto terminado o que serán utilizados por los educadores. De hecho, el 87% de los profesores utiliza contenidos de vídeo en el aula. Los videos pueden ser una poderosa herramienta educativa, pero las plataformas más populares también albergan una gran cantidad de contenido inapropiado para menores, y los creadores de este contenido podrían usar temas educativos para llamar la atención hacia su material. Este no es un riesgo nuevo, pero con el aumento de la digitalización su relevancia también crecerá.

3. Uso de herramientas de redes sociales en el proceso educativo. Las redes sociales (Instagram, Twitter, etc.) son un excelente instrumento para promover la participación de los estudiantes durante y después de clases, y también ayudan a que los profesores se conecten con sus estudiantes. Pero existen amenazas vinculadas a su contenido: comentarios ofensivos, contenido inapropiado, ciberacoso... La privacidad es otro punto para considerar, ya que es posible comprometer datos personales a través de aplicaciones o servicios mal configurados, incluso sin necesidad de usar instrumentos o vulnerabilidades especiales. Y tanto estudiantes como profesores pueden ser víctimas de este tipo de ataques.

> "Comprender los riesgos a los que nos exponemos y proteger nuestros dispositivos resulta clave"

4. Introducción de juegos en el proceso educativo. Casi todos los estudiantes ya saben que se puede aprender mucho con Minecraft, pero también hay muchos otros servicios que permiten aprender jugando (While True: Learn, Classcraft, Roblox...). Por desgracia, tan pronto como se incorporan juegos en el aula, se expone a los estudiantes a los mismos riesgos que enfrentarían si jugaran desde casa: trolls, bullying, archivos peligrosos que se hacen pasar por actualizaciones y complementos del juego, etc.

Otro frente que tampoco se puede olvidar proteger son las redes públicas, muy habituales en las universidades, y uno de los grandes vectores de ataque en este tipo de instituciones. Al tratarse de redes que no requieren autenticación para establecer una conexión, el ciberdelincuente puede posicionarse entre el usuario y el punto de conexión y obtener acceso sin restricciones a los dispositivos sin protección que se conecten.

También se pueden utilizar las conexiones Wi-Fi públicas no seguras para distribuir malware. Al compartir archivos a través de una red, el hacker puede introducir fácilmente software infectado en el equipo. En algunos casos, incluso han conseguido piratear el punto de conexión, lo que hace que aparezca una ventana emergente durante el proceso de conexión que ofrece una actualización de un software conocido. Cuando se hace clic en la ventana, se instala el malware.

Comprender los riesgos a los que nos exponemos en todos estos casos y proteger nuestros dispositivos resulta clave, y más en aquellos en los que los usuarios son menores, ya que en muchos casos se comparten los dispositivos móviles (ordenadores, tabletas, móviles) con los hijos, por lo que la información guardada en los mismos (contraseñas, números de tarjeta o incluso información de la empresa) puede también estar en riesgo. ■

GLOBAL KNOWLEGDE

EXPERTOS EN FORMACIÓN VIRTUAL AVANZADA

Descubre nuestros cursos y certificaciones oficiales impartidos por instructores acreditados, de la mano de los principales partners del sector.

¡TE ASESORAMOS!

info.cursos@globalknowledge.es

91 425 06 60

Global Knowledge™

a skillsoft company

ALCATEL-LUCENT ENTERPRISE: creando un mundo donde todo se conecta

Alcatel-Lucent Enterprise es un proveedor de soluciones de red, comunicaciones y nube del mundo que, con modelos de negocio flexibles en la nube, en las instalaciones y en entornos híbridos, ofrece tecnología que conecta todo y a todos.

Desde la compañía se apuesta por nuevas y mejores formas de trabajar juntos, para que las personas se comuniquen y colaboren de forma más eficaz. Todas sus soluciones se adaptan a las necesidades de cada organización, sea cual sea su tamaño, con seguridad integrada y un impacto medioambiental limitado.

PRESENCIA GLOBAL, REPUTACIÓN MUNDIAL

Más de 100 años de innovación han convertido a Alcatel-Lucent Enterprise en un socio para más de 1.000.000 de clientes en todo el mundo. Con sede en Francia y 3.400 partners comerciales en todo el mundo, Alcatel-Lucent Enterprise logra un alcance global efectivo con un enfoque local.

UN MUNDO DE SOLUCIONES INTELIGENTES

Alcatel-Lucent Enterprise proporciona soluciones de redes, comunicaciones y nubes de la

era digital específicas para cada sector, y aplicaciones y servicios para empresas de todos los tamaños en todo el mundo.

Al ofrecer la flexibilidad de la nube, en las instalaciones y en entornos híbridos, los clientes pueden elegir soluciones que se adaptan a sus necesidades y a sus objetivos empresariales.

❖ **Soluciones de comunicaciones de la era digital.** Soluciones de comunicación nativa, abierta, adaptable y duradera con alta escalabilidad y configurabilidad:

➤ Experiencia del usuario de telefonía centrada en la eficiencia, facilidad y productividad en tiempo real.

➤ Soluciones de colaboración flexible (en la nube/en las instalaciones / híbridas) con capacidad para integrar aplicaciones de terceros.

❖ **Soluciones de redes de la era digital.** Las redes autónomas y los flujos de trabajo automatizan las operaciones de red de misión crítica y mejoran la experiencia del usuario. Incorporación, gestión y seguimiento seguros de IoT para ayudar a ampliar la digitalización. Todo ello, con la certificación completa de ISO 9001 e ISO 27001.

❖ **Soluciones específicas por sectores:** La experiencia en los principales sectores y mercados ofrece a la compañía una perspectiva completa sobre lo que necesitan las diferentes empresas y organizaciones para transformar las redes y la comunicación digitales. Por ello, cuentan soluciones particularizadas para los sectores hotelero, de salud, de transporte, educativo o Administraciones Públicas. El objetivo de la firma es ofrecer soluciones tecnológicas que marcan la diferencia, conectando personas, máquinas, entidades y procesos, y creando un futuro más sostenible para todos. ■

MÁS INFORMACIÓN

- Alcatel-Lucent Enterprise
- Triunfar en la nueva forma de trabajar desde cualquier lugar y en todas partes (por IDC)
- Plataforma de comunicaciones Alcatel-Lucent Rainbow
- Arquitectura distribuida de la infraestructura de red de Alcatel-Lucent Enterprise
- SPB para vigilancia por vídeo
- Ciberseguridad en el campus educativo en la era de IoT y del RGPD

Una propuesta para cada necesidad

Son muchos los escenarios a asegurar y, por ello, la propuesta de ESET pasa por ofrecer una solución para cada necesidad. Conozcamos algunas de ellas.

❖ **ESET NOD32 Antivirus.** Se trata de una defensa esencial contra el malware con un mínimo consumo de recursos. Protege de todo tipo de amenazas digitales tales como virus, ransomware, rootkits, gusanos y software espía. También protege de las amenazas más sofisticadas especialmente diseñadas para evitar su detección, y neutraliza los ataques dirigidos y los exploits. Proporciona protección de páginas web ilegítimas que intentan obtener información privada, como datos de usuario y contraseñas.

❖ **ESET Internet Security.** Añade más seguridad para datos y familia. Protege el acceso a la banca online y recupera el control del router Wifi y la webcam. Además, protege a la familia con el Control Parental.

❖ **ESET Smart Security Premium.** La seguridad más completa, diseñada para los usuarios que lo quieren todo. Protege contra el robo de datos en caso de pérdida o robo del USB o el ordenador portátil, y, además, protege de forma remota el historial de navegación.

❖ **Mobile Security.** Seguridad móvil en cualquier parte. Protege el móvil o tablet y la información de

las crecientes amenazas en Android. Asimismo, permite recuperarlo con la función Anti-robo.

❖ **Parental Control.** Protección para los más pequeños y sus actividades online para que puedan disfrutar de una tecnología segura.

❖ **ESET Protect Essential.** Solución de ciberseguridad para la empresa con consola de administración en la nube. Proporciona protección multicapa contra el ransomware, ataques dirigidos y sin archivo. Ofrece seguridad con el mejor equilibrio entre detección, rendimiento y falsos positivos. Garantiza la visión a tiempo real de los endpoints, elaboración de informes y gestión de la protección para todos los sistemas operativos con la consola en la nube ESET Protect.

❖ **ESET Protect Entry.** Solución de ciberseguridad para la empresa con un nivel extra de seguridad: protección para los servidores desde la consola de administración en la nube. Proporciona protección multicapa para dispositivos y servidores contra ataques de ransomware, ataques dirigidos y sin archivo, amenazas avanzadas, ataques de red, botnets, o antispam. Permite la visualización global desde la consola de administración en la nube ESET Protect.

❖ **ESET Protect Advanced.** Solución para un nivel de ciberseguridad empresarial más avanzado con administración basada en la nube. Proporciona protección a la red de equipos y servidores de archivos contra ransomware, amenazas avanzadas y amenazas zero-day. Asegura los datos con el cifrado completo del disco y administra todo de forma fácil desde la consola en la nube ESET Protect.

❖ **ESET Secure Business Cloud.** Solución que busca un alto nivel de protección del servidor de correo y de todos los dispositivos de la empresa con administración basada en la nube. Proporciona protección evitando ataques de red, phishing, malware, ransomware, ataque sin archivo y filtra el spam para evitar el correo no deseado. Elimina las amenazas que se transmiten mediante el correo electrónico al servidor de correo. Avanzada tecnología que combina velocidad, precisión y un bajo consumo de recursos. Permite la personalización y control desde la consola de administración en la nube ESET Protect.

❖ **ESET Protect Complete.** Solución de protección completa para empresa que, además, mantiene seguras las aplicaciones de Microsoft 365 con administración basada en la nube. Proporciona máxima protección para la red de equipos, servidores, correo electrónico no deseado, de las aplicaciones de la empresa en la nube, contra todo tipo de amenazas: ransomware, avanzadas, día cero y malware; también protege tus datos con el cifrado de disco completo y todo administrado desde la consola en la nube ESET Protect.

❖ **ESET Protect Mail Plus.** Solución que protege las comunicaciones por correo electrónico con espacio seguro basado en la nube. Protege la empresa de los ataques de red y ofrece protección

directamente a través del servidor antes de llegar a las cuentas de correo de los usuarios, filtra los mensajes de correo no deseado, además de brindar seguridad frente a las amenazas persistentes avanzadas y amenazas día cero. Todo administrado desde la consola en la nube ESET Protect.

❖ **ESET Cloud Office Security.** Solución de protección avanzada para el correo, sharepoint y almacenamiento de Microsoft 365. Su combinación de filtrado spam, antimalware, antiphishing, escaneo y detección de páginas fraudulentas ayuda a proteger la comunicación, las aplicaciones y almacenamiento de la empresa en la nube además puede inspeccionar los objetos que están en cuarentena. ■

MÁS INFORMACIÓN

RANSOMWARE: Un vistazo al arte criminal de los códigos maliciosos

Tendencias en Ciberseguridad 2021

Una apuesta por el desarrollo de las habilidades que el profesional necesita

Global Knowledge – A Skillsoft Company, es la empresa centrada en la formación tecnológica y TI que ayuda a las personas y organizaciones a desarrollar las habilidades necesarias para triunfar en un mundo en constante cambio y evolución. Fundada en 1995, Global Knowledge cuenta con más de 1.500 empleados en todo el mundo y colabora en el éxito de más de 200.000 profesionales cada año.

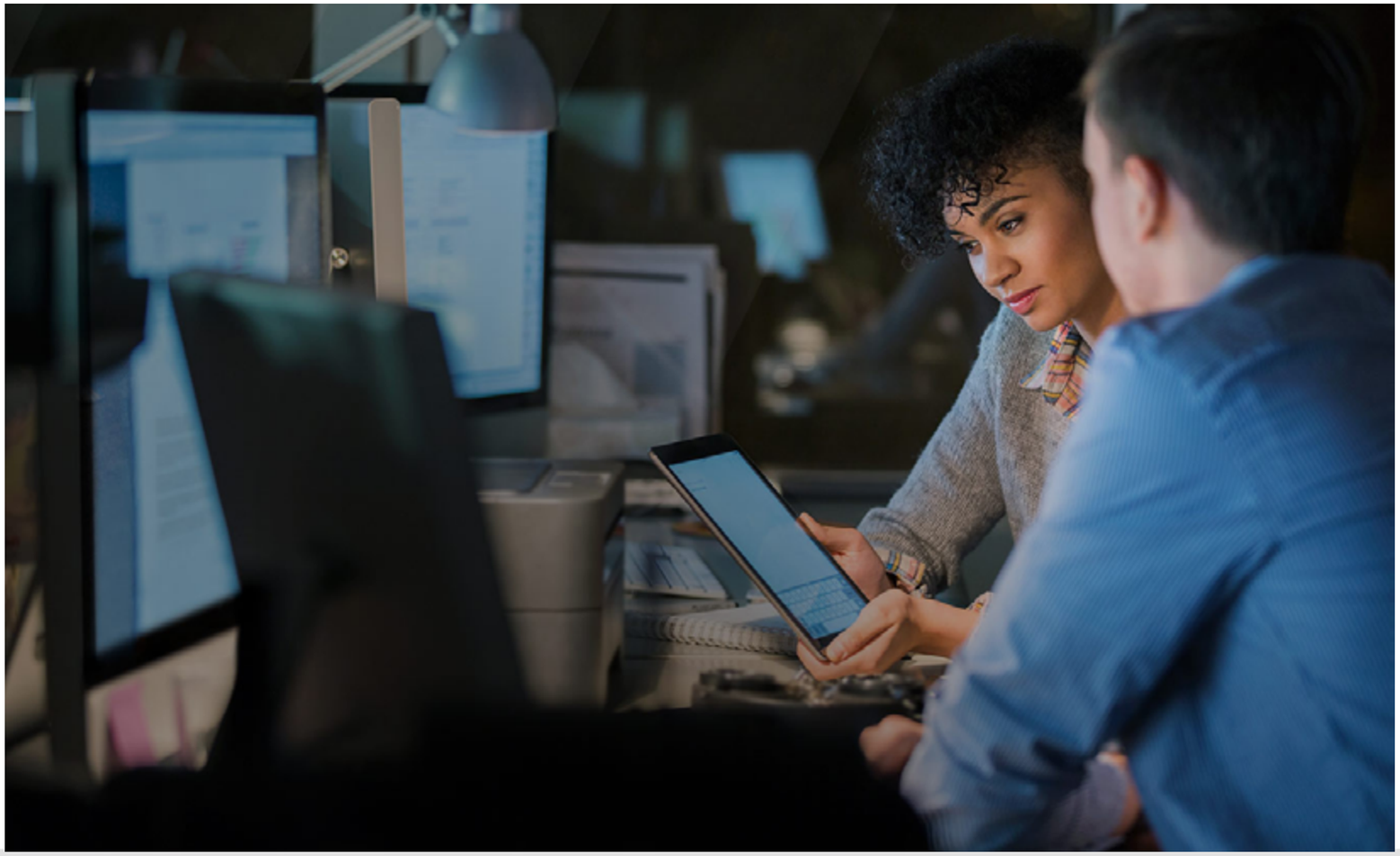
Con una amplia red internacional de oficinas y centros formativos, Global Knowledge dispone de capacidades y recursos para ofrecer una amplia oferta de formación, tanto en modalidad presencial como en formato online y virtual, a través de su red mundial de partners oficiales.

Algunos números que definen a Global Knowledge en la actualidad son:

- Más de 5.000 clases garantizadas al año.
- Más de 3.000 cursos de IT exclusivos.
- Más de 1.100 instructores de prestigio y reconocimiento profesional.
- El nivel de satisfacción general del alumno es de 95%.
- Es partner oficial de formación autorizado de compañías como Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Cisco, Citrix, IBM, ITIL, Red Hat, VMware...
- Cuenta con formación en más de 100 países.

Con una red internacional de oficinas e instalaciones de formación, Global Knowledge tiene la flexibilidad de ofrecer una amplia cartera de cursos, en aulas y a través de una red mundial de socios. Gracias a las diferentes modalidades de formación, Global Knowledge ofrece la posibilidad de formarse:

❖ **Clases presenciales.** Se ofrecen formaciones en persona, impartidas por expertos en la



La firma se centra en ayudar a las organizaciones a construir una fuerza laboral preparada, capacitada y con las destrezas necesarias para los puestos de trabajo del futuro

materia, que ponen lo último en equipamiento y tecnología a disposición del alumno.

❖ **Formato virtual.** El alumno aprovecha las formaciones con instructor en directo y le permite participar durante la sesión e interaccionar con el resto de asistentes de manera telemática.

❖ **Cursos on demand.** Se puede acceder de la forma más flexible a los vídeos formativos y actividades cualquier día, a cualquier hora, y en cualquier lugar, adaptándose a los horarios y necesidades de cada alumno.

Global Knowledge facilita los recursos necesarios para formar a todos los perfiles profesionales del sector tecnológico, y proporcionando soluciones de aprendizaje innovadoras y flexibles que preparan para el éxito. Todo ello, impulsado por el alto nivel de calidad que se impone en la compañía, manteniendo rigurosos estándares internos, para que el alumno reciba una experiencia de formación única y excepcional en todo momento.

Además, en junio de 2021, Global Knowledge se fusiona con Skillsoft para salir a bolsa y convertirse en empresa pública en Estados Unidos, creando así una empresa de formación corporativa con un amplio alcance global, para servir a, aproximadamente el 70 % de los clientes de la lista Fortune 1000, en más de 160 países y con más de 45 millones de estudiantes a nivel mundial. De esta manera, Skillsoft se posiciona como una de las empresas de digital learning más grandes de la industria, enfocada en ayudar a las organizaciones a construir una fuerza laboral preparada, capacitada y con las destrezas necesarias para los puestos de trabajo del futuro. ■

MÁS INFORMACIÓN

- Calendario de cursos
- Cursos garantizados
- Actualidad de Global Knowledge
- Salary Report 2020

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)

Una visión 360 de la seguridad

WatchGuard Technologies es una multinacional con 25 años de experiencia en el desarrollo de tecnología para el sector de la ciberseguridad. Cuenta con una oferta que combina tanto hardware como software, permitiendo crear un escudo de defensa en las organizaciones gracias a una propuesta integral que abarca desde la seguridad de red hasta la protección avanzada para el endpoint e inteligencia de red, así como la seguridad Wi-Fi y autenticación multifactor (MFA).

El objetivo de WatchGuard es hacer que la seguridad de nivel empresarial sea accesible a las organizaciones de todos los sectores y tamaños, a través de la simplicidad, ofreciendo seguridad inteligente y eficaz bajo la fórmula de soluciones fáciles de desplegar y gestionar.

Con 7 centros de operaciones y presencia directa en 21 países, WatchGuard permite a más de 250.000 clientes de todo el mundo proteger sus activos más importantes.

La compañía cuenta con un catálogo de soluciones que abarca desde los servicios de seguridad de red tradicionales hasta los más innovadores como protección contra malware avanzado, ransomware y pérdida de datos confidenciales, o servicios Zero-Trust.

El objetivo de WatchGuard es hacer que la seguridad de nivel empresarial sea accesible a las organizaciones de todos los sectores y tamaños, a través de la simplicidad, ofreciendo seguridad inteligente y eficaz bajo la fórmula de soluciones fáciles de desplegar y gestionar

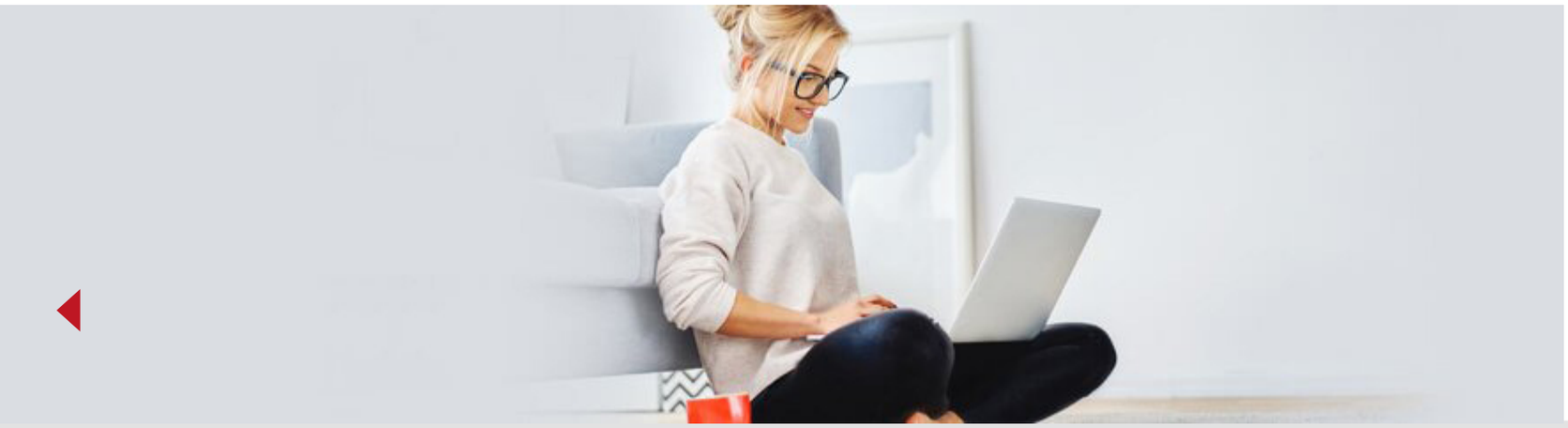
Por áreas, su propuesta se estructura de la siguiente manera:

❖ **Seguridad de red:** todos los servicios de seguridad de WatchGuard se ofrecen como una solución integrada en un dispositivo Firebox, tanto en entornos físicos como virtuales. Los Firebox destacan por su escalabilidad y están preparados para brindar el abanico completo de servicios de seguridad, junto con un conjunto de herramientas de visibilidad y gestión que permiten estar un paso por delante del panorama de amenazas.

❖ **Wi-Fi seguro con gestión en cloud:** con Secure Wi-Fi ofrecen conectividad Wi-Fi y seguridad patentada. Implementando un punto de acceso WatchGuard con Wi-Fi Cloud habilitado y una licencia de Secure Wi-Fi o Total Wi-Fi, se despliega todo el potencial de los puntos de acceso WatchGuard mediante un Sistema de Prevención de Intrusiones Inalámbricas (WIPS). Asimismo, WIPS garantiza la protección que cada usuario necesita, defiende el espacio aéreo 24x7 contra equipos no autorizados, ataques MitM y DoS, AP no autorizados y el resto de amenazas que acechan a los entornos Wi-Fi.

❖ **Protección de identidades:** la solución de MFA, AuthPoint, aporta la seguridad necesaria para proteger activos, cuentas e información, permitiendo que las empresas y sus trabajadores accedan de forma segura y sin preocupaciones a las aplicaciones corporativas desde cualquier lugar. Sencilla de manejar, se administra de forma centralizada desde WatchGuard Cloud.

❖ **Seguridad endpoint:** WatchGuard Endpoint Security ofrece las tecnologías necesarias para detener los ciberataques avanzados a los endpoints, incluyendo antivirus de nueva generación en la plataforma de protección de endpoints (EPP), detección y respuesta de endpoints (EDR) y soluciones de filtrado DNS. La solución insignia EPDR brinda protección EPP y EDR completa, así como servicios de búsqueda de amenazas o threat hunting y aplicaciones zero-trust, suministrados a través de un único agente ligero y gestionados desde una única plataforma cloud. ■



MÁS INFORMACIÓN

- WatchGuard Endpoint Security
- WatchGuard Total Security: Suscripciones a UTM
- MFA Poderosamente Sencilla

SOPHOS: Nuevas tendencias para potenciar la seguridad

Impulsada por la threat intelligence, IA y machine learning de SophosLabs y SophosAI, Sophos ofrece un catálogo de productos y servicios avanzados para proteger a los usuarios, las redes y los endpoints contra el ransomware, malware, exploits, phishing y la amplia gama de ciberataques.

Sophos proporciona una única consola cloud de gestión integrada, Sophos Central, como pieza central de un ecosistema de ciberseguridad adaptativo que cuenta con un data lake centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, partners, desarrolladores y otros fabricantes de ciberseguridad.

La firma vende sus productos y servicios a través de partners resellers y managed service providers (MSP) en todo el mundo, unas soluciones entre las que destacan:

❖ **Sophos Inercept X EDR/XDR.** Un sistema de protección endpoint que engloba la protección tradicional (firmas), junto con protección "next-gen" (Inteligencia Artificial, anti exploit, comportamiento, anti ransomware y anti-hacking) así como protecciones complementarias (control web, control de aplicaciones, cifrado, DLP...) y, por supuesto, EDR o, a día de hoy, XDR, gracias a la integración cruzada de datos con nuestros firewalls y sistemas de protección cloud. Su gestión se realiza a través de Sophos Central, lo que permite la interacción con otros productos de Sophos y gracias a su API, con cualquier fabricante.

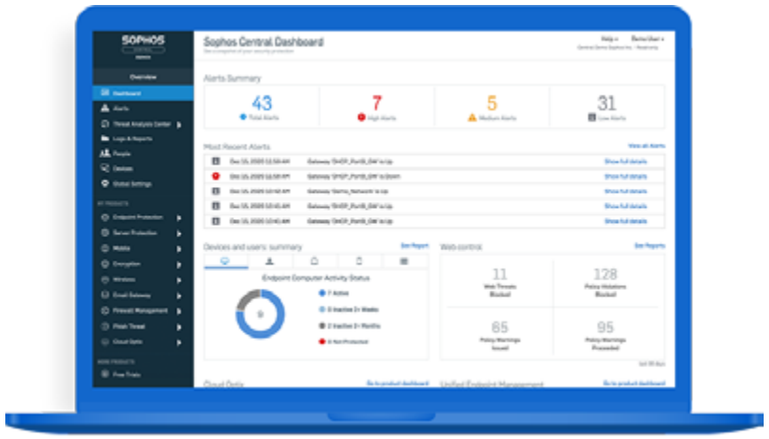
❖ **Sophos MTR, MTR-E y Rapid Response.** Se trata de un servicio gestionado de Respuesta frente a Amenazas, que ofrece a las

Sophos proporciona una única consola cloud de gestión integrada, Sophos Central, como pieza central de un ecosistema de ciberseguridad adaptativo que cuenta con un data lake centralizado que aprovecha un amplio conjunto de API abiertas

empresas funciones de búsqueda, detección y respuesta ante posibles amenazas 24/7. Formado por un equipo de detección de amenazas y profesionales expertos en dar respuesta, tomando medidas para neutralizar incluso las amenazas más sofisticadas. Sophos puede dar respuesta, apoyándose en el agente de Sophos para realizar las acciones oportunas para la detección y mitigación de la amenaza. Cualquier empresa que sufra un ataque activo puede recurrir a Sophos Rapid Response: un despliegue de productos y un equipo de expertos capaces de ver cuál es la situación dentro de la compañía, detener el ataque, si es posible, y detectar cómo ha venido, a quién ha afectado y limpiar para que pueda operar lo antes posible.

❖ **Sophos Firewall.** La seguridad de red desde la compra de Astaro en 2008 por Sophos ha seguido evolucionando hasta llegar a los modernos Sophos Firewall, gestionados de forma centralizada desde Sophos Central, integrándose con el Endpoint y servicios como MTR así como hidratando el lago de datos para permitir detectar, englobándose dentro de su estrategia XDR. La arquitectura de Xstream de Sophos Firewall protege la red de las amenazas más recientes al tiempo que acelera el tráfico importante de SaaS, SD-WAN y aplicaciones en la nube.

❖ **Sophos Email.** Seguridad del correo electrónico más inteligente con IA. Las actuales amenazas para el correo electrónico evolucionan rápidamente, y las empresas en expansión necesitan una seguridad predictiva para el email, es decir, que combata las amenazas de hoy día sin perder de vista el mañana.

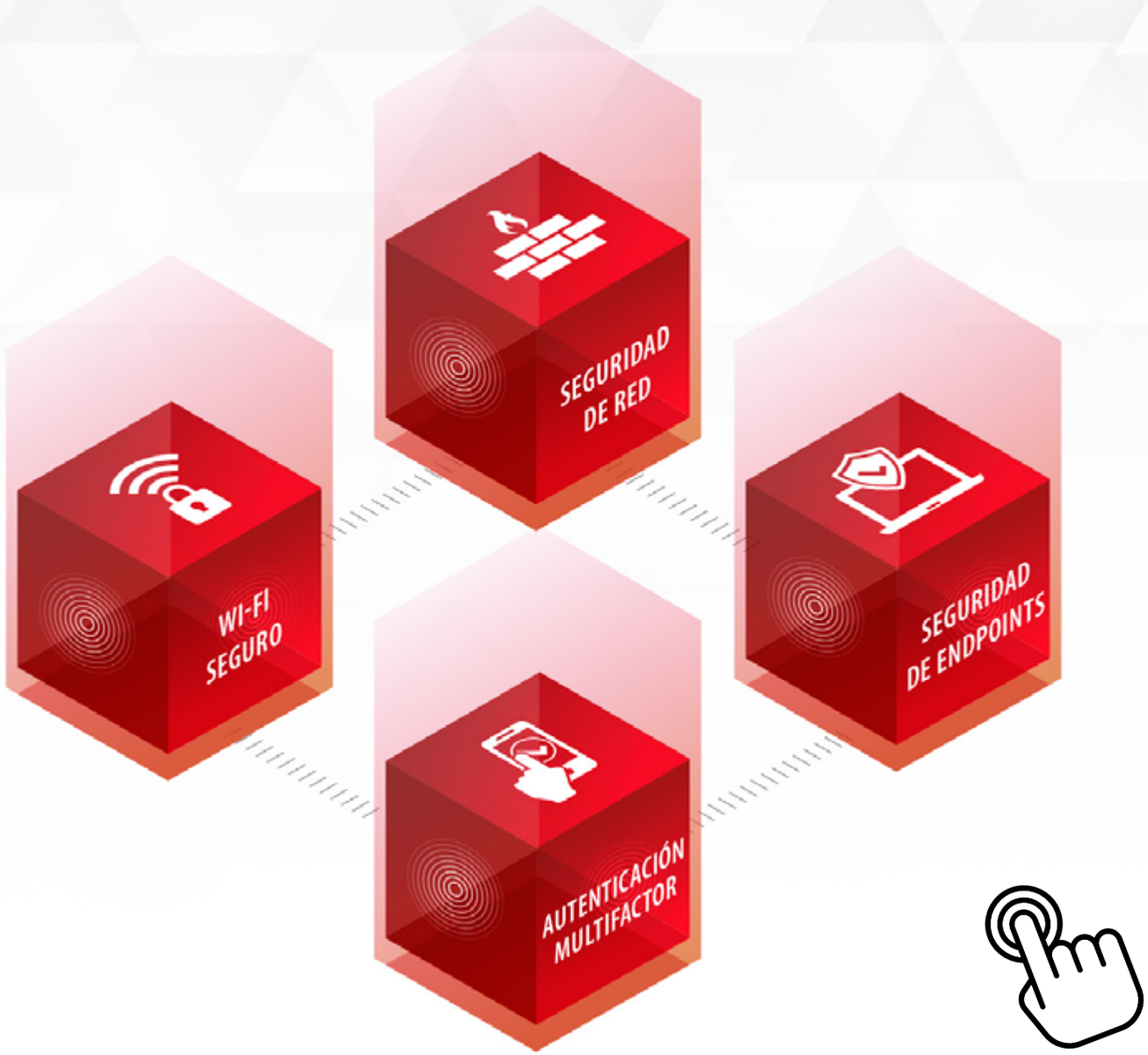


❖ **Sophos Cloud Optix**. Conscientes de que la TI está migrando a la nube, Sophos empezó a hablar de CSWP y CSPM, gracias tanto al agente para servidores como a Cloud Optix, el cual audita los recursos que tengamos sobre proveedores de nube pública como AWS, Azure, Google Cloud o Kubernetes tanto en cualquiera de estos entornos como locales. Además, se integra tanto con la protección de instancias y servicios como MTR, lo que proporciona más visibilidad e información que será recogida en el DataLake. ■

MÁS INFORMACIÓN

- El estado del Ransoware
- El estado del Ransoware en Educación
- Sophos XG Firewall para la educación

SMART SECURITY, SIMPLY DONE.



SEGURIDAD DE RED • AUTENTICACIÓN MULTIFACTOR • WI-FI SEGURO • SEGURIDAD DE ENDPOINTS

900 90 70 80

spain@watchguard.com

PROTECCIÓN INTELIGENTE

Múltiples servicios trabajan juntos de manera inteligente para prevenir, detectar y responder instantáneamente a los ciberataques con políticas automatizadas, así como supervisar e informar sobre el estado de tu infraestructura de TI.

VISIBILIDAD ACCIONABLE

Las herramientas de visibilidad accionable te permiten identificar amenazas de manera proactiva, al tiempo que proporcionan acciones correctivas contra los problemas conocidos.

GESTIÓN SIMPLIFICADA

Nuestra plataforma de gestión basada en la nube despliega, configura y mantiene tu seguridad de forma rápida y sencilla en múltiples productos de seguridad, empresas y sitios.

PIONEROS EN CIBERSEGURIDAD DURANTE 25 AÑOS.

25 ANNIVERSARY WatchGuard®