byte TI

Nº 331 | Noviembre 2024

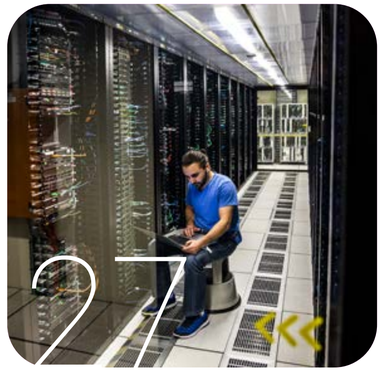
¿Cuál es el impacto real de IoT

Gobierno IT: privacidad y cumplimiento normativo

Gestión de riesgos: medidas de ciberseguridad en NIS 2

COMPARATIVA
Servicios de detección y respuesta de amenazas

mkm PUBLICACIONES



N.º 331 | ÉPOCA IV
Edita: Publicaciones Informáticas MKM
Noviembre 2024.

MKM PUBLICACIONES
Managing Director
Ignacio Sáez (nachosaez@mkm-pi.com)

BYTE TI
Director
Manuel Navarro (mnavarro@mkm-pi.com)

Redacción
Vanesa García (vgarcia@revistabyte.es)

Coordinador Técnico
Regina de Miguel

Colaboradores
J. Palazón, I. Pajuelo, O. González, M. López, F. Jofre, A. Moreno, Mª J. Recio, JJ. Flechoso, D. Puente, A. Herranz, C. Hernández.

Fotógrafos
P. Varela, E. Fidalgo

Diseño de portada
María Torre

Diseño y maquetación
María Torre

REDACCIÓN
Avda. Adolfo Suárez, 14 – 2º B
28660 Boadilla del Monte. Madrid
Tel.: 91 632 38 27 / 91 633 39 53
Fax: 91 633 25 64
e-mail: byte@mkm-pi.com

DEPARTAMENTO COMERCIAL
Directora comercial: Isabel Gallego (igallego@mkm-pi.com)
Account Manager: Laura Sierra (lsierra@mkm-pi.com)
Tel.: 91 632 38 27

DEPARTAMENTO DE EVENTOS Y COMUNIDAD
Coordinadora: María Vicente (mvicente@mkm-pi.com)
Tel. 91 632 38 27

SUSCRIPCIONES
e-mail: suscripciones@mkm-pi.com

Revista mensual de informática
ISSN: 1135-0407

Depósito legal: B-6875/95

Carta del Director

Manuel Navarro Ruiz
Director de BYTE TI

¿Tiene Ayuso capacidad para alimentar tanto centro de datos?

Según diferentes "radiografías", España se está convirtiendo en un polo de atracción de centros de datos. Tanto si nos fijamos en el informe de El País como en el de D+I de El Español que los sitúa en casi un centenar, se llega a la conclusión de que somos un país muy atractivo para esta industria. Se trata, en principio, de una buena noticia ya que atrae inversiones, impacta positivamente en la creación de empleo y fomenta el desarrollo empresarial. Sin embargo: ¿Tenemos capacidad energética para tanto centro de datos?

Ambos estudios señalan a la Comunidad de Madrid como la región en la que se acumula la mayor concentración de data centers y, aunque Cataluña ocupa la segunda posición, es Aragón la que en un futuro superará a ambas. La clave de este crecimiento hay que encontrarla en que es una de las comunidades con mayor capacidad de generación de energía renovable en España.

Sin embargo, Madrid, carece de esas capacidades generadoras. Se trata de una región que depende en gran medida de la importación de electricidad debido a su alta demanda y su casi nula capacidad de generación. A pesar de esto, la atracción de empresas para instalar los centros de datos es una prioridad para el Gobierno que preside Isabel Díaz-Ayuso, que desde que comenzó a gobernar vio que la digitalización debía ser un factor diferencial para hacer crecer a la región.

Esa apuesta tiene innumerables ventajas, pero también presenta diferentes retos. Seis CCAA en España tienen saldo positivo de generación de electricidad. Por contra, el resto gasta más de lo que produce. Así que la pregunta es ¿qué ocurriría si, como ha sucedido con Aragón, esas comunidades con saldo positivo comienzan a apostar también por la inversión en centros de datos? ¿Podría Madrid alimentar los que ya tiene? A día de hoy, Madrid no tiene ya capacidad para absorber la demanda de energía, pero eso es un problema al que no sólo va a tener que hacer frente esta región. Ya ocurre en otras partes del mundo. Seguramente, la solución se encuentre en la energía nuclear. No me extrañaría ver a la presidenta madrileña presentar un proyecto para desarrollar una planta nuclear en Madrid. Seguramente, contará con el apoyo de la todavía Ministra de Transición Ecológica, Teresa Ribera, que recientemente ha cambiado de opinión sobre dicha energía.

Actualidad

Acronis MSP Global 2024 proyecta un gran crecimiento del sector

Acronis ha reunido esta semana en PortAventura (Tarragona), a toda la comunidad MSP Global. En esta ocasión, el día previo al evento, los medios tuvimos la oportunidad de asistir a su Partner Day, con una mesa redonda que contó con la participación de varios líderes de la compañía.

Por Vanesa García. Port Aventura.

Entre ellos Ezequiel Steiner (CEO), Kevin Reed (CISO), Alona Geckler (SVP Business Operations), y Denis Cassinerio (Senior Director y GM de varias regiones), que dieron a conocer el estado actual de la empresa, sus avances en el sector, las tendencias del futuro de los MSPs y el nivel de inclusión femenina en la industria tecnológica.

Actualizaciones de Acronis en 2024

La empresa ha lanzado importantes novedades este año, destacando su solución de Extended Detection and Response (XDR), que amplía su capacidad más allá de la protección de endpoints. Además, anunciaron un crecimiento del 90% en cargas de trabajo protegidas y un incremento del 18% en la cantidad de socios.

Otro hito importante fue la adquisición de una participación mayoritaria de Acronis por parte de EQT, con el objetivo de acelerar la expansión de la plataforma. También se destacó la expansión de sus centros de datos, con nuevas instalaciones en México, Brasil y Berlín, impulsando la estrategia de cumplimiento local y ciberprotección integrada.

Crecimiento global y en EMEA

A nivel global, Acronis experimentó un crecimiento del 43% en sus facturaciones en la nube (ARR), mientras que sus cargas de trabajo facturables llegaron a los 6 millones. En la región EMEA, hubo un aumento del 91% en las cargas de trabajo avanzadas de EDR, con un crecimiento de clientes del 23,21%. La empresa cuenta con 23 centros de datos en esta región, con un nuevo centro a ser inaugurado en Berlín.

Perspectiva de los MSPs hacia 2030

Se proyecta un crecimiento significativo en la industria para el año 2030, con un aumento del 75% en el mercado de servidores, un incremento del 119% en endpoints, y un crecimiento del 48% en los centros de datos. Factores como la transformación digital, el uso de la inteligencia artificial

Acronis MSP Global 2024 proyecta un gran crecimiento del sector

(IA), y la automatización impulsarán estos cambios, creando un entorno más complejo con una mayor superficie de ataque para ciberamenazas.

A medida que el número de pequeñas y medianas empresas (SMEs) que utilizan MSPs aumenta, se estima que el coste de los ataques cibernéticos para estas empresas alcanzará los 8,4 billones de dólares.

Unidad de Investigación de Amenazas

Kevin Reed, CISO de Acronis, explicó cómo la empresa aborda los desafíos de seguridad, centrándose en la investigación de vulnerabilidades, inteligencia de amenazas y análisis forense. La compañía proporciona información diaria sobre vulnerabilidades y amenazas específicas para los MSPs, mejorando la capacidad de sus clientes para responder a los ciberataques. Reed destacó la importancia de parches, gestión de configuración, detección de malware y copias de seguridad como medidas fundamentales para combatir las amenazas modernas.

Amenazas cibernéticas en EMEA y la directiva NIS2

Denis Cassinerio destacó la evolución de las ciberamenazas en Europa: Mientras que el ransomware tiende a estabilizarse, las detecciones de malware y URLs maliciosas han aumentado considerablemente, con Italia y España experimentando las mayores subidas en detecciones de malware. Por su parte, en Alemania, las amenazas de ransomware persisten, mientras que Bulgaria ha visto un fuerte incremento en ataques basados en URLs maliciosas.

Cassinerio también abordó la Directiva NIS2, que establece medidas de gestión de riesgos de ciberseguridad para proveedores de servicios esenciales en la UE. Esta normativa entrará en vigor en 2024 y se centrará en incidentes de seguridad, protección de redes, y gestión de riesgos en la cadena de suministro. De este modo, la directiva resalta la necesidad de adoptar tecnologías innovadoras, como la IA, para mejorar la prevención de ciberataques.

Resultados de la encuesta FOMO

Por su parte, Alona Geckler presentó los resultados de una encuesta que explora los desafíos que enfrentan las mujeres en la ciberseguridad. El 71% de las encuestadas mencionó que trabajan más horas para progresar en sus carreras, y el 70% cree que los hombres son promovidos más rápidamente que las mujeres.

La encuesta también revela que el 84% de las mujeres en el sector tecnológico piensan que la inclusión de más mujeres en roles de liderazgo sería beneficiosa para las organizaciones tecnológicas. Además, se observó que la mentoría, la equidad salarial y las oportunidades de desarrollo profesional son cruciales para empoderar a las mujeres en esta industria.

Actualidad

Telefónica lanza Network Slicing 5G para empresas

Telefónica Empresas ha mejorado su servicio de Movistar Intranet al incorporar la capacidad de Network Slicing. Con esta actualización, Telefónica se convierte en el primer operador en España en ofrecer una conectividad móvil privada de alta calidad extremo a extremo. Esto permite a las empresas y entidades públicas acceder a sus redes corporativas de manera segura y en movimiento, sin necesidad de estar conectados a la red fija de la oficina.

El servicio no solo facilita la interconexión entre usuarios y dispositivos con conectividad móvil 5G a través de la red Movistar, sino que también permite la creación de redes privadas seguras (VPN) para dispositivos móviles. Esto es especialmente útil en situaciones de alta demanda o cuando se necesita optimizar las comunicaciones con nuevas tecnologías que requieren mayor movilidad o menor latencia.

La red 5G Stand Alone de Telefónica ofrece mayores velocidades, la capacidad de conectar más dispositivos, latencias más bajas y la funcionalidad de network slicing. Esta capacidad es ideal para casos de uso como el teletrabajo en entornos congestionados, la gestión de flotas de vehículos conectados y la conectividad de cajeros automáticos en eventos masivos.

Adrián García Nevado, director de Empresas de Telefónica España, destaca que estamos en una era de movilización continua de consumidores y empleados conectados, lo que exige accesos a redes y protección de datos de forma constante y simultánea.

Network Slicing 5G

Movistar Intranet es una solución económica que no requiere despliegues adicionales y que integra dispositivos móviles en la red corporativa, facilitando el tráfico seguro a través de la red móvil de Telefónica. La funcionalidad de network slicing optimiza el uso de recursos y mejora la experiencia del usuario en situaciones de alta demanda.

Actualmente, 800 clientes han contratado dos millones de líneas con el servicio Movistar Intranet. Network Slicing, apoyado en el 5G de Telefónica, ya cubre el 89% del país y asegura una conectividad de altas prestaciones.

Manuel Lopez

Neomanía: la novedad obsoleta

La sociedad vive inmersa en una vorágine de novedades tecnológicas. La neomanía, esa obsesión enfermiza por lo nuevo, se ha convertido en un problema social. La velocidad vertiginosa del avance tecnológico nos ha convertido en adictos a la actualización constante. La digitalización de la sociedad del siglo XXI ha acelerado este proceso. Somos bombardeados constantemente con novedades, y la sensación de obsolescencia nos acecha en cada esquina. La IA, la realidad virtual, el metaverso, ... cada nueva tendencia nos promete un futuro mejor, pero nos deja anclados en un presente de constante búsqueda de lo último, convirtiéndonos en consumidores compulsivos.

¿Cómo sobrevivir en este mundo de Neomaníacos? La respuesta no está en resistirnos al cambio, sino en aprender a gestionarlo. Debemos cultivar la capacidad de discernir entre lo verdaderamente útil y lo que es simple ruido, ya que puede ser la clave para escapar de la rueda de la neomanía. Además, es fundamental desarrollar un pensamiento crítico que nos permita cuestionar las tendencias y no dejarnos arrastrar por ellas ciegamente, de forma que podamos tomar decisiones más conscientes y construir un futuro tecnológico más sostenible y humano. Pasemos de “Neomaníacos” a “Pragmaníacos”.

Actualidad

La visión computacional revolucionará la Industria 4.0

La visión computacional se basa en la captura de imágenes a través de cámaras, videos o fotografías para analizar y obtener información de manera similar a la visión humana.

Esta tecnología supera las capacidades humanas en varios aspectos, como el uso de cámaras térmicas y la obtención de imágenes a nivel microscópico. Los sistemas de visión artificial, potenciados por la computación en la nube, son útiles para la verificación de identidad, la moderación de contenido, el análisis de transmisiones de video y la detección de errores, entre otros.

"En Bosch, como pioneros en Industria 4.0, vemos la visión computacional como un pilar fundamental de la Industria 4.0 y estamos comprometidos a integrar esta tecnología para crear fábricas más inteligentes, seguras y eficientes. No solo ayudará a las empresas en su tarea de digitalización, si no que poco a poco, permitirá que muchos de aquellos procesos que son largos, monótonos y aburridos, se hagan de manera rápida y automatizada" destaca Juan Antonio Relaño Pinilla, responsable de tecnología e innovación de Robert Bosch España.

El CIO de Bosch destaca seis áreas donde la visión computacional transformará el futuro de la industria:

Control de calidad e inspección: Los sistemas de visión computacional pueden inspeccionar productos en las líneas de montaje con rapidez, detectando defectos que el ojo humano podría pasar por alto. Esto asegura una calidad casi perfecta, reduce desperdicios y mejora la satisfacción del cliente. Bosch utiliza robots con el sistema APAS, que combina robótica flexible y procesamiento de imágenes para realizar inspecciones automáticas.

Mantenimiento predictivo: Integrando la visión computacional en sensores IoT, se logra un mantenimiento predictivo avanzado. Los sistemas de inspección visual monitorean constantemente los equipos, detectando señales tempranas de desgaste o fallos, lo que minimiza el tiempo de inactividad y optimiza los programas de mantenimiento.

Colaboración máquina-humano: Esta tecnología facilita una colaboración fluida entre humanos y máquinas en las fábricas. Los robots con visión computacional se adaptan a los movimientos humanos en tiempo real, garantizando una cooperación segura y eficiente, aumentando la productividad y creando un entorno de trabajo más seguro.

Optimización de la cadena de suministro: La visión computacional transforma la cadena de suministro al proporcionar visibilidad en tiempo real de los inventarios, automatizando el conteo de productos y generando alertas instantáneas sobre el stock. Esto mejora la logística, reduce errores y aumenta la eficiencia general.

Mejora de la seguridad en el trabajo: Los sistemas de visión avanzada juegan un papel crucial en la protección de los empleados, detectando peligros potenciales y alertando a los supervisores sobre situaciones riesgosas, creando un entorno laboral más seguro y con menos accidentes.

Actualidad

En tres años todas las empresas tendrán un responsable de rendimiento

En los próximos tres años, todas las empresas con presupuestos superiores a 200 millones de euros anuales en tecnología de la información tendrán un responsable de rendimiento. Esto se debe a los ahorros significativos, entre un 15% y un 30%, que esta función puede aportar a los costos tecnológicos del negocio. Un estudio de Orizon revela que reducir los costes tecnológicos es una prioridad para el 88% de los responsables de TI. Esto se debe a la creciente desconfianza de los directivos sobre el valor real de la tecnología y el constante aumento de sus costos.

La migración a entornos complejos como la nube ha generado sobrecostos inesperados de alrededor del 45% en los presupuestos tecnológicos, y cerca del 80% de las organizaciones no ha alcanzado los objetivos previstos. En el sector bancario español, las 10 principales entidades han duplicado su gasto tecnológico desde 2015, y se espera que supere los 6.600 millones de euros en 2025.

El 40% de las empresas ya acuden al rendimiento

El 40% de las empresas ya ha comenzado a integrar profesionales dedicados a la gestión del rendimiento, bajo títulos como “responsable de proyectos especiales” o “responsable de proyectos TI para TI”. Estos profesionales se centran en asegurar que las infraestructuras y aplicaciones tecnológicas funcionen correctamente y cumplan con los objetivos establecidos, ya sea internamente o a través de proveedores, y al costo previsto. Orizon señala que la creación de esta función es crucial para contener los sobrecostos, aunque el 85% de estos nuevos responsables mencionan la complejidad y volatilidad de los sistemas como el principal obstáculo para alcanzar sus objetivos. La solución, según Orizon, radica en el uso de herramientas de big data, analítica avanzada e inteligencia artificial para detectar, analizar y corregir fallos en toda la cadena tecnológica. Además, las organizaciones solo podrán optimizar sus costos si disponen de una visión unificada de la tecnología del negocio.

FERNANDO JOFRE

NIS2: no esperemos al legislador

Ya pasó el 17 de octubre, y aquí seguimos sin una transposición nacional de la directiva europea. Aun sin tener un marco legislativo propio, ya es vinculante. Como referentes, podemos adecuarnos a certificaciones y estándares como la ISO 27001 o al ENS. Al menos cumpliendo con estos estándares tendremos protocolizados procedimientos y rutinas orientadas a minimizar los riesgos, y mejoraremos los tiempos de respuesta para retomar la capacidad operativa. Pero tampoco estaremos inmunes a ataques. No es cuestión únicamente de prepararnos con medidas adecuadas, sino de asegurarnos de que también lo están haciendo nuestros proveedores.

Según Fortinet es necesario evaluar los riesgos de seguridad; realizar un inventario preciso de activos y procesos; documentar evaluaciones y puntuaciones de riesgo; mantener una postura de seguridad continua; proteger la cadena de suministro; implementar soluciones seguras por diseño; designar a los responsables y siempre notificar incidentes significativos en un plazo máximo de 24 horas, con informes detallados en 72 horas y un mes; incorporar medidas anti ramsomware; adoptar enfoques de confianza cero en la arquitectura de red y fomentar la colaboración y un enfoque integral en ciberseguridad.

Actualidad

Salesforce mejora la IA empresarial con Agentforce y su red de partners

La Inteligencia Artificial (IA) y la automatización están transformando la manera en que las marcas interactúan con sus clientes. Así lo destaca un estudio reciente de Salesforce, donde revela que el 84% de los CIOs consideran que la IA será tan crucial para sus negocios como lo fue Internet en su momento. Sin embargo, solo el 11% ha implementado completamente esta tecnología, enfrentándose a desafíos técnicos y organizativos, principalmente en seguridad e infraestructura de datos. Salesforce, con su reciente lanzamiento de Agentforce, está bien posicionada para ayudar a las empresas en este proceso, ofreciendo la posibilidad de construir agentes autónomos sobre su plataforma CRM.

“Vemos muchas aplicaciones atractivas de los LLM, pero estos suelen utilizar información genérica de Internet, lo que puede reproducir sesgos y errores”, comenta Gonzalo Goñi, Director de Ingeniería de Soluciones de Salesforce. “Agentforce integra la IA de manera precisa en cada empresa, utilizando datos específicos del CRM, lo que mejora significativamente la relevancia de sus respuestas”.

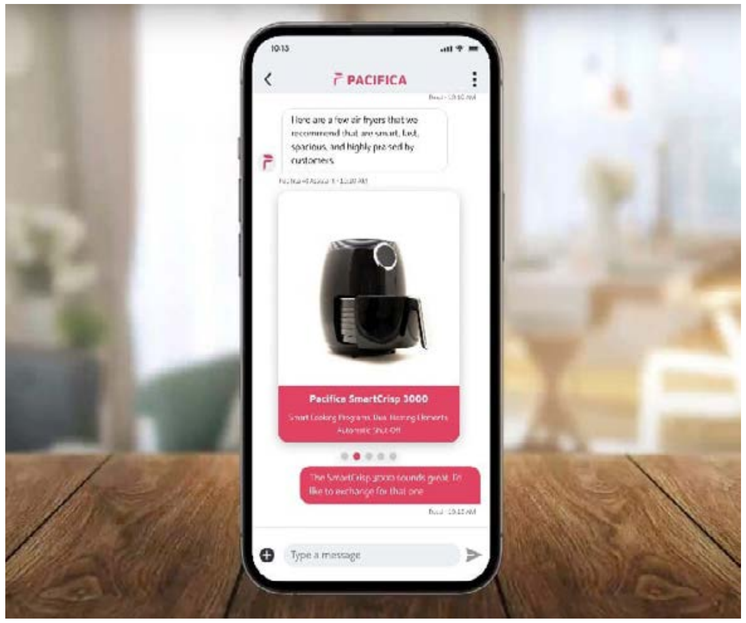
Ecosistema de Partners

Salesforce ha lanzado la Agentforce Partner Network, el primer ecosistema para agentes autónomos de IA, compuesto por empresas como Workday, Amazon Web Services, Box, Certinia, Copado, Coupa, Google, Honeywell, IBM, Zoom y NVIDIA.
Este ecosistema permite a los clientes acceder a agentes pre-diseñados a través de la App "Exchange", el marketplace de Salesforce, y ofrece funcionalidades adicionales para personalizar los agentes según las necesidades de cada negocio.

“Nuestra red de partners es fundamental, y en esta tercera ola de la IA, necesitamos apoyarnos en ellos para llevar a nuestros clientes al siguiente nivel”, señala Marta González, Directora de Ventas de Alianzas y Partners de Canal. “Estas alianzas permiten a los equipos crear y personalizar sus propios agentes. Nuestros partners españoles jugarán un papel clave en la introducción de Agentforce en el mercado nacional”.

Transformación Basada en Datos

Agentforce representa el futuro de la IA, respondiendo a las demandas de las empresas que buscan competir en el mercado digital. Con ella, las empresas combinarán su personal especializado con agentes autónomos capaces



de gestionar tareas de servicio, ventas, marketing y comercio, aumentando la eficiencia y permitiendo a los empleados centrarse en tareas de mayor valor.

En sectores con picos estacionales, como el turismo, los agentes autónomos pueden gestionar eficientemente las solicitudes de información y cambios en reservas, evitando la necesidad de contratar y formar personal temporal.

Actualidad

Fujifilm lanza en España su nueva serie de Impresoras Multifunción Apeos

Fujifilm Spain ha anunciado la introducción en el mercado español de su nueva serie de impresoras multifunción de alta calidad, Apeos. Esta serie, desarrollada por FUJIFILM Business Innovation Corp, ya se lanzó con éxito en Italia y Reino Unido en abril. La llegada a España representa un paso más en su expansión por Europa, con planes de lanzamiento en otros países.

FUJIFILM Business Innovation es el principal proveedor de impresoras multifunción A3 en la región de Asia-Pacífico, con millones de dispositivos en uso en oficinas de todo el mundo. Hasta abril de este año, estos productos no estaban disponibles en Europa bajo la marca Fujifilm. “Es emocionante entrar en el mercado europeo de impresoras de oficina después de nuestro éxito en el negocio de impresoras de producción de tóner en Europa desde 2021”, comentó Taku Ueno, vicepresidente Senior de la División de Tecnología de Dispositivos de FUJIFILM Europa. “El lanzamiento de nuestras impresoras de oficina es el siguiente paso natural tras la introducción exitosa de impresoras de producción de alta calidad con la marca Fujifilm”.

Apeos: nuevas impresoras multifunción

La serie Apeos de impresoras multifunción A3 está diseñada para satisfacer las necesidades de productividad, fiabilidad y seguridad del entorno laboral moderno. Estas impresoras destacan por su facilidad de uso, seguridad mejorada y operatividad rápida y sencilla, apoyando así el éxito de los usuarios en Europa.

Con décadas de experiencia en impresión e imagen, Fujifilm ha creado la serie Apeos para el lugar de trabajo contemporáneo. Estas impresoras ofrecen capacidades de impresión remota y móvil, funciones de seguridad avanzadas y credenciales de sostenibilidad excepcionales, apoyando la transformación digital y adaptándose a las demandas del entorno de oficina post-Covid.

Joan Casas, Director General Adjunto de Fujifilm España S.L., añadió: “Estamos orgullosos de la amplitud y calidad de nuestros productos y servicios. La tecnología de impresión de tóner seco y el desarrollo de soluciones de impresión de oficina han sido fundamentales para Fujifilm, y ahora poder ofrecer impresoras de oficina directamente en el mercado español es un gran beneficio para nuestros clientes y muy emocionante para nosotros”.

Características principales de la serie Apeos

- **Calidad:**
  - Resolución de impresión de 1200 x 2400 ppp.
  - Tecnología IReCT para ajuste digital de la imagen.
  - Manejo versátil de soportes con velocidades de 20 a 70 páginas por minuto.
- **Seguridad:**
  - Validación de seguridad BLI.
  - Protección contra accesos no autorizados.
  - Protección sólida de datos.
- **Usabilidad / Fiabilidad:**
  - Operaciones rápidas sin tiempo de espera.
  - Flexibilidad en la distribución de la oficina.
  - Conectividad con dispositivos móviles.
  - Interfaz de usuario sencilla y luz de atención.
- **Sostenibilidad:**
  - Tecnologías IH para reducir el consumo de energía.

Actualidad - Te interesa

Por qué libros de texto y tabletas deben coincidir en el aula

Por Raúl Sanahuja, responsable de comunicación en Epson Ibérica

Atrás quedaron los días de libros de texto polvorientos y pizarras chirriantes. Las aulas de hoy están llenas de pantallas interactivas, portátiles y una amplio abanico de herramientas digitales. Aunque no cabe duda de que la tecnología ofrece posibilidades apasionantes para el aprendizaje, un movimiento creciente insta a la comunidad educativa, en general, a replantearse el enfoque único de la tecnología en las aulas.

Un reciente estudio de Epson puso de relieve que una gran dependencia de las herramientas digitales -en concreto, portátiles y tabletas- puede provocar lagunas en el aprendizaje. En la actualidad, el 49% de docentes en España cree que los portátiles y las tabletas pueden tener un efecto perjudicial en el aprendizaje. A pesar de ello, los responsables políticos de todo el mundo siguen impulsando la innovación digital y la inteligencia artificial en las escuelas. La cuestión a la que la comunidad educativa debe dar respuesta es: ¿hacia dónde nos dirigimos?

Entender la evolución del panorama y crear una solución que lo respalde empieza por comprender qué opinan las personas más cercanas sobre el impacto de la tecnología en la educación.

Por supuesto, las mejoras tecnológicas en la educación han hecho la vida más fácil al alumnado. En comparación con una pila de cuadernos, una tableta o un portátil son relativamente ligeros. Por otro lado, la tecnología también ha dificultado las cosas al profesorado que se ve a menudo desbordado por una pesada carga de trabajo y tiene que adaptarse a las nuevas tecnologías. Algunos centros han implantado herramientas para controlar y restringir el uso de la tecnología, pero pueden ser engorrosas y llevar mucho tiempo, lo que les deja atrapados entre «enseñar o actuar como guardias de prisión».

Lograr el equilibrio adecuado

La solución no es prescindir por completo de la tecnología, sino encontrar el equilibrio adecuado. De hecho, el 88% de docentes y familias en nuestro país han observado un impacto positivo del uso de libros de texto y hojas

de trabajo tradicionales en las aulas. Más de dos tercios (69%) de los profesores afirman que mejoran la capacidad de lectura, mientras que el 52% de docentes -y el 43% de las familias- afirman que los materiales impresos permiten retener mejor los conocimientos.

Estos resultados concuerdan con la creciente evidencia académica que sugiere que el alumnado aprende mejor en papel que en pantallas individuales. studios de instituciones como el Instituto Karolinska de Suecia han puesto de relieve que las herramientas digitales, aunque beneficiosas en algunos contextos, a menudo perjudican el aprendizaje.

Ahora existe una oportunidad para el cambio. La creciente tensión entre el uso de la tecnología en casa y en la escuela ha llevado a reclamar una estrategia más cohesionada, en la que las herramientas digitales no se consideren un sustituto del aprendizaje tradicional, sino un complemento. Se trata de reequilibrar los recursos digitales y en papel para las aulas. Al reequilibrar los recursos, los educadores pueden reducir el tiempo dedicado a supervisar y gestionar las herramientas digitales, lo que les permite centrarse en lo más importante: la enseñanza.

Además, la comunidad docente puede adaptarse mejor a los distintos estilos de aprendizaje: el 46% de los profesores y el 43% de las familias está de acuerdo en que el uso de materiales impresos ayuda más a los alumnos diversos. La tecnología siempre tendrá un lugar en las aulas, pero no debe ser la única. Tomemos como ejemplo la introducción de las calculadoras en los años ochenta, a pesar de la preocupación de que el alumnado pudiera fracasar en el aprendizaje de las matemáticas. Era una tecnología que mejoraba el aprendizaje sin comprometer el dominio de las destrezas fundamentales por parte del alumnado.

El reto, por tanto, consiste en equilibrar la innovación con prácticas pedagógicas basadas en la evidencia. Todo ello debe basarse en los conocimientos de quienes están en primera línea de la educación. Tanto las familias como el profesorado ven a menudo los efectos de primera mano de las políticas destinadas a modernizar la educación y sus opiniones, ahora más que nunca, deben tenerse en cuenta.

Equilibrio entre tecnología y educación

Las prisas por adoptar la tecnología en la educación han creado un movimiento pendular, dejando algunas aulas sin el equilibrio esencial entre los materiales de aprendizaje digitales y tradicionales. Es importante recordar que el objetivo no son sólo aulas equipadas digitalmente, sino alumnado alfabetizado digitalmente, sin olvidar los métodos de enseñanza probados. Por eso, la comunidad educativa debe invertir en la tecnología adecuada que complemente los métodos tradicionales, como impresoras de alta calidad y pantallas interactivas. Responsables políticos, profesionales de la enseñanza y fabricantes de tecnología deben trabajar juntos para garantizar que la tecnología mejore el aprendizaje, no que lo dificulte.

Si adoptamos un enfoque equilibrado, podemos crear un sistema educativo que dote a los y las estudiantes de las herramientas que necesitan para el futuro, no sólo en lo relativo a la competencia digital, sino también a sólidas competencias básicas y de una profunda comprensión que se deriva de la interacción con materiales tradicionales.

Aunque seguirá habiendo incertidumbres en torno a la tecnología en la educación y muchas preguntas para las que aún no tenemos todas las respuestas, una cosa está clara: los libros de texto y las tabletas tienen cabida en el mismo aula; solo tenemos que encontrar el equilibrio adecuado.

Actualidad - Te interesa

El IPCEI-CIS avanza hacia la Soberanía Digital de Europa

Por Sara Madariaga. Head of Arsys Lab

Puesto en marcha hace menos de un año, el Proyecto Importante de Interés Común Europeo de Infraestructura y Servicios en la Nube de Nueva Generación (conocido por su acrónimo en inglés IPCEI-CIS) es la gran iniciativa de la Unión Europa para crear un ecosistema europeo que facilite el tratamiento y explotación del dato por parte de las empresas y fortalezca la competitividad europea y la digitalización.

Sólo tres empresas españolas participan directamente en este proyecto y una de ellas es el proveedor cloud Arsys, que está ultimando el primer gran hito de sus desarrollos para el IPCEI-CIS. Sara Madariaga, Head of Arsys Lab, el departamento de innovación que coordina la participación de la compañía en este proyecto europeo, nos explica cómo está avanzando Arsys en los primeros meses del IPCEI-CIS.

¿Cómo está evolucionando el IPCEI-CIS?
Aunque estamos hablando de un proyecto de I+D que se extenderá hasta 2031, todos los participantes tenemos un calendario individual de hitos que estamos alcanzando y dan paso a las siguientes fases del proyecto, ya que esta iniciativa tiene un fuerte componente de coordinación internacional y avances habilitadores. En noviembre, alcanzaremos uno de los hitos que tenemos previsto desde Arsys, crucial para el buen rumbo de este proyecto: la definición del estándar de monitorización de centros de datos que se propondrá para todo el IPCEI-CIS.

¿En qué consiste exactamente este sistema de monitorización de centros de datos?
Aunque haya muchos indicadores comunes (PUE, WUE, CADE, etc.), no existe un estándar para monitorizar un centro de datos. Nosotros, en Arsys, por ejemplo, monitorizamos alrededor de 1.200 señales del datacenter.

Eso se debe a que en la monitorización de centros de datos se suelen utilizar desarrollos ad hoc, que captan toda la complejidad de las instalaciones, pero no están estandarizados ni se pueden replicar fácilmente, dos características que necesitamos para este proyecto.

¿Por qué es importante este hito y cómo va a ayudar al proyecto?
El estándar de monitorización que utilizaremos

Actualidad - Te interesa

El IPCEI-CIS avanza hacia la Soberanía Digital de Europa

en el IPCEI-CIS simplificará la contratación de servicios IT y será un sistema abierto e interoperable, encaminado hacia la seguridad y la sostenibilidad, por lo que acelerará la adopción de las soluciones de procesamiento de datos. Así las empresas que accedan a este ecosistema podrán comparar más fácilmente métricas de estas instalaciones en términos de rendimiento y disponibilidad, pero también de sostenibilidad o cumplimiento normativo, factores clave en el proyecto y en la digitalización de las empresas.

En el horizonte más cercano, este hito, además, pondrá en marcha otras iniciativas en las que trabajamos en este proyecto, como el gemelo digital del centro de datos.

¿Cuáles son esas iniciativas que estáis desarrollando en Arsys para el IPCEI-CIS?
Estamos trabajando en tres grandes áreas de innovación muy interrelacionadas: una plataforma que unifique cloud y edge computing a nivel de capacidad técnica; un sistema que permita utilizar todo el potencial de esta plataforma para desarrollar aplicaciones de datos; y por último, un gemelo virtual de un centro de datos, para mejorar el rendimiento y sostenibilidad de estas instalaciones. Estas iniciativas cuentan con el apoyo del Plan de Recuperación, Transformación y Resiliencia, a través de una ayuda de Estado de 8,4 millones de euros, y tenemos previsto finalizarlas en 2026, aunque continuaremos involucrados en el IPCEI-CIS en sus siguientes etapas.

¿Y cómo estáis abordando estas iniciativas desde Arsys?
En Arsys nos pusimos a trabajar en el IPCEI-CIS desde el primer día. Tenemos un equipo multidisciplinar dedicado en exclusiva a este proyecto, con un jefe de proyecto y 8 especialistas altamente cualificados de distintos perfiles técnicos: administradores de sistemas, desarrolladores, ingenieros… Además, están colaborando otras áreas de Arsys: comercial, marketing, financiero, jurídico o RRHH. Es un trabajo conjunto, porque somos conscientes de que estamos embarcados en el diseño y el desarrollo de la nube europea del futuro.

Más información de la participación de Arsys en el IPCEI-CIS: arsys.es

Webinars BYTE TI

Retención de Clientes: Estrategias de Intelligent CX

La lealtad de los clientes está en declive, así lo demuestra la actualidad global y el entorno altamente competitivo en el que nos encontramos en estos momentos. Esta tendencia al alza puede ser revertida, pero muchas marcas aún no saben cómo hacerlo. Estamos presenciando un cambio significativo en diversas áreas de la sociedad, con consumidores que están alterando sus hábitos de compra, lo que complica la planificación de marketing.

Además, los nuevos perfiles de consumidores y sus patrones de compra exigen modelos de negocio mucho más innovadores y tecnologías más avanzas. Y es que, ya es un hecho que las marcas que continúan operando de manera tradicional, corren el riesgo de perder cuota de mercado y, eventualmente, desaparecer.

Para hablar sobre esto, desde BYTE TI hemos organizado un webinar en colaboración con Emilio Osete, CEO de Digiu Digital, centrado en cómo retener clientes, así como las mejores formas de lanzar mensajes consistentes y relevantes en diversas plataformas, acelerar el tiempo de valor, llegar a los clientes en momentos clave con interacciones personalizadas o gestionar el tráfico web y crear contenido individual, entre otras cosas.

La importancia de la Retención de Clientes

La retención de clientes es una estrategia esencial para cualquier empresa que busque maximizar su rentabilidad y eficiencia operativa. Emilio Osete destaca que retener a un cliente es significativamente más económico que adquirir uno nuevo. Y es que, según varios estudios, adquirirlo puede ser hasta 25 veces más costoso que retenerlo, “Esto se debe a que la adquisición de clientes requiere una inversión considerable en marketing y ventas. En cambio, la retención de clientes permite a las empresas maximizar la rentabilidad al reducir los costos asociados con la adquisición”, explica.

De la misma manera, existen fórmulas específicas para medir estos costos, como el Customer Acquisition Cost (CAC) y el Customer Retention Rate (CRR). “Estas métricas ayudan a las empresas a entender mejor el impacto financiero de sus estrategias de retención y adquisición”.

Además, la fidelización de clientes no solo se trata de mantener a los clientes actuales, sino también de convertirlos en defensores de la marca que recomienden los productos o servicios a otros. Por ello, “ganar un cliente es hasta 25 veces más caro que retenerlo”, afirma Osete.

Webinars BYTE TI

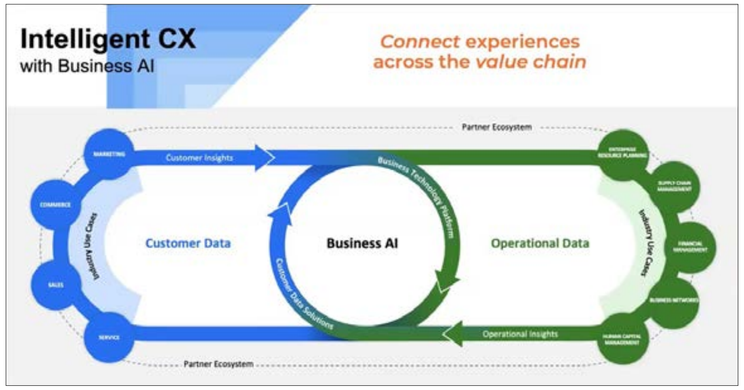
Retención de Clientes: Estrategias de Intelligent CX

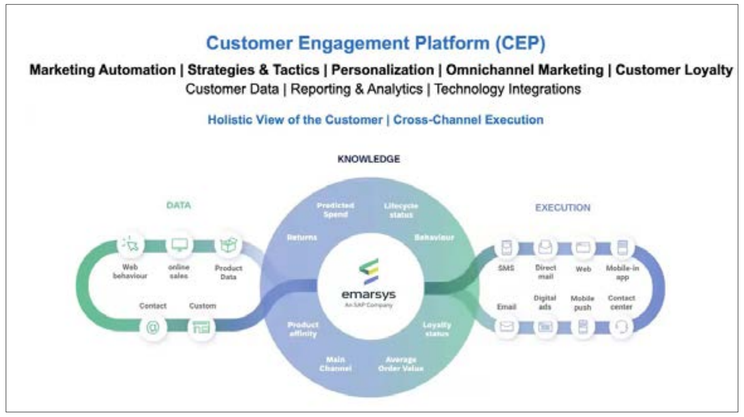
Desafíos a tener en cuenta

Uno de los principales desafíos en la retención de clientes es la personalización. Osete menciona la paradoja de la personalización, donde las empresas deben equilibrar la personalización con la privacidad del cliente. Ejemplos como el algoritmo de Netflix, nos muestra cómo las empresas pueden personalizar la experiencia del cliente sin comprometer su privacidad, “hoy en día todo el mundo dice que la personalización es el rey, y entonces siempre tenemos un debate que surge también entre personalización y privacidad”.

Otro desafío es el exceso de comunicación. Las empresas a menudo bombardean a los clientes con mensajes constantes, lo que puede resultar en una sobrecarga de información y una experiencia negativa. Osete sugiere que las empresas deben buscar formas más sutiles y naturales de interactuar con los clientes, como lo hace Apple Watch con sus sugerencias de actividad física. “Hay que buscar estrategias que lo que hagan es precisamente influirte, pero de una manera mucho más sutil”.

La fatiga del feedback es otro problema común. Los clientes a menudo se sienten abrumados por las constantes solicitudes de encuestas y feedback. Para mitigar esto, Osete recomienda integrar herramientas de feedback de manera más fluida en la experiencia del usuario, como





los sistemas de satisfacción en los baños de los aeropuertos. “La única manera que tenemos para competir esto es buscar herramientas que nos permita introducirlo de una manera mucho más sencilla”, explica.

Estrategias de Fidelización

Para abordar estos desafíos, existen varias estrategias de fidelización. Una de ellas es la creación de programas de fidelización más dinámicos y atractivos. Utilizando el ejemplo de los retos de fitness de Apple Watch, CEO de Digiu Digital expone cómo las empresas pueden hacer que sus programas de fidelización sean más divertidos y atractivos para los clientes. “Te plantea retos que cambian en los meses o con personas o en aniversarios o en cosas así, que lo que hacen es que sea más divertido”.

Adicionalmente, la atención al cliente inconsistente también es un problema que afecta la retención de clientes. Osete subraya la importancia de tener una atención al cliente centralizada y eficiente. “Las plataformas tecnológicas pueden ayudar a las empresas a gestionar mejor la atención al cliente y asegurar que los clientes reciban un servicio de alta calidad en todo momento. Normalmente hay pocas compañías que tengan una atención al servicio muy centralizada”, comenta Osete.

Herramientas de Intelligent CX

Durante el webinar, Osete presentó la herramienta Emarsis Customer Engagement de SAP, diseñada para mejorar la retención y fidelización de clientes. Esta plataforma permite a las empresas personalizar la experiencia del cliente a través de múltiples canales, como email, móvil y web. Asimismo, integra inteligencia artificial (IA) para ofrecer recomendaciones personalizadas y optimizar las campañas de marketing.

De esta forma, Emarsis es una herramienta fácil de usar, diseñada para que los departamentos

de marketing puedan operarla sin necesidad de intervención del departamento de IT. La plataforma ofrece más de 60 escenarios predefinidos y utiliza IA para proponer tácticas y estrategias basadas en los datos generados por las campañas. “Es una herramienta pensada para departamentos de marketing, para poder de verdad cambiar”.

Casos de Éxito

Para ilustrar el impacto de Emarsis, Osete detalla varios casos de éxito: Por ejemplo, Puma utilizó Emarsis para personalizar sus campañas de recuperación de carritos abandonados, logrando una mayor conversión de ventas. Pizza Hut también implementó Emarsis para personalizar sus programas de puntos y mejorar la retención de clientes.

“Han utilizado 11 tácticas predefinidas en Emarsis para generar modelos personalizados para poder recuperar o captar ese tipo de ventas”, explica.

Otro caso destacado fue el de una empresa de moda que automatizó sus campañas de marketing en todos los canales utilizando Emarsis. Esto les permitió crear experiencias personalizadas y aumentar la eficiencia de sus campañas de marketing. “Es un caso muy de éxito porque han logrado la capacidad de automatizarlo en todos los canales y cambiar un poco la idea y el paradigma de cómo operaban en el departamento de marketing”.

Impacto de la IA en la Retención de Clientes

La inteligencia artificial juega un papel crucial en la retención de clientes, y es que, la IA puede analizar grandes volúmenes de datos para identificar patrones y tendencias en el comportamiento del cliente. Esto permite a las empresas personalizar sus estrategias de marketing y ofrecer experiencias más relevantes a los clientes. “La inteligencia artificial te puede dar muchísimo, porque la capacidad que tiene es inmensa, no podemos ni siquiera medirla”, reitera.

Además, la IA puede ayudar a las empresas a optimizar sus campañas de marketing en tiempo real. Por ejemplo, Emarsis utiliza IA para ajustar automáticamente el contenido y el momento de envío de los emails, asegurando que los mensajes lleguen a los clientes en el momento más adecuado. “La capacidad que tiene la inteligencia artificial de favorecer y de poder darnos lo que se llaman insights o soluciones va a ser inmensa”, concluye Osete.

Desayunos BYTE TI

Gobierno IT. Privacidad y cumplimiento normativo

La privacidad y el cumplimiento normativo, es un aspecto fundamental para tener un buen Gobierno IT en cualquier organización. Para hablar sobre ello, Byte TI, junto con HCL y DataDog, organizaron un encuentro que contó con la participación de David Caballero, CIO de Kymatio; Manuel Asenjo, CIO de Broseta; José Luis Berrocal, EMEA security sales leader de HCL Software; Carlos Castells, CIO de Serban; Daniel Damas, head of IT assurance de Nationale-Nederlanden; Alejandro Expósito, CIO de Servatrix; Jaime Alonso, sales engineering manager de DataDog e Ildefonso Vera, director de transformación digital de Isdefe.

Implementar políticas robustas de privacidad y cumplir con el conjunto de normativas exitentes, proteger los datos sensibles para fortalece la confianza de los clientes son sólo algunos de los aspectos que deben tenerse en cuenta en un buen gobierno de las TI. Una correcta estrategia reducirá el riesgo de sanciones legales a la vez que mejorará la continuidad del negocio y fomentará una cultura de responsabilidad y transparencia. En este sentido tanto DataDog como HCL Software son dos firmas que están ayudando a las organizaciones a desarrollar una correcta estrategia de Gobierno IT. La primera de ellas es una una plataforma SaaS de monitoreo, observabilidad y análisis que ofrece una visión unificada de la infraestructura y las aplicaciones, permitiendo a las empresas supervisar el rendimiento y la seguridad en tiempo real. De esta forma, ayuda a las empresas a cumplir con las normativas existentes e implementa medidas de seguridad avanzadas para proteger los datos sensibles.

Desayunos BYTE TI

Gobierno IT. Privacidad y cumplimiento normativo

Alejandro Expósito
CIO de Servatrix

Carlos Castells
CIO de Serban

Daniel Damas
head of IT assurance de Nationale-Nederlanden

David Caballero
CIO de Kymatio

Por su parte, HCL Software, es la división del gigante indio HCL. En el apartado del Gobierno IT, su propuesta incluye soluciones que aseguran el cumplimiento de las diferentes regulaciones. Además, implementan sistemas para identificar, evaluar y mitigar riesgos relacionados con el incumplimiento normativo y desarrollan tecnologías avanzadas para proteger datos sensibles y garantizar la privacidad de la información.

Ambas compañías están ayudando a sus clientes a adaptarse a una realidad en la que el cumplimiento de las legislaciones empieza a ser cada vez más complejo. Tal y como explicó Ildefonso Vera, director de transformación digital de Isdefe, “o nos adaptamos o afectará a la productividad de las empresas. Tenemos cambios constantes prácticamente todos los meses, por lo que hay que estar atentos a las nuevas llamadas y a lo que sale en el mercado. Los departamentos internos de IT deben encargarse de gestionar servicios. En nuestro caso, estamos trabajando en tres direcciones: asegurar la continuidad de negocio, asegurar datos de clientes y proveedores y una tercera linea que es la seguridad de la información, porque cada vez se manejan más datos.

Alejandro Expósito, CIO de Servatrix, afirmó que en el caso de su compañía, “tenemos una ventaja y es que somos una spinoff de la Universidad Autónoma y está todo por hacer, lo cual es una ventaja ya que no tienes que adaptarte y no hay un legacy. La mentalidad tenemos tienen sobre el control o el Gobierno IT es que la ciberseguridad y la protección de los datos deben formar parte del ADN de la compañía”.

La diferencia entre las formas de operar de las empresas quedó muy clara desde el principio. Por ejemplo, y tal y como expuso Daniel Damas, head of IT assurance de Nationale-Nederlanden, “nuestra idiosincrasia es totalmente diferente a la que tienen otras firmas. Por ejemplo, en nuestro caso estamos completamente regulados. Y eso provoca que nos adelantemos a lo que pueda venir. Esto es algo que, por ejemplo, estamos haciendo con la NIS2 actualmente. El Gobierno todavñia no ha transpuesto la directiva a la legislación española, pero queremos estar preparados para cuando lo haga, así que lo que hemos hecho es adaptarnos a la IS27000”.

Encuentros BYTE TI

Gobierno IT. Privacidad y cumplimiento normativo

Ildefonso Vera
director de transformación digital de Isdefe

Jaime Alonso
sales engineering manager de DataDog

José Luis Berrocal
EMEA security sales leader de HCL Software

Manuel Asenjo
CIO de Broseta

Carlos Castells, CIO de Serban, explicó que sus desafíos son varios: “En nuestro caso, tenemos, por un lado, el GAP tecnológico, pero por otro, estamos adquiriendo empresas en otros países que tienen regulaciones diferentes con lo que tienes que adaptarte a todas ellas. A todo esto hay que añadir que tienes que dar servicios a los clientes y mantener todas las regulaciones es complejo. La parte más importante para nosotros es por tanto la observabilidad”.

Por su parte, Manuel Asenjo, CIO de Broseta, dio prioridad a la protección. Tal y como explicó, “para Broseta el principal objetivo y lo más importante de nuestra estrategia es no perder la credibilidad por parte de los clientes. Por este motivo la protección de sus datos es una de las partes más importante”.

Como abordar la situación

Proteger datos y cumplir la normativa supone, como hemos visto, distintos retos. Pero hay algunos elementos fundamentales y que deberían ser comunes a todas las empresas. En este sentido, José Luis Berrocal, EMEA security sales leader de HCL Software, cree que “el abordaje correcto es cuando el negocio está alineado con las estrategias de TI y se automatizan las funciones. Se trata de implementar estrategias que tienen sentido. Nuestra herramienta permite que las empresas cumplan con todas y cada una de las regulaciones que existen. Entre otras cosas, realizamos un control completo de todas las herramientas que tienen implementadas las empresas”.

Por su parte, Jaime Alonso, sales engineering manager de DataDog afirmó que “las empresas que tienen éxito en el gobierno IT son aquellas que tienen una cultura adecuada. Si siguen trabajando en silo es más complicado, mientras que aquellas que tienen alineada la seguridad y el compliance con el resto de equipos y divisiones son las que tienen éxito”.

En este sentido, Ildefonso Vera afirmó que “en el caso de Isdefe, lo que intentamos es involucrar a todo el mundo en la parte de la ciberseguridad, para que todo esté alineado. Es verdad que esto genera más burocracia, pero no queda más remedio si quieres cumplir con la legislación”

Para Alejandro Expósito, “lo que es burocracia y esos procesos que son tediosos son un tema cultural. En mi caso, negocio es el que obliga a cumplir con la parte de ciberseguridad y

de cumplimiento. Si no cumplimos con una normativa, en nuestro caso, puede suponer el frenazo de un determinado proyecto. Así que son los propios usuarios los que te exigen cumplir con las normas. La gobernanza está para proteger los datos".

En muchas ocasiones "el problema es que no siempre el cliente interno está alineado. Hay veces que el cliente lo único que quiere es el sello que le permite demostrar que cumple con la normativa, pero le da igual el resto de cosas", afirmó David Caballero, CIO de Kymatio.

Para Daniel Damas de Nationale.Nederlanden "tiene que haber un balance. Nosotros estamos experimentando con diferentes actuaciones porque el área de seguridad tiene unos patrones muy bien definidos y lo que queremos es mejorar el pipeline. Si un departamento o un usario no cumple con las reglas, entonces eres un stopper. En nuestro caso, ahora todo el mundo sabe que cuando alguien pasa una aplicación sabe que ya cumple con las normas".

Para Carlos Castells, "es cierto que todo el mundo quiere un sello, pero ha tenido que venir una normativa para exigir que realmente se cumple con ella. Es triste que esto suceda. El problema es cambiar los procesos y la cultura de las empresas sobre todo en aquellas que tienen un cierto tiempo de existencia".

> **Uno de los problemas habituales es que, en numerosas ocasiones, el cliente interno no está alineado con los objetivos de gobernanza y de seguridad**

Capacitación de empleados

Uno de los problemas principales es el relacionado con la capacitación de los empleados. Se trata de que se empapen de una nueva cultura de la ciberseguridad y eso puede resultar complejo en algunos casos. En este sentido, Damas considera que "una de las claves es la de no imponer cómo se debe actuar. Se trata de que sea el empleado el que se de cuenta de la importancia de realizar acciones con seguridad. De esta forma, si comete un error la próxima dejará de cometerlo".

Luego está el problema de la experiencia y la edad. Aunque durante el debate, algunos participantes aseguraron que a los más jóvenes resulta difícil imponerles determinadas normas, la mayoría considera que el principal reto viene de parte de los empleados más mayores, a los que es más complejo cambiarles su forma de trabajar. En este sentido, el portavoz de Isdefe afirmó que "la gente joven acepta mejor aspectos como mesas limpias o el doble factor de autenticación"

Para el CIO de Serban, la procedencia de los empleados y los países en los que se encuentran también es un apartado a tener en cuenta: "Por ejemplo, los alemanes tienen muy clara la importancia de la seguridad, mientras que en otros países no tienen ninguna preocupación por ello".

Manuel Asenjo, CIO de Broseta, destacó, en este sentido, la parte cultural: "en la cultura europea estamos hiperregulados lo que nos diferencia de otras regiones del mundo y luego también es importante el apartado del apoyo de la dirección. La dirección te tiene que apoyar al 100% porque es la fórmula para avanzar".

"Ahí la normativa ha beneficiado mucho -asegura Daniel Damas de Nationale-Nederlanden-. Cuando tu le dices al Comité de Dirección que te puedes enfrentar a problemas penales tú como persona, entonces toma conciencia de la importancia de cumplir con las normativas". En este sentido, Alejandro Expósito consideró que "cumplir con la norma no es una cuestión del CEO, sino de todo el comité de dirección. Por eso se ve que ya se da mucha más importancia a estos aspectos por parte de los consejos"

Desayunos BYTE TI

Cuál es la realidad del trabajo híbrido

A pesar de que muchas empresas están empezando a apostar por el presencialismo, el trabajo híbrido es una realidad. Para tratar esta temática Byte TI organizó un encuentro, junto a Kyocera, que contó con la participación de Rafael Corrales, CIO de Nuubo; Raquel Pinillos, Business Solutions Director de Kyocera; Andrés Gómez, Jefe del departamento de gestión y dirección de TI y Comunicaciones del Congreso de los Diputados; Antonio Gil, Director Corporativo de Operaciones y Sistemas del Grupo GVC Gaesco; Jesús Valverde, CIO de Isemaren; Mario Robledo, Director de equipos y sistemas Atrevia; Roberto Gutiérrez, Cloud Lead Nationale-Nederlanden e Ildefonso Vera, director de transformación digital de Isdefe

Hasta hace no mucho, el trabajo híbrido se veía como una solución temporal. Sin embargo, las empresas pronto se dieron cuenta de sus beneficios, como la reducción de costos operativos y el aumento de la satisfacción y productividad de los empleados. El trabajo digital debe tener una característica principal: facilitar acceso a todas las herramientas necesarias para poder realizar el trabajo diario desde cualquier sitio que tenga acceso a una conexión a Internet.

Pero, ¿cuál es la situación actual del teletrabajo? ¿Están las empresas volviendo a las dinámicas presencialistas? Para Jesús Valverde, CIO de Isemaren, “en nuestro caso no tenemos ningún problema con el teletrabajo. La dificultad es la de conseguir que siempre haya presencia en las tres oficinas que tenemos y esto lo hacemos con políticas transversales. Tenemos un ecosistema mixto y luego tenemos la parte colaborativa. Se trata de que el empleado tenga las mejores herramientas para poder mejorar su productividad”.

Por su parte, Mario Robledo, Director de equipos y sistemas Atrevia, aseguró que “nosotros nos hemos basado en todo el ecosistema de Microsoft, que nos proporciona una gran seguridad. Además es un entorno sencillo para el empleado. Eso nos permite tener un esquema de trabajo híbrido que consiste en que hay tres días en los que se va a la oficina y dos se puede trabajar desde casa”

Roberto Gutiérrez, Cloud Lead Nationale-Nederlanden, afirmó que “antes de la pandemia ya habíamos iniciado una evolución hacia el trabajo híbrido, pero fue con el Covid cuando impulsamos el uso de las herramientas colaborativas. En la actualidad, tenemos un modelo mixto presencial/teletrabajo. Hay que guiar un poco a los usuarios

Desayunos BYTE TI

Cuál es la realidad del trabajo híbrido

Andrés Gómez
Jefe del departamento de gestión y dirección de TI y Comunicaciones del Congreso de los Diputados

Antonio Gil
Director Corporativo de Operaciones y Sistemas del Grupo GVC Gaesco

Jesús Valverde
CIO de Isemaren

Ildefonso Vera
director de transformación digital de Isdefe

para que se adapten a las nuevas tecnologías. La parte negativa es que pierdes cierto contacto con los compañeros. Así que hay muchas veces que nos reunimos en la oficina para fomentar ese contacto".

Ildefonso Vera, director de transformación digital de Isdefe, considera que "la globalización y el avance tecnológico son dos factores que han impulsado el teletrabajo. Nosotros apostamos por el trabajo híbrido y apostamos por Microsoft para las herramientas colaborativa. Hemos automatizado y digitalizado los procesos que le facilitan la vida al trabajador. Pero además se ha producido un cambio en la mentalidad: para retener y atraer el talento, se demanda la flexibilidad más que la parte económica. Esto tiene más riesgos en lo que a seguridad se refiere porque se amplia el perímetro y tienes que implementar nuevas medidas de seguridad". También en el caso de Nuubo se empezó a trabajar en entornos híbridos antes de la pandemia. Rafale Corrales, CIO de la compañía explicó que "nosotros apostamos por un modelo híbrido libre, aunque hay veces que nos reunimos todos en la oficina. En cuanto a las herramientas de colaboración nos decidimos por Google Workspace. En su momento, las personas se tuvieron que adaptar, pero ahora estamos viendo que los nuevos trabajadores que se incorporan a la compañía no tienen problema en relación al trabajo híbrido".

Andrés Gómez, Jefe del departamento de gestión y dirección de TI y Comunicaciones del Congreso de los Diputados, afirmó que "tenemos la mitad de usuarios migrados a Microsoft 365 y el resto están todavía en modo on-premise aunque en Enero el 100% estarán en la plataforma de colaboración. En nuestro caso tenemos sólo trabajo presencial porque en el Congreso es difícil de aplicar. Ahora el teletrabajo se utiliza poco, pero lo utilizamos en excepciones por ejemplo en bajas por enfermedad".

Lo importante: las personas

Antonio Gil, Director Corporativo de Operaciones y Sistemas del Grupo GVC Gaesco afirmó que "yo no soy un convencido del teletrabajo, pero sí lo soy de la conciliación. Sólo tengo una o dos personas que se acoplan a un sistema de teletrabajo. Cada uno elige, según las circunstancias. Con la pandemia la gente empezó a posteriori a volver a la oficina. Si estamos abiertos a incorporar el teletrabajo, pero tratando la problemática según las necesidades de cada persona. Tenemos implementadas diferentes herramientas colaborativas con Atlassian. En nuestro caso el principal problema es el de la concienciación

Encuentros BYTE TI

Cuál es la realidad del trabajo híbrido

Mario Robledo
Director de equipos y sistemas Atrevia

Rafael Corrales
CIO de Nuubo

Raquel Pinillos
Business Solutions Director de Kyocera

Roberto Gutiérrez
Cloud Lead Nationale-Nederlanden

de las personas en materia de ciberseguridad".

Raquel Pinillos, Business Solutions Director de Kyocera consideró que es importante tratar cada una de las circunstancias: "Los equipos de desarrollo, por ejemplo, es casi imposible que vayan a trabajar de forma presencial. A mí me gusta el discurso que se ha adoptado y es señalar que lo importante son las personas. Lo que ha provocado la hibridación del puesto de trabajo es que ahora las empresas se están centrando en mejorar la experiencia de empleado. Eso incluye a la seguridad. En Kyocera estamos viendo que los equipos de tecnología están volcados en mejorar la experiencia del cliente y en este sentido estamos apreciando dos tendencias grandes: la seguridad, porque el tema de trabajo colaborativo ya está muy adoptado y la otra, la de mejorar el gobierno de la información para que, por ejemplo, el Teams no se convierta en un repositorio de documentos desperdigados". Sobre esto último, Jesús Valverde, afirmó que "en nuestro caso había que implementar un modelo de gobierno y eso fue lo que hicimos. La tecnología nos permite ser ágiles y entregar al cliente el valor que espera, pero el coste de un servicio va metido en el proyecto y es el responsable del mismo el que se preocupa, por ejemplo, de borrar versiones de proyectos para impedir que se eleve el coste. La tecnología tienen que ayudar al empleado a ser lo más eficiente posible"

Pero no sólo es mejorar la eficiencia. Antonio Gil afirmó que, además de ello, "estamos cambiando los modelos de gobernanza, también porque estamos obligados a cumplir con la legislación vigente. Por eso, tenemos que gestionar la gobernanza del dato".

El reto de la IA

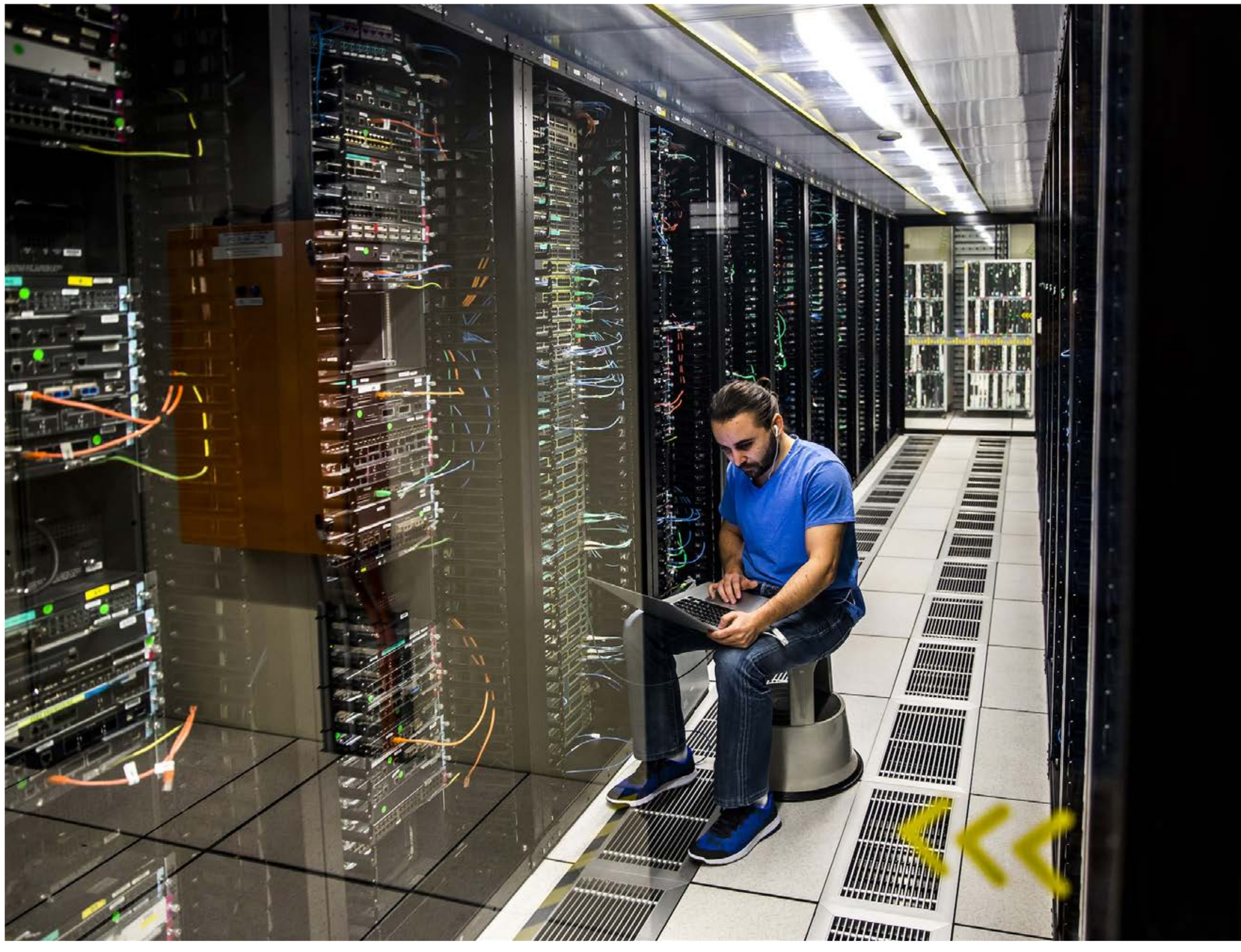
La aparición de la Inteligencia Artificial generativa puede suponer todo un reto en la gobernanza. En este sentido, Rafael Corrales aseguró que "hace ocho meses implantamos un procedimiento interno y lo primero que hemos hecho es aislar el uso de la IA para uso personal. Al final, creo que de lo que se trata es de concienciar a las personas sobre los usos. Si haces esa concienciación, al final, las personas cumplen".

Raquel Pinillos afirmó que "lo que nos están pidiendo los clientes son alternativas a Copilot y ChatGPT, porque, al final no confían y desconocen quién maneja los datos con los que trabajan las aplicaciones de IA generativa. La realidad es que para organizaciones que quieran que no haya respuestas que no sean erróneas, hay aplicaciones para que sólo se basan en información de la propia compañía".

Comparativa

5 servicios de detección y respuesta de amenazas

Conocidos también por las siglas TDR (del inglés Threat Detection and Response), bajo el nombre de servicios de detección y respuesta de amenazas se engloba un conjunto de procesos y tecnologías avanzadas que tienen un firme y claro propósito: identificar, analizar y responder de manera rápida y proactiva a las ciberamenazas vertidas sobre las organizaciones empresariales (el origen de estos ataques informáticos pueden afectar a los sistemas, las redes o los dispositivos que normalmente utilizan). El hecho de que brinden una detección rápida, ofrezcan una respuesta ágil y consideren todos los posibles aspectos relacionados con la seguridad de la empresa -en vez de centrarse en un área específica o elemento- ayuda a mantener la integridad y la disponibilidad de los datos.



Así funcionan

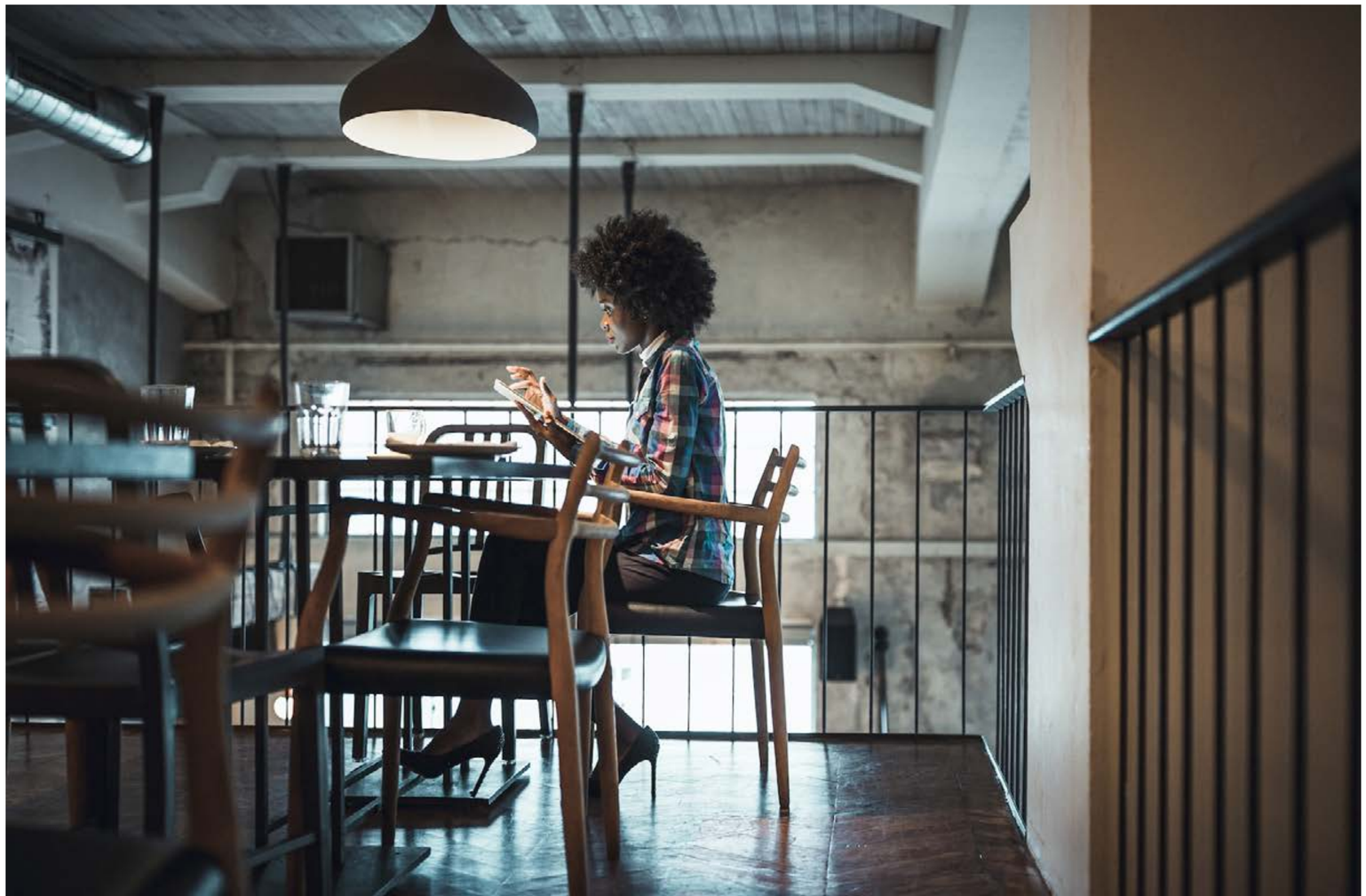
Aunque cada fabricante cuenta con sus propias tecnologías y soluciones, los servicios de detección y respuesta de amenazas aplican, en líneas generales, una serie de fases y procesos que incluyen en primer lugar una función de vigilancia o monitoreo constante en busca de cualquier actividad considerada sospechosa y que a priori podría comprometer la seguridad

Comparativa

5 servicios de detección y respuesta de amenazas

de una red, un sistema o una infraestructura. Esta fase de vigilancia se acompaña de análisis de comportamiento que lo que persiguen es la identificación de estas amenazas antes de que actúen.

Que los servicios de detección y respuesta de amenazas delimiten una línea de lo que se considera normal y luego monitorizan de continuo el sistema para localizar cualquier sospecha o desviación es lo que va a permitir a una empresa responder de manera oportuna. Para acelerar la identificación y mitigación de las amenazas es habitual que se apliquen diferentes tecnologías de automatización en muchos de los procesos no solo de detección, sino también de respuesta. Para que esta respuesta sea lo más eficaz posible lo habitual es que se coordinen entre sí varias herramientas; herramientas que supervisen desde identidades y redes hasta aplicaciones y nubes pasando por puntos de conexión.



Una vez se determina cómo se ha producido y llevado a cabo la ciberamenaza en cuestión, y tras evaluar los daños producidos, tienen lugar las fases de contención y de erradicación. En la primera el propósito es frenar la expansión del ciberataque: para ello, los equipos de seguridad y herramientas disponibles separan identidades, redes y dispositivos infectados, aislándolos del resto de los sistemas de la organización. Mientras, en la segunda, además de eliminar la raíz del incidente, se corrigen las vulnerabilidades que podrían exponer a la compañía a futuros ataques similares. Es habitual, en otro orden de cosas, que los servicios de detección y respuesta de amenazas faciliten la generación de informes cuya documentación recoge lo que ha sucedido y la manera en que se ha resuelto el incidente.

Beneficios destacados

Las organizaciones que adquieren esta clase de soluciones disfrutan de diferentes ventajas que van más allá de una detección temprana o una respuesta rápida frente al ataque recibido. Destacan, entre otros, la reducción del tiempo de inactividad y el cumplimiento normativo ya que existe un marco legal que exige la protección de la privacidad y los datos.

Comparativa

5 servicios de detección y respuesta de amenazas

Cisco Hypershield

La multinacional estadounidense, especializada en servicios y productos relacionados con telecomunicaciones y redes, participa en esta comparativa con Hypershield. Se trata de una solución que ofrece al ámbito empresarial un conjunto de capacidades para detectar y para bloquear ataques a las cargas de trabajo procedentes de vulnerabilidades tanto conocidas como desconocidas. Con el objetivo de proteger los centros de datos y las nubes informáticas, aprovecha tanto la inteligencia artificial como los datos sobre exploits de Cisco Talos; así es como se denomina al grupo de investigación y de respuesta ante amenazas de ciberseguridad de Cisco.

Hablando de amenazas, Hypershield resuelve tres desafíos clave de los clientes ante su defensa. El primero de estos desafíos son las actualizaciones preverificadas: la solución, a este respecto, automatiza el proceso laborioso y lento de probar e implementar actualizaciones una vez que están listas. El segundo desafío es la segmentación automática. ¿Qué significa? Una vez que el atacante está en la red, la segmentación es clave para detener su movimiento lateral. Hypershield observa, razona de modo automático y reevalúa constantemente las políticas existentes para segmentar la red de forma autónoma. Finalmente, se encuentra la protección distribuida contra exploits en minutos, no en semanas o meses.

Dado que los atacantes convierten 'en armas' las vulnerabilidades recientemente publicadas más rápido de lo que los defensores pueden parchear, Hypershield promete una protección de manera casi instantánea frente a exploits sin parche.

Como solución de seguridad nativa de inteligencia artificial para proteger y escalar los centros de datos, la propuesta de Cisco ha sido construida con tecnología diseñada originalmente para grandes gestores de nubes públicas o hyperscalers. Ahora disponible para equipos de TI empresariales de todos los tamaños, este fabric de seguridad basado en eBPF (hace referencia a una tecnología de programación proveniente del término Extended Berkeley Packet Filter) de código abierto sitúa las medidas de protección donde sea necesario.

Aprovecha, de igual modo, la tecnología de NVIDIA Morpheus para acelerar la detección de anomalías en la red y los microservicios NVIDIA AI Foundry y NIM para impulsar asistentes de inteligencia artificial de seguridad personalizados para la empresa; en el caso de Morpheus, hablamos de un framework de aplicaciones abierto que facilita a los desarrolladores de ciberseguridad crear pipelines de IA optimizados con un triple propósito: filtrar, procesar y clasificar grandes volúmenes de datos en tiempo real. Al

conceder un nuevo nivel de seguridad al centro de datos, la nube y el edge, Morpheus emplea la tecnología de IA para identificar, capturar y actuar sobre amenazas y anomalías que antes eran imposibles de identificar. Proporciona además análisis de gráficos en tiempo real; aprovecha los modelos de lenguaje para el aprendizaje no supervisado; y ofrece una visibilidad del 100% de los datos para crear soluciones que supervisen las actividades de registro e identifiquen anomalías y amenazas dentro de una red. Funciona con los firewalls de las organizaciones, aplicando automatización, flujos de trabajo e inteligencia artificial para brindar no solo protección frente vulnerabilidades nuevas y conocidas en cuestión de minutos; también protección lateral.

Cisco
contacto
www.cisco.es
A consultar

Comparativa

5 servicios de detección y respuesta de amenazas

Palo Alto Networks Precision AI

La firma ofrece una serie de soluciones de seguridad que le ayudan a integrar su tecnología Precision AI. Diseñada para contrarrestar las amenazas generadas por la inteligencia artificial y proteger a las organizaciones, combina inteligencia artificial generativa (GenAI), machine learning (ML) y deep learning (DL) para una defensa proactiva contra los atacantes. Entrando en detalle, las soluciones basadas en Precision AI ofrecen protección contra las amenazas impulsadas por tecnología de inteligencia artificial como amenazas de día cero, ataques de comando y control, y ataques de secuestro de DNS. Dado que el sistema se nutre de datos globales, la capacidad de detección de amenazas mejora de continuo.

Bajo el paraguas de Precision AI se identifican tres soluciones. La primera, denominada AI Access Security, permite que las compañías empleen herramientas de IA con confianza al proporcionar visibilidad total, controles de seguridad y protección proactiva de los datos. Asegura, asimismo, que puedan adoptar la inteligencia artificial sin comprometer su seguridad. AI Security Posture Management (AI-SPM), la segunda, identifica vulnerabilidades, prioriza configuraciones erróneas y mejora el cumplimiento normativo, protegiendo la infraestructura desde su desarrollo hasta su implementación. La tercera de las soluciones ha sido bautizada con el nombre de AI Runtime Security: su objetivo es proteger las aplicaciones impulsadas por inteligencia artificial en tiempo real, enfrentando amenazas como las inyecciones de prompt y modelos de denegación de servicio (DoS). Garantiza, de igual forma, que los resultados generados por los modelos de esta tecnología resulten seguros y protejan contra los ataques.

En otro orden de cosas, la tecnología sobre la cual ha trabajado Palo Alto Networks ofrece una serie de beneficios clave para la seguridad empresarial. Por ejemplo, apuesta por un enfoque en la automatización y proactividad que no solo permite que la solución reaccione a las amenazas, también que anticipe ataques futuros. Esto se logra por medio de la emisión de alertas proactivas que proporcionan mejores prácticas y un soporte directo dentro del flujo de trabajo para una respuesta más rápida y efectiva.

Como experta en ciberseguridad la firma ha adoptado, por otro lado, un enfoque de 'plataformización' que busca eliminar las barreras entre diferentes soluciones de seguridad. Dicho enfoque le ayuda a brindar una plataforma unificada que mejora la eficiencia operativa y optimiza la defensa en entornos de red, nube y centros de operaciones de seguridad. La

integración de los sistemas facilita una protección más coherente y robusta, mejorando la capacidad de las empresas para enfrentarse a amenazas cibernéticas complejas. Mientras, el concepto de 'Secure AI by Design' garantiza que todo el ecosistema de IA quede protegido desde la fase inicial de diseño. Esto implica priorizar la integridad y el cumplimiento de los marcos de seguridad de IA, asegurando que las aplicaciones y herramientas impulsadas por esta tecnología sean seguras desde el desarrollo hasta su implementación. Precision AI y las soluciones asociadas están diseñadas para ofrecer una seguridad más autónoma, contextualmente informada y accionable con el propósito de proteger al mundo empresarial de una era que cada vez está más dominada por la inteligencia artificial.

Palo Alto Networks
+49 (0) 69 9675 8365
www.paloaltonetworks.es

A consultar. Las soluciones estarán disponibles de manera general en el cuarto trimestre del año fiscal 2024 y el primer trimestre del año fiscal 2025.

Comparativa

5 servicios de detección y respuesta de amenazas

Sophos Managed Detection and Response (MDR)

Un servicio 24 x 7 totalmente gestionado y prestado por personal experto que detecta y responde a los ciberataques dirigidos a los ordenadores, los servidores, las redes, las cargas de trabajo en la nube, las cuentas de correo electrónico… Esta es la carta de presentación del servicio de detección y respuesta de amenazas de Sophos; el fabricante promete que sus herramientas bloquean hasta un 99,98% de las amenazas.

Si ahondamos en sus características, Sophos MDR es compatible con la telemetría de seguridad de proveedores como Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace … En este caso, la telemetría (por medio de esta técnica lo que se hace es ampliar la visibilidad del entorno) se consolida, correlaciona y prioriza automáticamente con información exhaustiva del ecosistema de ciberseguridad adaptativa Sophos Adaptive Cybersecurity Ecosystem (ACE) y la unidad de información sobre amenazas Sophos X-Ops. Además de evitar las actividades maliciosas, Sophos ACE permite buscar indicios débiles de amenazas que requieren intervención humana para detectarlas, investigarlas y eliminarlas. También cobran especial valor los informes semanales y mensuales a disposición de la organización empresarial. A estes respecto, Sophos Central es un panel de control que cumple no solo con la gestión de la solución, ayuda a recibir alertas en tiempo real y generar informes. Esta documentación incluye información exhaustiva sobre las ciberamenazas detectadas y las investigaciones de seguridad que se hayan efectuado.

Las compañías interesadas en Sophos MDR disfrutarán de otras prestaciones que les serán útiles en su día a día. Por ejemplo, el fabricante proporciona a las organizaciones

un responsable de respuesta a amenazas dedicado que colabora con el equipo interno de la empresa (también partners externos) en cuanto se identifica una amenaza y trabaja con ella hasta que se resuelve el incidente. Junto a las recomendaciones proactivas para mejorar la postura de seguridad de la compañía, Sophos lleva a cabo un análisis de causa raíz para identificar los problemas subyacentes que han provocado el incidente, bridando así orientación prescriptiva para resolver vulnerabilidades de seguridad a fin de que no puedan ser explotadas en el futuro.

Función ‘Comprobar la cuenta de Sophos’. Por medio de esta opción, el servicio revisa de continúo los ajustes y las configuraciones de los endpoints gestionados por la plataforma Sophos XDR para asegurar que mantienen su máximo rendimiento. Por otro lado, en el caso de las compañías que deciden no optar por la respuesta a incidentes integral de Sophos MDR, el equipo de operaciones de Sophos MDR puede ejecutar acciones de contención para interrumpir la amenaza y evitar su propagación. Esto reduce la carga de trabajo de los equipos de seguridad internos y les permite aplicar medidas de remediación rápidamente.

Resulta interesante la sesión informativa mensual Sophos MDR ThreatCast. Presentada por el equipo de operaciones de Sophos MDR y disponible en exclusiva para los clientes de Sophos MDR, revela datos clave relativos a la información sobre amenazas más recientes y las prácticas de seguridad recomendadas.

Sophos
910 621 230
www.sophos.com/es-es
A consultar

Comparativa

5 servicios de detección y respuesta de amenazas

Trend Micro Vision One XDR

Esta solución destaca por ofrecer capacidades de detección y respuesta integradas en el email, la red, el endpoint, el servidor y las cargas de trabajo cloud. Para ello, emplea la tecnología XDR desarrollada por la firma que escala a través del mayor número de fuentes posibles para disponer de las detecciones más completas que se han generado lo antes posible. Dentro de este contexto, la plataforma de Trend Micro emplea tecnología machine learning y apilamiento de datos no solo para detectar ataques, sino para proporcionar alertas tempranas de posibles incidentes a través de análisis predictivos.

Además de visualizar rápidamente toda la historia de cada uno de los ataques, Vision One XDR ayuda a que las organizaciones mejoren su eficiencia operativa. Lo hace aprovechando varias herramientas y tecnología de inteligencia artificial que profundizan en técnicas y estrategias específicas que buscan indicadores de ataque y de compromiso. Incluso es posible integrar resultados de terceros con la plataforma (que es compatible con API) para disponer de una mayor cantidad de datos (firewall, gestión de vulnerabilidades, redes, gestión de acceso de identidad, SIEM y SOAR) para optimizar los procesos y los flujos de trabajo existentes. De igual modo, el enfoque híbrido y nativo de XDR y ASM- por el que apuesta la solución- beneficia a los equipos de seguridad de las empresas al disponer de una telemetría de actividad más rica; pero no solo en los datos de detección, sino en todas las capas de seguridad con un contexto y una comprensión completos. El resultado es una detección de riesgos y amenazas más temprana y precisa, y una investigación más eficiente.

En referencia a la investigación precisa de estas amenazas, la identificación de incidentes críticos, priorizados según la gravedad y el alcance del impacto, es la ruta más rápida para obtener mejores resultados empresariales y de seguridad. Trend Vision One permite, dentro de este contexto, 'concentrarse' en lo que necesita atención correlacionando actividades de baja fiabilidad con incidentes de alta fiabilidad, lo que supone menos alertas y más priorizadas.

Las prestaciones ofrecidas por la plataforma de Trend Micro se complementan con otras características de interés y utilidad para el día a día de la empresa. Por ejemplo, se arroja una profunda visibilidad y prevención de amenazas para endpoints y servidores correlacionando automáticamente los datos en varias capas de seguridad para una detección más rápida, una mejor investigación y un

menor tiempo de respuesta. De igual modo, brinda protección para todos los dispositivos con DNR y ayuda a conocer cuáles son los usuarios con mayores privilegios y aquellos expuestos a mayores riesgos.

Con Trend Micro Vision One XDR es posible, en otro orden de cosas, ampliar la detección y la respuesta más allá de las cuentas de emails analizando el correo electrónico, los registros de amenazas y su comportamiento para disponer de una mayor visibilidad de las actividades consideradas sospechosas. Para predecir posibles brechas de explotación, la plataforma mide y pondera diferentes factores de riesgo como vulnerabilidades, controles de seguridad y configuraciones erróneas, entre otros.

Trend Micro
913 69 70 30
www.trendmicro.es
A consultar

Comparativa

5 servicios de detección y respuesta de amenazas

WatchGuard MDR

WatchGuard MDR es un servicio de ciberseguridad personalizable y escalable 24 x 7 diseñado para que los proveedores de servicios gestionados (MSP) que trabajan para satisfacer la creciente demanda de los clientes de ciberseguridad gestionada tengan un acceso más fácil a este servicio. Gestionado por un equipo de expertos en ciberseguridad e impulsado por inteligencia artificial, ofrece monitorización de seguridad de endpoints de primer nivel, threat hunting, detección de ataques, e investigación y satisfacción con recomendaciones guiadas para remediar los activos afectados y mejorar la postura de seguridad del cliente. Dicho equipo atesora una larga experiencia en ámbitos como el aprendizaje automático y los análisis de seguridad. Así, su trabajo consiste exactamente en supervisar, buscar, detectar y contener las amenazas que se 'esconden' en los endpoints durante el día, al tiempo que evalúan la superficie de ataque para fortalecer la postura de seguridad de la organización empresarial y mejorar su resistencia frente a las amenazas.

Sus características relevan, asimismo, que proporciona capacidades avanzadas de detección y respuesta a amenazas sobre WatchGuard EDR, EPDR y Advanced EPDR que permiten a los MSP construir ofertas de seguridad robustas y completas para sus clientes. Viene, a este respecto, con el soporte del servicio automatizado Zero-Trust Application Service de WatchGuard; Threat Hunting Service; analíticas de seguridad avanzadas; e inteligencia de amenazas.

A la monitorización que realiza de la actividad de los endpoints y recopilación de datos, se suman otras prestaciones de interés. Este es el caso de la identificación y detección proactivas: para minimizar el tiempo de detección y mitigación de amenazas, WatchGuard MDR emplea, entre otros, machine learning y técnicas avanzadas para identificar indicadores de ataque. Las empresas disponen, igualmente, de un servicio de notificación inmediata de incidentes con información clave como, por ejemplo, los equipos afectados. También destacan los informes semanales del estado de la seguridad y los mensuales referidos a la actividad de la compañía: para generar confianza a la cartera de clientes proporcionándoles informes periódicos sobre el estado de su seguridad, los proveedores de servicios tienen la opción de personalizarlos para involucrar mejor a estos con su servicio MDR y proporcionarles a la vez comentarios a lo largo del proceso.

Como fabricante de tecnología de seguridad cibernética, WatchGuard pone al servicio de las compañías lo que denominan 'buscadores de amenazas'. La función que tienen estos analistas es correlacionar las señales débiles de comportamiento anormal con inteligencia de amenazas y determinar si se deben investigar más. Además, formulan hipótesis de ataques con la inteligencia de amenazas más actualizada para encontrar las técnicas y los procedimientos más adecuados. Otras características de interés de WatchGuard MDR son las siguientes: supervisión continúa de Microsoft 365, retención de telemetría de 365 días en la nube, pautas de corrección y de mitigación, playbooks personalizados para la contención automatizada de filtrados por endpoints, informes recurrentes de objetivos de defensa de Microsoft 365, cumplimiento de los requisitos reglamentarios y la notificación inmediata de incidentes al punto de contacto elegido por correo electrónico o teléfono.

WatchGuard
911 410 918
www.watchguard.com/es
A consultar

Conclusiones

Todas las opciones presentadas a esta comparativa son válidas e interesantes para cualquier compañía, pero al final la clave se encuentra en las necesidades que debe cubrir cada empresa. Sin embargo, en nuestra opinión, dos de ellas destacan sobre el resto: nos referimos a las propuestas de Cisco Hypershield y Sophos Managed Detection and Response (MDR). La primera destaca, entre otros, por aprovechar el potencial de la inteligencia artificial, la segmetación autónoma y la protección distribuida contra exploits en minutos. De Sophos Managed Detection and Response (MDR) resaltamos su compatibilidad con la telemetría de seguridad de proveedores como Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google…

Respecto a las otras tres soluciones, Palo Alto Networks ha desarrollado alrededor de Precision AI las siguientes tres solucione avanzadas: Runtime Security, Access Security y Security Posture Management (AI-SPM). Por su parte, Trend Micro Vision One brinda (entre otras muchas prestaciones) una integración completa que ofrece una optimización de los flujos de trabajo con un ecosistema que incluye SIEM, SOAR, IAM, firewall, información sobre amenazas y gestión de servicio de TI. Finalmente, la solución WatchGuard MDR ha sido diseñada de manera específica para los proveedores de servicios gestionados (MSP)

ASPECTOS DESTACADOS

Fabricante	Cisco	Palo Alto Networks	Sophos	Trend Micro	WatchGuard
Nombre del modelo	Hypershield	Precision AI	Managed Detection and Response	Vision One XDR	MDR
Valoración	★★★★	★★★★	★★★★	★★★★★	★★★★★
Características clave	• Actualizaciones pre-verificadas. • Segmentación autónoma. • Construido con tecnología diseñada originalmente para grandes gestores de nubes públicas o hyperscalers. • Funciona con los firewalls existentes de las organizaciones, aplicando automatización, flujos de trabajo e inteligencia artificial para ofrecer protección frente a vulnerabilidades nuevas y conocidas en minutos, y protección lateral. • Protección distribuida contra exploits en minutos.	• Las soluciones basadas en Precision AI son: Access Security, Security Posture Management (AI-SPM) y Runtime Security. • Combina inteligencia artificial generativa (GenAI), machine learning (ML) y deep learning (DL). • Las plataformas de seguridad de Palo Alto Networks (Strata, Prisma y Cortex) se benefician de las capacidades de Precision AI para proteger redes, infraestructuras y aplicaciones empresariales. • El ecosistema de IA esté protegido desde la fase inicial de diseño. • Enfoque de 'plataformización'.	• Equipo 24/7 de expertos en respuesta a las amenazas. • Responsable de respuesta a incidentes dedicado. • Compatible con la telemetría de seguridad de proveedores como Microsoft, CrowdStrike, Palo Alto Networks, Fortinet… • Informes semanales y mensuales. • Respuesta a incidentes integral.	• Identificación de incidentes críticos, priorizados según la gravedad y el alcance del impacto. • Mejora de la eficiencia operativa. • Capacidades XDR, ASRM y zero trust diseñadas a medida. • Integración completa: optimice flujos de trabajo con un ecosistema que incluye SIEM, SOAR, IAM, firewall, información sobre amenazas, gestión de servicio de TI... • SOC fortalecido.	• Identificación y detección proactiva 24/7 . • Opciones para la mitigación y directrices para la remediación. • Buscadores de amenazas. • Informe semanal del estado de la seguridad e informes mensuales de actividad. • Monitorización 24/7 de la actividad de los endpoints y recopilación de datos.

¿Cuál es el impacto real de IoT?

Vanesa García

Internet de las Cosas (IoT) se ha consolidado como una de las tecnologías más transformadoras de nuestra era, revolucionando sectores desde la manufactura hasta la salud. En un mundo cada vez más interconectado, el IoT no solo facilita la comunicación entre dispositivos, sino que también impulsa la eficiencia operativa y la innovación.

Los informes lo confirman. Según McKinsey, el IoT ha alcanzado su mayoría de edad, con aplicaciones que abarcan desde hogares inteligentes hasta smart cities. Y es que, la adopción de esta tecnología no solo optimiza procesos, sino que también permite a las organizaciones anticiparse a las necesidades del mercado y responder con agilidad a las oportunidades emergentes.

"El IoT está desempeñando un papel muy relevante en una parte importante del proceso de transformación digital de muchas organizaciones. Sobre todo, por su capacidad para automatizar procesos y optimizar el uso de recursos, pero también porque permite extraer información valiosa de los datos generados por toda clase de dispositivos conectados y de los entornos donde las personas desarrollan su actividad. Gracias a esta conectividad, las empresas pueden tomar decisiones más informadas en tiempo real y mejorar la eficiencia. Además, el IoT abre nuevas oportunidades de negocio y puede contribuir a mejorar la experiencia del cliente a muy distintos niveles", afirma Pedro L. Martinez Busto, Southern Europe SASE, DCN y NaaS Business Lead de HPE Aruba.

El impacto del IoT en las ciudades es particularmente notable. La tecnología contribuye a mejorar la gestión urbana y su sostenibilidad, por ejemplo, reduciendo el consumo de agua y optimizando la recogida y el transporte de residuos. Asimismo, la adopción del IoT en el sector salud ha permitido avances significativos en la atención médica, desde el monitoreo remoto de pacientes hasta la gestión eficiente de recursos hospitalarios.

En esta misma línea, Rocío Dantart, Directora de IoT Industrial para EMEA en Cisco, destaca: "El IoT está impulsando la transformación digital al conectar dispositivos y permitir el análisis de datos en tiempo real, lo que mejora la eficiencia operativa, reduce costes y crea nuevos modelos de negocio basados en datos. Según los datos de Cisco, los sectores donde IoT y el IoT Industrial crece con mayor rapidez son las empresas de servicios públicos (eléctricas, gas, agua, residuos…), las fábricas (automoción, alimentación, químicas, farmacéuticas…), el transporte (ferroviario, puertos, aeropuertos, gestión de autopistas) e incluso la minería".

Siguiendo este punto, la adopción del IoT no solo optimiza procesos, sino que también permite a las organizaciones anticiparse a las necesidades

del mercado y responder con agilidad a las oportunidades emergentes. La capacidad de integrar tecnologías digitales en el mundo físico está creando un valor significativo en diversos entornos, desde fábricas hasta hogares, y está transformando la manera en que interactuamos con nuestro entorno.

"El IoT es un catalizador de la eficiencia, la productividad y la innovación. Es una herramienta que permite a las empresas recopilar y analizar datos en tiempo real, lo que facilita la toma de decisiones inteligentes, la optimización de procesos y ofrecer mejores experiencias a sus clientes", añade Miguel Ángel Fernández, Director de Marketing en LG Electronics España.

Sectores líderes en IoT

El Internet de las Cosas (IoT) está revolucionando múltiples sectores, impulsando la eficiencia, la conectividad y la innovación. A continuación, se presentan las opiniones de varios expertos sobre los sectores que más están apostando por esta tecnología.

Martinez Busto destaca la adopción del IoT en sectores como las oficinas, el sector residencial y la industria hotelera. Según él, estos sectores están aprovechando el IoT para mejorar la gestión de recursos y la experiencia del cliente. "Aunque es prematuro señalar sectores específicos como líderes absolutos en la adopción del IoT, está claro que está ganando terreno en muchos ámbitos, especialmente en aquellos que dependen de la automatización y la conectividad. Los entornos de oficina, el sector residencial y la industria hotelera son ejemplos claros de sectores que destacan en esta adopción".

Por su parte, Dantart subraya el crecimiento del IoT en áreas emergentes como las ciudades inteligentes, los servicios de atención sanitaria, la logística, la agricultura y el sector automotriz. Enfatiza además la importancia de la conectividad y la ciberseguridad en estos sectores, "dentro de las áreas emergentes con mayor potencial en primer lugar están las ciudades inteligentes (iluminación, seguridad pública, gestión del tráfico, estaciones de carga eléctrica, gestión de parking, gestión de flotas de vehículos de emergencia), los servicios de atención sanitaria (monitorización remota de pacientes mediante sensores biométricos), logística (rastreo en tiempo real de inventarios y flotas), agricultura (sensores para monitorizar cultivos y optimizar el uso de agua y fertilizantes) y automotriz (con vehículos conectados que ofrecen conducción asistida y servicios inteligentes)".

Los que más están invirtiendo en IoT, en opinión de David Polo, Enterprise Sales Director Iberia de Ericsson, son los sectores de automoción, transporte, energético, defensa y seguridad, y logística son La empresa destaca cómo el IoT está mejorando la seguridad, la eficiencia y la gestión en tiempo real en estos sectores. "Actualmente, los sectores que más están apostando por IoT son: Automoción: Mejora la seguridad y eficiencia mediante vehículos conectados. Transporte: Optimiza rutas y gestión de flotas en tiempo real. Energético: Facilita la gestión de redes inteligentes y eficiencia energética. Defensa y seguridad: Aumenta la precisión y control en operaciones con sensores

y drones. Logística: Monitorea y optimiza cadenas de suministro y transporte".

Trejo menciona que, además del sector consumo con el hogar digital, la agricultura y los transportes son sectores que están viendo grandes beneficios del IoT, "aparte del sector consumo con el hogar digital, en nuestro caso hemos desarrollado proyectos de conectividad de datos para granjas inteligentes y redes de transportes como metrovalencia, mediante routers M2M 4G/5G que ofrecen infinidad de datos, geolocalización y mucho más, por lo que la agricultura y los transportes pueden ser de los más beneficiados si se dotan de las tecnologías de conectividad más eficientes junto a una gestión de esos datos lo más eficiente posible".

En resumen, el IoT está siendo adoptado de manera significativa en sectores diversos, cada uno aprovechando sus capacidades para mejorar la eficiencia, la conectividad y la innovación. La transformación digital impulsada por el IoT está creando nuevas oportunidades y optimizando procesos en múltiples industrias.

Estrategias empresariales y tecnologías emergentes

El desarrollo del Internet de las Cosas (IoT) en las empresas es un proceso complejo que requiere una estrategia bien definida para maximizar sus beneficios. Según un informe de TecnoFuturo, muchas empresas aún enfrentan desafíos significativos en la implementación de estrategias de IoT, incluyendo la seguridad de los datos, la interoperabilidad de dispositivos y la gestión de grandes volúmenes de datos. Además, la falta de una estrategia clara puede llevar a inversiones ineficientes y a la subutilización de las capacidades del IoT.

El Southern Europe SASE, DCN y NaaS Business Lead de HPE Aruba, señala que aunque muchas organizaciones están adoptando el IoT, la falta de una estrategia clara puede ser un obstáculo, "aunque es prematuro señalar sectores específicos como líderes absolutos en la adopción del IoT, está claro que está ganando terreno en muchos ámbitos, especialmente en aquellos que dependen de la automatización y la conectividad. Los entornos de oficina, el sector residencial y la industria hotelera son ejemplos claros de sectores que destacan en esta adopción".

Del mismo modo, la Directora de IoT Industrial para EMEA en Cisco, destaca la importancia de la conectividad y la ciberseguridad en la implementación de estas tecnologías, "dentro de las áreas emergentes con mayor potencial en primer lugar están las ciudades inteligentes (iluminación, seguridad pública, gestión del tráfico, estaciones de carga eléctrica, gestión de parking, gestión de flotas de vehículos de emergencia), los servicios de atención sanitaria (monitorización remota de pacientes mediante sensores biométricos), logística (rastreo en tiempo real de inventarios y flotas),

agricultura (sensores para monitorizar cultivos y optimizar el uso de agua y fertilizantes) y automotriz (con vehículos conectados que ofrecen conducción asistida y servicios inteligentes)".

En consecuencia, el desarrollo del IoT está siendo impulsado por varias tecnologías emergentes, entre las que destacan la inteligencia artificial (IA), el edge computing, el blockchain y, especialmente, las redes 5G. Según un informe de Inserty, la integración de IA con IoT permite el análisis de grandes volúmenes de datos en tiempo real, optimizando procesos y mejorando la toma de decisiones. Del mismo modo, el edge computing reduce la latencia al procesar datos cerca de su origen, algo crucial para aplicaciones industriales y de automatización.

Está claro que las redes 5G juegan un papel fundamental en la expansión del IoT al ofrecer una mayor capacidad de dispositivos conectados, menor latencia y mayor eficiencia energética.

Las aplicaciones más emergentes del IoT se encuentran en las ciudades inteligentes, los servicios de atención sanitaria, la logística, la agricultura y el sector automotriz

Sobre esto, en opinión del el Enterprise Sales Director Iberia de Ericsson, las redes 5G son esenciales para el desarrollo del IoT, ya que permiten una mayor capacidad de dispositivos conectados y una mayor eficiencia energética, "actualmente, los sectores que más están apostando por IoT son: Automoción: Mejora la seguridad y eficiencia mediante vehículos conectados. Transporte: Optimiza rutas y gestión de flotas en tiempo real. Energético: Facilita la gestión de redes inteligentes y eficiencia energética. Defensa y seguridad: Aumenta la precisión y control en operaciones con sensores y drones. Logística: Monitorea y optimiza cadenas de suministro y transporte".

Apps más usadas e interoperabilidad

El Internet de las Cosas (IoT) ha encontrado aplicaciones en una amplia variedad de sectores, desde la manufactura hasta la salud, pasando por el hogar inteligente y las ciudades conectadas. Según un informe de McKinsey, las aplicaciones más comunes del IoT incluyen la gestión de activos, el monitoreo de condiciones, la automatización de procesos y la optimización de la cadena de suministro. Estas aplicaciones permiten a las empresas mejorar la eficiencia operativa, reducir costos y ofrecer mejores servicios a sus clientes.

Pedro L. Martinez Busto destaca que las aplicaciones de IoT más utilizadas se

encuentran en la gestión de oficinas, el sector residencial y la industria hotelera, “en las oficinas, el IoT se está utilizando para gestionar de manera eficiente las salas de reuniones o la climatización. En el sector residencial, la domótica lleva años creciendo de forma sostenida, centrándose sobre todo en el control de la iluminación y la calefacción. Por su parte, los hoteles están adoptando soluciones conectadas para gestionar la temperatura y los accesos, lo que mejora tanto la experiencia del cliente como la eficiencia operativa”.

Mientras que para Rocío Dantart, las aplicaciones más emergentes del IoT se encuentran en las ciudades inteligentes, los

servicios de atención sanitaria, la logística, la agricultura y el sector automotriz, “dentro de las áreas emergentes con mayor potencial en primer lugar están las ciudades inteligentes (iluminación, seguridad pública, gestión del tráfico, estaciones de carga eléctrica, gestión de parking, gestión de flotas de vehículos de emergencia), los servicios de atención sanitaria (monitorización remota de pacientes mediante sensores biométricos), logística (rastreo en tiempo real de inventarios y flotas), agricultura (sensores para monitorizar cultivos y optimizar el uso de agua y fertilizantes) y automotriz (con vehículos conectados que ofrecen conducción asistida y servicios inteligentes)”.

Otro punto a tener en cuenta es la interoperabilidad, un desafío crítico en el desarrollo del IoT. Según un informe de Gartner, la falta de interoperabilidad puede limitar la adopción del IoT y reducir su efectividad. Pero, ¿cómo podemos bordar este desafío?. Las empresas están adoptando estándares abiertos, protocolos comunes y plataformas de integración que facilitan la comunicación entre dispositivos de diferentes fabricantes.

Desde HPE Aruba subrayan la importancia de una estrategia integral, pues no todas las organizaciones tienen una estrategia clara y estructurada para el desarrollo del IoT, “esto no va solo de conectar dispositivos, esto trata de garantizar que estos se integren de manera efectiva con otros sistemas y que los datos generados se utilicen de forma inteligente. Servicios como IoT Operations de Aruba Central simplifican el despliegue de nuevas aplicaciones IoT y proporcionan visibilidad de los dispositivos no Wi-Fi en la red, permitiendo una estrategia más eficaz”.

Asimismo, para asegurar la interoperabilidad también es necesario cumplir con la regulación vigente y los estándares de la industria. Así lo aseguran desde Cisco, “la necesidad de cumplir con la regulación vigente y los estándares que requiere la industria, la integración con sistemas heredados, la dificultad para implementar una seguridad integral y la complejidad que implican las implementaciones a escala son algunos de los desafíos que inciden en el éxito de las estrategias IoT y el IoT Industrial”.

Desafíos de seguridad en el IoT

El Internet de las Cosas (IoT) presenta numerosos desafíos de seguridad debido a la gran cantidad de dispositivos conectados y la diversidad de fabricantes y estándares.. Además, la complejidad de las redes IoT y la falta de estándares de seguridad unificados aumentan el riesgo de brechas de seguridad.

Martinez Busto destaca la importancia de una estrategia integral de seguridad, “no todas las organizaciones tienen una estrategia clara y

estructurada para el desarrollo del IoT. Esto no va solo de conectar dispositivos, esto trata de garantizar que estos se integren de manera efectiva con otros sistemas y que los datos generados se utilicen de forma inteligente. Servicios como IoT Operations de Aruba Central simplifican el despliegue de nuevas aplicaciones IoT y proporcionan visibilidad de los dispositivos no Wi-Fi en la red, permitiendo una estrategia más eficaz"

Además, hay que tener en cuenta que la ampliación de la red IoT con múltiples sistemas interconectados crea múltiples puntos de entrada sensibles a ataques. Como bien señala Eduard Mateu Biosca, Global Product Manager IoT Solutions de Giesecke+Devrient, la falta de estándares específicos de seguridad, o políticas inadecuadas para identificar el usuario en los sistemas de autenticación y control de acceso, son un riesgo para garantizar la privacidad de dichos usuarios. El cifrado de datos, o incrementar la seguridad en el control de acceso y autenticación, pueden mitigar estas vulnerabilidades. "Estos desafíos han sido identificados por la Unión Europea como un elemento crítico para la resiliencia de las infraestructuras IoT, tal y como se recoge en la EU Cyber Resilience Act. Asimismo, organizaciones tecnológicas como la GSMA, trabajan en estándares y programas de certificación como eSA, que protegen las redes IoT ante ataques a su integridad. Giesecke+Devrient, consciente

de la relevancia de construir infraestructuras IoT resilientes a estos desafíos en seguridad, participa en estas y otras iniciativas".

Relacionado con esto, surge la pregunta sobre qué impacto tiene la tecnología Blockchain en la seguridad del IoT, y cómo están las empresas utilizando el aprendizaje automático en estas tecnologías. Y es que, según un informe de Deloitte, Blockchain puede proporcionar una capa adicional de seguridad al crear registros inmutables y verificables de todas las transacciones y comunicaciones entre dispositivos IoT. Esto reduce el riesgo de manipulación de datos y mejora la trazabilidad y la transparencia.

David Polo, Enterprise Sales Director Iberia de Ericsson, destaca cómo Blockchain y el ML están transformando la seguridad del IoT. "Las tecnologías emergentes son las que están impulsando el desarrollo del IoT, con el 5G a la cabeza. Esta red permite mayor conectividad, baja latencia y capacidad para manejar millones de dispositivos, esenciales para aplicaciones como ciudades inteligentes y vehículos autónomos.

El 5G permite la expansión de aplicaciones IoT en sectores como la manufactura, la salud, el transporte y las ciudades inteligentes, gracias a su capacidad de manejar grandes volúmenes de datos y conexiones simultáneas. Además, la IA y el aprendizaje automático permiten a los dispositivos IoT analizar datos en tiempo real, tomar decisiones autónomas y mejorar las funciones, optimizando procesos, y prediciendo fallos"

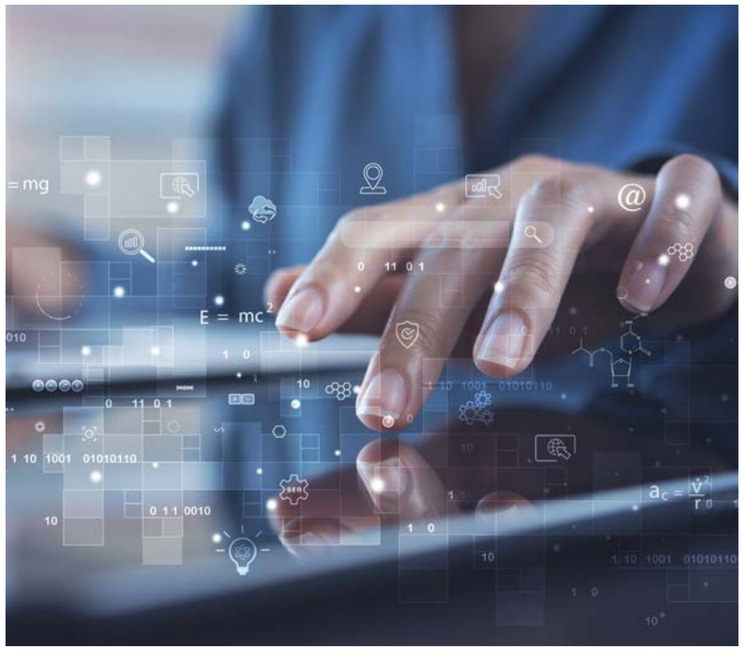
Tendencias para los próximos cinco años

El Internet de las Cosas (IoT) está en constante evolución, y las tendencias para los próximos cinco años apuntan a una integración aún más profunda de esta tecnología en diversos sectores. Según un informe de McKinsey, se espera que el IoT continúe expandiéndose, con un enfoque en la conectividad 5G, la inteligencia artificial (IA) y la sostenibilidad.

Siguiendo este punto, desde HPE Aruba, destacan que la automatización y la conectividad serán claves en el futuro del IoT, "en los próximos cinco años, veremos una mayor adopción de tecnologías como la inteligencia artificial y el machine learning, que permitirán a los dispositivos IoT tomar decisiones autónomas y optimizar procesos en tiempo real. Además, la conectividad 5G jugará un papel crucial al proporcionar la infraestructura necesaria para soportar una gran cantidad de dispositivos conectados".

Otra tendencia destacada según Cisco será la sostenibilidad y la eficiencia energética, "con el IoT ayudando a las empresas a reducir su huella de carbono y mejorar la eficiencia energética. Además, la integración de la IA permitirá un análisis más profundo de los datos generados por los dispositivos IoT, facilitando la toma de decisiones informadas y la optimización de recursos".

La inteligencia artificial (IA) también permitirá que el IoT se transforme y obtenga un análisis más avanzado de los datos y la automatización de procesos. Según un informe de Deloitte, la IA está mejorando la capacidad de los dispositivos IoT para aprender de los datos, identificar patrones y tomar decisiones autónomas.

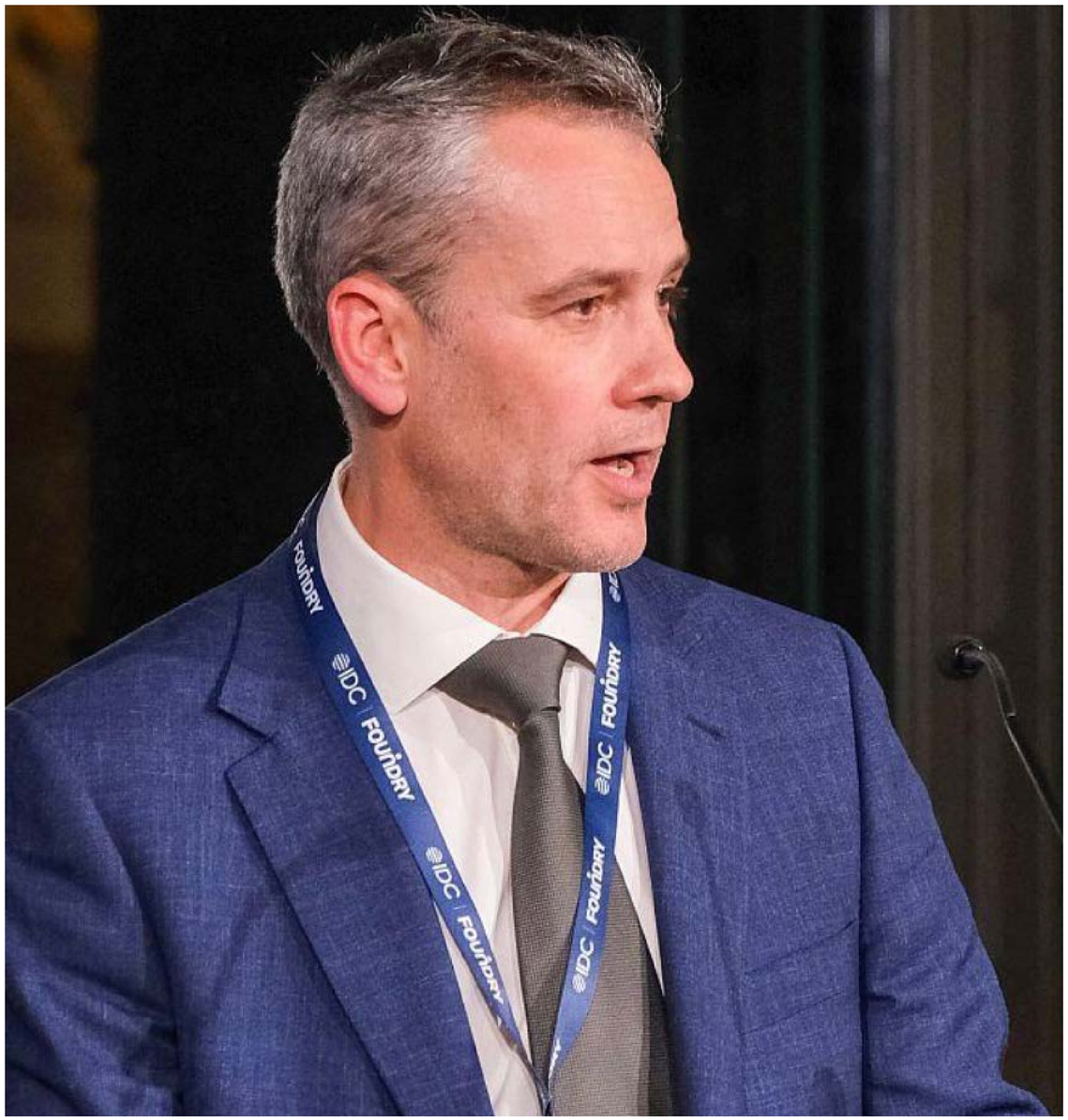


Sobre esto, desde Ericsson, recalcan el impacto de la IA en la seguridad y la eficiencia del IoT. "La IA y el aprendizaje automático están permitiendo a los dispositivos IoT analizar datos en tiempo real, tomar decisiones autónomas y mejorar las funciones, optimizando procesos y prediciendo fallos. En Ericsson, estamos aprovechando tanto el Blockchain como el aprendizaje automático para desarrollar soluciones IoT más seguras, inteligentes y eficientes. Estas tecnologías abren nuevas oportunidades para la innovación en múltiples sectores industriales".

En resumen, las tendencias para los próximos cinco años en el IoT incluyen una mayor adopción de la inteligencia artificial, la conectividad 5G y un enfoque en la sostenibilidad. Sin duda, la IA está desempeñando un papel crucial en el desarrollo del IoT, permitiendo un análisis más avanzado de los datos y la automatización de procesos. Por lo que, la combinación de estas tecnologías emergentes permitirá a las empresas maximizar el potencial del IoT y transformar sus operaciones en un entorno cada vez más conectado.

Juan Antonio Relaño Pinilla

CIO de Bosch



¿Cuál crees que es el impacto de IoT en la actualidad?
El Internet de las Cosas (IoT) está revolucionando prácticamente todos los aspectos de nuestra vida y nuestras industrias. Su impacto viene dado por la interconexión de una cantidad monstruosa de dispositivos: no solo máquinas, sino también personas, animales y ciudades enteras. Hoy en día, existen miles de millones de dispositivos conectados a internet, desde sensores industriales hasta electrodomésticos inteligentes. Además, millones de personas llevan en su bolsillo un smartphone con una capacidad de computación mucho más potente que los superordenadores que llevaron al hombre a la luna. Este vasto ecosistema ha creado un entorno donde la conectividad es omnipresente y las oportunidades de innovación son infinitas.

¿Qué tecnologías están impulsando el IoT?
5G: Permite una conectividad masiva de dispositivos con una latencia mínima, lo que es esencial para las aplicaciones críticas en tiempo real. Además, posibilita la transmisión de grandes cantidades de información a un repositorio en la nube que por comparación con datos históricos nos ayudara a establecer patrones a partir de los cuales desarrollar nuevas soluciones y servicios.

Edge Computing: El procesamiento de datos en el mismo dispositivo, cerca de donde se generan, reduce la latencia y el ancho de banda necesario, lo que es clave para aplicaciones industriales.

Sensórica avanzada. Estos sensores actúan como los "ojos y oídos" de Internet, capturando datos esenciales que permiten a los dispositivos "ver" y "escuchar" el mundo que les rodea.

Inteligencia Artificial: La IA permite analizar el enorme volumen de datos generados por los dispositivos IoT y sacar conclusiones accionables, mejorando la eficiencia operativa. Ahora hablamos del AIoT que junto con el Edge Computing permitirá a dispositivos inteligentes recoger información

del mundo exterior, procesarla, y generar un resultado sin intervención del humano.

Pensemos en el freno de emergencia de un coche. En milésimas de segundo y sin que el humano sea capaz de reaccionar, un coche es capaz de advertir la presencia de un vehículo que se aproxima a gran velocidad a través de sus sensores, la información viaja del sensor al ordenador del coche, ahí es procesada y entendida, se genera una respuesta de frenado de emergencia, que se transmite al sistema de frenado y el vehículo frena. Todo esto en milésimas de segundo y antes de que el conductor se haya percatado siquiera de que se aproxima otro vehiculo.

En el desarrollo de IoT, ¿en qué os estáis enfocando en Bosch?
En Bosch, nos hemos centrado en el desarrollo de la Industria 4.0, donde el IoT juega un papel crucial. Una de nuestras principales apuestas es la "Fábrica del Futuro", una fabrica en la que solo el suelo y el techo son fijos. El resto del espacio es flexible y modular, permitiendo una producción personalizada en función de los requerimientos de nuestros clientes. Aquí, las comunicaciones M2M (Machine to Machine) y el análisis de datos, habilitados por redes 5G, mejoran la eficiencia y la productividad de manera radical. En Bosch, estamos volcados en lograr que nuestras fábricas sean más inteligentes y capaces de adaptarse en tiempo real a las demandas del mercado. También estamos

> **En Bosch, nos hemos centrado en el desarrollo de la Industria 4.0, donde el IoT juega un papel crucial**

implementando IoT en el ámbito de la movilidad conectada, donde nuestros sensores proporcionan datos que mejoran la seguridad y eficiencia de los vehículos. En la gestión energética, utilizamos dispositivos conectados para controlar y optimizar el consumo energético en fábricas y edificios.

¿Qué casos de uso propios de IoT estáis utilizando en Bosch?
El IoT está integrado en múltiples áreas de Bosch. Uno de los casos de uso más avanzados es el mantenimiento predictivo. Utilizamos sensores y datos en tiempo real para anticipar posibles fallos en maquinaria, lo que minimiza tiempos de inactividad y maximiza la productividad. Otro ejemplo es el control de calidad en nuestras líneas de producción. Aquí, los dispositivos IoT y la inteligencia artificial trabajan juntos para detectar defectos en productos que de otra manera pasarían desapercibidos, mejorando la calidad y reduciendo el desperdicio.

¿La seguridad es el principal reto de IoT?
Sin duda, la seguridad es uno de los mayores retos del IoT. Con la enorme cantidad de dispositivos conectados y la diversidad de los mismos, la seguridad debe ser abordada desde un enfoque integral. La seguridad de todo el sistema depende del eslabón más débil de la cadena. En la actualidad la ley de Moore y la ley de Nielsen han posibilitado que sea muy económico transformar cualquier dispositivo “thing” en un “Smart Thing”. Tostadoras y secadores con conexión WIFI son un claro ejemplo de ello, pero también una puerta de entrada a ataques cyberneticos en dispositivos que no cuentan con medidas de seguridad suficientes.

Por eso, hay que trabajar intensamente en fortalecer cada parte del ecosistema, desde los sensores hasta la nube. Los datos que se transmiten entre máquinas y dispositivos son fundamentales para optimizar procesos, pero también representan un objetivo crítico para potenciales ataques cibernéticos. La prioridad es garantizar que toda la cadena esté protegida, de modo que el IoT no solo sea sinónimo de eficiencia, sino también de confianza y seguridad.

Legalidad TIC

¿Hay que aplicar la normativa sobre IA?

JAVIER LÓPEZ, Socio de Écija Abogados

En diciembre de 2023 la artista catalana Alicia Framis anunció su deseo de casarse en el verano de 2025, en Róterdam (Holanda), con un holograma creado con Inteligencia Artificial (IA), para culminar su proyecto "The Hybrid Couple". Esto no es más que una muestra más de la inmersión de la IA en nuestras vidas, lo que está exigiendo a los Reguladores a estrechar la vigilancia sobre el uso de esta tecnología.

Así, en junio de 2024, Meta se vio obligada a paralizar su proyecto de entrenar a sus LLM utilizando contenido público compartido por adultos en Facebook e Instagram en la Unión Europea, debido a las objeciones de la Comisión de Protección de Datos de Irlanda (DPC), en coordinación con el resto de las Autoridades de Datos europeas.

Debido a la incertidumbre sobre las nuevas posibilidades que se irán abriendo con el más que previsible desarrollo de las IA, una de las cuestiones que más preocupan es la determinación de los controles éticos y legales necesarios para su correcto funcionamiento. En ese sentido, se promulgó el Real Decreto 817/2023, de 8 de noviembre, por el que se establece un entorno controlado de pruebas (sandbox), para el ensayo de sistemas de inteligencia artificial.

De esta forma, su objetivo es crear un entorno controlado de pruebas de Inteligencia Artificial y evaluar los riesgos para la seguridad, la salud y los derechos fundamentales de las personas, así como obtener guías basadas en la evidencia y la experimentación que faciliten el alineamiento con la (entonces) propuesta del Reglamento de la tecnología.

Con similares preocupaciones y pretensiones, se creó en Estados Unidos en febrero de 2024 el AI Safety Institute Consortium (AISIC), integrado por más de doscientas organizaciones especializadas en IA, programadores, académicos e investigadores, con la misión de lograr que el desarrollo y la implementación de la Inteligencia Artificial sea segura y confiable.

De esta manera, sus funciones son servir de espacio de intercambio de conocimientos y datos, participar en la investigación y desarrollo colaborativo e interdisciplinario, alcanzar una comprensión completa y efectiva del impacto de la IA en la sociedad y la economía norteamericana, facilitar el desarrollo cooperativo y la transferencia de tecnología y datos, así como la evaluación de prototipos.

La normativa sobre IA

Por lo que a España se refiere, en mayo de 2024 se presentó la "Estrategia de Inteligencia Artificial

Legalidad TIC

¿Hay que aplicar la normativa sobre IA?

2024”, plan estructurado en tres ejes, que activarán ocho palancas de acción. El Eje 1 incluye el impulso a la inversión en supercomputación, el incremento de la capacidad de almacenamiento sostenible, la generación de modelos de lenguaje para una infraestructura pública y el fomento del talento en IA. El Eje 2 pretende promover la IA en el Sector Público –Proyecto GobTechLab–, ayudar a la expansión de la IA en el sector privado –Programa Kit Consulting– y la promulgación de una futura Ley de Ciberseguridad. Y el Eje 3, se encomienda a la AESIA (Agencia Española de Supervisión de Inteligencia Artificial).

En cuanto a la normativa europea, en junio de 2024, el Consejo de la UE promulgó el Reglamento (UE) 2024/1732 del Consejo de 17 de junio de 2024 (con entrada en vigor el 9 de julio de 2024), que ha modificado el Reglamento (UE) 2021/1173 del Consejo de 13 de julio de 2021 por el que se crea la Empresa Común de Informática de Alto Rendimiento Europea (EuroHPC), para poner su capacidad al servicio de pymes y empresas emergentes de inteligencia artificial, conocidas como “Fábricas de Inteligencia Artificial”, y mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la comercialización y la utilización de la IA.

Y el 12 de julio de 2024 se publicó en el Diario Oficial de la Unión Europea (DOUE) el famoso

Reglamento de IA (Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial), que entró en vigor el 1 de agosto de 2024, y que será plenamente aplicable a los dos años desde su publicación en el DOUE, esto es, el 1 de agosto de 2026, sin perjuicio de que se han establecido diferentes hitos para la aplicación de algunas materias:

- prácticas prohibidas (6 meses)
- códigos de práctica (9 meses)
- normas de Inteligencia Artificial de uso general, incluida la gobernanza (12 meses)
- obligaciones para sistemas de alto riesgo (36 meses)

No hay que perder de vista la sanciones que prevé el Reglamento de IA, consistentes en multas de hasta 15 000 000 € o, si el infractor es una empresa, de hasta el 3 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior. En el caso de que la infracción se refiera a usos prohibidos, dicha multa podría ser de hasta 35 000 000 € o, si el infractor es una empresa, de hasta el 7 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

Asimismo, en esta línea, el pasado 5 de septiembre de 2024 se firmó por la Comisión Europea el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho, que es el primer instrumento internacional jurídicamente vinculante sobre IA, y que está abierto a la firma de otros países.

Se enfoca en que la tecnología esté centrada en el ser humano, sea coherente con los derechos humanos, la Democracia y el Estado de Derecho, y sea fiable por transparencia, solidez, seguridad, gobernanza y protección de datos; pivotando en torno al concepto de riesgo para establecer la normativa aplicable. También se pone énfasis en el apoyo a una innovación segura a través de espacios controlados de pruebas (sanbox), así como en los mecanismos de supervisión.

Mujeres TIC

Medora Miranda Valdemoro

Directora de Negocio de Tecnología, Securitas Seguridad España

Fecha de nacimiento: 03/08/1978
Hijos: 2
Hobbies: Tenis, esquí, leer, viajar, aprender...
Estudios: Ingeniera de Telecomunicaciones, Licenciada en Investigación y Técnicas de Mercado

¿Cómo llegó al mundo TIC?
Fue el entorno natural en el que empezar al terminar Ingeniería de Telecomunicaciones. Desde entonces he cambiado numerosas veces de funciones ocupando muy diversas posiciones, pero siempre relacionadas con la tecnología.

¿Qué es lo que más valora de su trabajo?
La capacidad de transformar que me proporciona y el continuo aprendizaje al que me obliga.

En su opinión ¿qué es lo que falla para que las mujeres no apuesten más por el estudio de carreras STEM?
Destacaría factores como la persistencia de estereotipos erróneos asociados a los profesionales de este sector, la falta de visibilidad sobre el enorme abanico de posibilidades que se abre una vez estudias una de estas carreras, y los fallos de un modelo educativo al que habría que darle una vuelta.

¿Cree que existe el "techo de cristal" en las empresas TIC?
En mi experiencia personal el principal techo (y no quiero decir que sea el único) es el que nos ponemos nosotras mismas. El nivel de autoexigencia que solemos imponernos nos lleva a veces a ponernos límites a la hora de acceder a puestos superiores o directivos. Tampoco podemos obviar la desigualdad que todavía persiste en el reparto del cuidado de los hijos junto con la falta de flexibilidad de muchas compañías.

¿Cuál debería ser la solución?
Educación, educación, educación… Y políticas de compañía adaptadas a los requerimientos de la vida actual.

¿Una política de cuotas puede resolver el problema?
Una política de cuotas puede ayudar, y me consta que lo está haciendo, pero no es la solución estructural. Es un "mal" necesario para luchar con la tremenda disparidad de la que partimos.

Mujeres TIC

Medora Miranda Valdemoro, Directora de Negocio de Tecnología, Securitas Seguridad España

¿Qué dificultades se encontró usted para llegar a la posición que tiene actualmente?
Curiosamente, hasta que no me creí que podía hacerlo igual o mejor que cualquiera, todo eran dificultades.

¿Qué es lo que más valora de su empresa con respecto a la integración de la mujer?
Que en ningún momento he percibido que se hiciera ningún tipo de diferenciación a nivel laboral en función del sexo por ningún miembro de la compañía, y que se prima la aportación al negocio y la productividad frente al presentismo y las jornadas laborales inflexibles.

¿Cómo compatibiliza su vida laboral con la personal?
Mi compromiso con la empresa es total y mi aportación no se mide por las horas que paso en la oficina. Esto me permite organizarme y compatibilizar. Además, a nivel personal, mi pareja y yo tenemos un peso similar en el cuidado de los niños

¿Tiene su empresa planes para poder compatibilizar ambas?
En Securitas tenemos implantadas medidas de conciliación según las funciones y las condiciones personales, incluyendo horario flexible o días de teletrabajo, así como numerosas adaptaciones y condiciones especiales para trabajadores con menores o dependientes a su cargo, familias monoparentales, etc.

¿Qué cree que hay que mejorar en general para que se pueda compatibilizar mejor la vida privada o personal? ¿Es un problema de las empresas, de las relaciones de pareja o de uno mismo?
Yo creo que es una mezcla de las tres. Es clave que se alcance un equilibrio real en las parejas a la hora del cuidado de los niños y esto a veces no se tiene, precisamente, por las propias mujeres, que tienen el falso convencimiento de que es algo que deben echarse a las espaldas. Adicionalmente, las empresas deben poner mecanismos y educar a los mandos y a los directivos en el sentido de que en lo que tenemos que avanzar en este país es en productividad, no en echarle horas y horas y que estas además tengan que ser necesariamente presenciales.

¿Le han servido los estudios que hizo para realizar su labor actual?
Cuando estudias una ingenieria, del tipo que sea, estas preparada para muchísimas posiciones laborales, independientemente de los conocimientos concretos del puesto o la industria, que se pueden adquirir. En mi caso, diría que sí.

Solucione el problema de la educación en España...
Nuestro modelo educativo ha evolucionado a un ritmo más lento de lo que lo han hecho los avances tecnológicos y las opciones laborales que surgen asociadas a los mismos. Por eso es necesario un reenfoque integral del sistema para conseguir que los estudiantes conozcan y visualicen estas múltiples opciones.

Si tuviera que aconsejar a un joven qué estudiar de cara a obtener un futuro laboral estable, ¿por dónde le orientaría?
Lo primero que le diría es que estudie lo que le guste: cuando a alguien le gusta lo que hace, es más sencillo tener un futuro laboral. Lo segundo sería que valore muy seriamente las carreras STEM, ya que probablemente no conozca la enorme variedad de posibilidades que le abren para elegir trabajo ahora y en el futuro.

¿Hacia dónde cree que va el sector TIC? En su opinión, ¿cuáles van a ser las tendencias que realmente van a transformar la sociedad?
Ahora mismo tan solo podemos vislumbrar como va a ser el mundo del futuro gracias a las nuevas tecnologías. No podemos ni imaginar las posibilidades y, como no podía ser de otra manera, los riesgos, a los que nos vamos a enfrentar.
Pero estoy segura de que, si somos capaces de aprovecharlas, y creo que así será, podremos hacer de este mundo un lugar mucho más interesante, seguro, justo e igualitario de lo que es ahora.

Un CIO en 20 líneas

"Sanitas es innovación para cuidar personas"

José Luis Ruiz

CIO de Sanitas y Bupa Europe & LatinAmerica

Sanitas lleva tiempo potenciando sus procesos de transformación digital, lo que la ha convertido en una de las empresas de referencia del sector sanitario por ello. Buena parte de la responsabilidad de esa modernización corresponde a la labor llevada a cabo por José Luis Ruiz, CIO de Sanitas y Bupa Europe & LatinAmerica.

Aunque ocupa esta posición desde abril de 2023, Ruiz lleva trabajando en el área tecnológica de la compañía desde abril de 2021 donde era el director de Arquitectura y Desarrollo de IT. Este doctor e ingeniero de telecomunicaciones por la UPM ha impulsado en Sanitas, diversos proyectos de digitalización como la modernización y migración al cloud del core asegurador de Sanitas, proyectos de transformación digital o la internacionalización de la plataforma BluaU para los países de Bupa Europe & LatinAmerica. José Luis, recibió hace unos días a un reducido grupo de medios especializados, entre los que se encontraba Byte TI, en los que explicó cuál es la labor del departamento que dirige y cuáles son los principales retos a los que se enfrenta.

El departamento de tecnología de Sanitas se caracteriza por una alineación perfecta con los objetivos que persigue la organización. Tal y como explica el CIO de la compañía, "nuestro objetivo no es otro que cuidar a las personas y cuidar de la salud. Esto se palpa en nuestros hospitales, en nuestras clínicas, en nuestros centros de atención y también en nuestras residencias de mayores. Nosotros cuidamos de la salud de las personas y lo

Un CIO en 20 líneas

José Luis Ruiz, CIO de Sanitas y Bupa Europe & LatinAmerica

hacemos claramente apoyándonos en la innovación.

La salud digital

Uno de los conceptos de los que más orgulloso se muestra José Luis Ruiz es la apuesta que lleva haciendo la organización por la denominada salud digital. Blua es una plataforma que complementa las instalaciones hospitalarias y acerca los cuidados asistenciales a las personas gracias a la digitalización. El éxito de la plataforma, tal y como explica Ruiz nace de su servicio de vídeo-consulta que ya está consolidado: "El año pasado realizamos alrededor de 800 000 vídeo-consultas y llevamos más de 3 millones de vídeo-consultas desde que lanzamos la plataforma. En Sanitas fuimos pioneros en ese sentido porque nosotros ya teníamos este servicio antes de que irrumpiera la pandemia. Es cierto que, al principio, costó un poco porque muchas personas dudaban. Siempre hemos estado acostumbrados a ir al médico, queríamos que nos ausculte, que nos observe… Muchas veces, la incorporación y el éxito de la tecnología depende de la actitud de las personas y, en este caso, poco a poco, la gente empezó a confiar en ello. Tal es así que ya no solamente hacemos la vídeo-consulta, es que ya mandamos la receta y la mandamos con un QR para que el paciente vaya directamente a la farmacia a comprar el medicamento".

Fruto de ese éxito se fue desarrollando la plataforma Blua a la que se le fueron incorporando distintos servicios digitales y aplicaciones. Blua ofrece a los clientes de Sanitas diversas herramientas digitales de prevención, diagnóstico y cuidado digital como los programas digitales de salud donde nutricionistas, entrenadores personales, psicólogos y otros profesionales de la salud diseñan planes personalizados y realizan un seguimiento para que el cliente alcance los objetivos marcados. También tendrán acceso a Evalúa tus síntomas, un asistente médico virtual que ofrece triaje y pre-diagnóstico a los pacientes, derivándoles, si fuera necesario, a consulta presencial o videoconsulta.

La innovaciones en Sanitas son continuas. El último servicio incorporado a la plataforma es "Chequea tu Salud". "Se trata de un servicio que hemos desarrollado en el que el paciente puede comprobar cuál es el estado de su audición, de su vista o de su corazón. Es como si fuera un chequeo médico sólo que ese chequeo lo realizas tú en tu móvil. Somos una empresa que innovamos pensando en el paciente. El año pasado lanzamos "Cuida a tu Mente", un servicio de salud digital orientado a problemas psicológicos. Se trata de utilizar la tecnología para hacer un prediagnóstico, para cualificar el nivel del problema y el tipo de problema que pueda tener un paciente para derivarle, si lo necesita, al especialista".

La seguridad, prioritaria

Al igual que para todas las empresas, la seguridad es un factor quizá más relevante en una compañía como Sanitas, que maneja una gran cantidad de datos sensibles. Tal y como explica Ruiz, "todo lo que tiene que ver con tecnología y con nuestra estrategia es que lo hagamos de una forma segura. Manejamos muchos datos sensibles y tenerlos protegidos es algo que nos lleva mucho tiempo, mucho esfuerzo y mucha dedicación. Para Sanitas es una prioridad que la seguridad sea parte del diseño de cualquier desarrollo que llevemos a cabo. No podemos permitirnos que no sea así".

Los procesos internos

Si se quiere dar un buen servicio en un entorno seguro, la modernización de las plataformas con las que opera Sanitas es esencial. El CIO de la compañía explica que "hemos conseguido llegar a un 90% de modernización de nuestras aplicaciones apoyándonos en el cloud. Para nosotros la nube no es un lugar al que llegar, sino un entorno en el que podamos desarrollar aplicaciones con unas características concretas: que sean resilientes, que no se caigan, que se puedan modificar rápido. La nube significa que si tienes un encargo de negocio de hacer un proyecto, lo puedas hacer en semanas y no se tarde meses en poder entregarse. Por eso, nos hemos marcado como objetivo que para el siguiente ciclo estratégico, todo, el 100%, se encuentre en la nube".

Aplicación Práctica

Digitalización con propósito: el ejemplo de FUNDACIÓN JUAN XXIII

FUNDACIÓN JUAN XXIII, una organización sin ánimo de lucro, lleva más de 55 años trabajando para la inclusión sociolaboral de personas en riesgo o situación de vulnerabilidad psicosocial, especialmente con discapacidad intelectual y/o enfermedad mental. Lejos de lo que pudiera pensarse, tras esa definición se esconde una entidad que apuesta por la digitalización como fórmula para dar todo tipo de servicios de TI a empresas y organizaciones para cumplir con su propósito social.

Cualquier organización que tenga que solucionar algún tipo de necesidad tecnológica va a recurrir a la ayuda de un fabricante TIC o a una consultora que le ayude a implementar y desarrollar un proyecto. Son muy pocas las empresas que conocen que, en un momento dado, una entidad sin ánimo de lucro puede resolver su problemática. Hasta que entran en un espacio como el de FUNDACIÓN JUAN XXIII y descubren que son capaces de resolver y dar respuesta a sus necesidades, con la ayuda de otros partners con los que van de la mano. Esta Fundación ofrece un amplio conjunto de servicios a las empresas. Una propuesta que va desde la logística hasta el outsourcing o servicios de marketing, entre otras. Una de las actuaciones en las que tiene una mayor experiencia y que cuenta con la confianza de múltiples empresas, entre ellas muchas pertenecientes al IBEX 35, es el área Digital Data. Esta división, dirigida por Salud Martín, se ha convertido en todo un referente en la prestación de servicios de digitalización y gestión documental a empresas, promoviendo al mismo tiempo el empleo inclusivo.

La historia de esta división viene de lejos. Dado que la Fundación era experta en

Aplicación Práctica

Digitalización con propósito: el ejemplo de FUNDACIÓN JUAN XXIII

la custodia de archivos y documentos, en el año 2013 empiezan a digitalizarlos. “A partir de ahí empezamos a ofrecer a las empresas escanear sus documentos con tecnología OCR para extraer los datos relevantes. Fue un salto importante, no sólo ofrecíamos la digitalización para agilizar las búsquedas de información o disponer de una copia de respaldo, sino que nos especializamos en la captura de metadatos y el tratamiento de toda esa información. Invertimos en maquinaria para escanear grandes volúmenes de documentos, en tecnología de captura de datos, en el desarrollo de un gestor documental y adaptamos las instalaciones creando un entorno donde los archivos pudieran ser manipulados y tratados con la máxima seguridad. Los servicios han ido evolucionando a lo largo de estos años y si bien seguimos siendo un proveedor de servicios de gestión documental, hemos trabajado para convertirnos en un partner de servicios BPO para acompañar a las empresas en la digitalización de sus procesos de negocio”.

Desde entonces Digital Data se ha convertido en una línea fundamental dentro del ecosistema de servicios que presta FUNDACIÓN JUAN XXIII, cuyos beneficios se destinan a su labor social para la creación de empleo de personas en riesgo o situación de vulnerabilidad psicosocial y a a seguir desarrollando proyectos e invirtiendo en i+D para proporcionar a sus clientes las mejores soluciones tecnológicas y adaptadas a sus necesidades.

En definitiva, la división se ha convertido en un actor protagonista en servicios de gestión documental y BPO, que más allá de ofrecer custodia de archivos, destrucción confidencial certificada, digitalización masiva OCR, grabación de datos y validación documental, ofrece soluciones de digitalización de procesos de negocio de la mano de partners. Esta transformación ha supuesto un reto muy importante para la organización, ya que como afirma la directora de Digital Data de FUNDACIÓN JUAN XXIII, “es imprescindible la formación continua del equipo. Acompañar a un cliente en la digitalización de un proceso implica involucrarse en sus operaciones. Nos convertimos en el back office que da soporte y agiliza procesos administrativos con ayuda de tecnología y esto implica conocer muy bien los procedimientos y políticas de gestión del dato del cliente y también manejar la tecnología que los soportan. Trabajar junto con el cliente nos permite crear un equipo de trabajo muy especializado para la prestación de su servicio”.

Digital Data se ha posicionado de esta forma, en proporcionar a las organizaciones soluciones SaaS a medida para la digitalización de sus procesos de forma segura. El proceso, además es paulatino. Salud Martín explica que “las empresas comienzan externalizando con nosotros la digitalización de los expedientes de RRHH y los procesos relacionados con el Onboarding, para pasar después a la formación y la PRL, la homologación de proveedores o la gestión y el pago de facturas, entre otros”.

Una de las grandes ventajas para las organizaciones es que, gracias a los años de experiencia de esta área en el procesamiento de datos, las empresas pueden manejar grandes volúmenes de información de manera eficiente. Pero los beneficios son múltiples tal y como enumera Martín: “Les proporcionamos a los clientes el acceso a un catálogo de soluciones SaaS y la posibilidad de integrarlas con otros sistemas como su portal del empleado o ERP. Asimismo, les ofrecemos consultoría gratuita en la digitalización de sus procesos documentales con un amplio abanico de profesionales especializados en el producto. Otra de las ventajas es que ponemos en

Aplicación Práctica

Digitalización con propósito: el ejemplo de FUNDACIÓN JUAN XXIII

marcha el PMV en fase piloto sin ningún compromiso de contratación, y todo ello apoyándonos en una red de partners de primer nivel".

La importancia de los partners

Todo este entramado que ha posicionado a FUNDACIÓN JUAN XXIII en un referente en la gestión documental y del dato de nuestro país, no sería posible si no contase con esa red de partners con la que trabaja la división de Digital Data. Como destaca Martín: "Contamos con partners de primer nivel y nuestros servicios de consultoría acompañan a la empresa de principio a fin, desde el análisis de la situación actual y recomendación de soluciones tecnológicas, hasta la puesta en marcha de pilotos e implantación final de la solución. Nosotros somos un servicio BPO de 360º. Somos las personas que están en el back office, somos el archivo donde se custodian los documentos y los datos y la logística capaz de recoger grandes volúmenes de documentación. En lo que se refiere a tecnología, poseemos desarrollos propios de gestión documental que integramos con otros sistemas, pero sobretodo, apostamos por generar alianzas estratégicas con partners especializados en diferentes tecnologías para proporcionar a nuestros clientes el mejor de los servicios. Cada cliente tiene una necesidad diferente y trabajamos adhoc, poniendo en marcha un servicio que digitalice un proceso concreto y a un precio competitivo". Efectivamente, la división trabaja con algunas de las empresas líderes en sus campos, como AWS para los entornos cloud, Fujitsu y PFU (EMEA) Limited para la digitalización de procesos documentales, IA generativa y RPA, Polytropo, para el desarrollo de soluciones de gestión documental e integración de sistemas, mientras que Factum y Enthec se encargan de la parte de ciberseguridad.

Un apartado importante es el de la firma digital que permite a las empresas firmar documentos de manera electrónica de forma segura y legal. Se trata de uno de los servicios más demandados por su facilidad de uso y su capacidad para ser empleada en diferentes entornos empresariales. Para ello cuenta con la ayuda de referentes del sector como son Seal Sign y Rubricae.

Como explica Martín, "el objetivo de contar con varios partners es porque cada uno tiene un modelo de negocio diferente que cubre distintos requerimientos. Nosotros podemos llegar a acuerdos con diferentes empresas tecnológicas. No nos cerramos a nada porque se trata de una relación que beneficia a ambas partes y sobre todo a nuestros clientes".

Para la directora de Digital Data "trabajar con partners y aliados tecnológicos es fundamental porque nos permite co-crear servicios BPO a medida y optimizar mucho los costes. Se trata de una carta de presentación muy competitiva en la que se pone en valor lo mejor de cada parte. El partner es experto en su tecnología y nosotros en el back office administrativo y la prestación de servicios de gestión documental. Es importante señalar que esta alianza beneficia a todas las partes. A nosotros nos hace más competitivos y con capacidad para liderar grandes proyectos y, por otro lado, el partner y el cliente, cuentan con un socio de servicios BPO, que más allá de la calidad y la profesionalidad, apuesta por crear impacto social con cada servicio. Nuestra misión es el desarrollo de las personas en riesgo o situación de vulnerabilidad psicosocial. Nuestro éxito más allá de los ingresos, se mide por el número de puestos de trabajo que hemos conseguido crear y por la mejora en el desarrollo personal y profesional del equipo. Gracias a los clientes y los partners, hacemos que la misión sea posible".

Tendencias

Qué aporta la FP ante la escasez de perfiles digitales

Inmaculada Ascaso, Directora en mope formación

Hay 120.000 plazas de perfiles tecnológicos sin cubrir en las empresas españolas según el informe de "Anatomía de la brecha de talento tecnológico" realizado por la asociación DigitalES, y las previsiones confirman que esta cifra aumentará: se necesitarán 1,4 millones de profesionales en España durante los próximos diez años.

En España la tasa de empleo del sector IT alcanza el 81,5 % y el 43 % de las empresas prevé contratar más profesionales tecnológicos. Actualmente el sector TIC es el líder global en contrataciones con un 31 %, pero siguen faltando profesionales formados y cualificados.

ΩSegún datos de minsait una de cada dos organizaciones utiliza ya hoy la IA para mejorar y optimizar sus procesos internos y,en concreto, para la mejora del diagnóstico y prevención de enfermedades, así como la mejora de la atención, gestión y análisis de pacientes. Por su parte, los grandes hiperescalares como Amazon, Google, Meta y Microsoft están promoviendo el desarrollo de todo tipo de herramientas impulsadas por la IA diseñadas no sólo para grandes empresas sino también para pymes.

En el caso de la ciberseguridad, las cifras hablan por sí solas sobre la necesidad de incorporar profesionales expertos en esta área. Según el último informe anual de amenazas de CrowdStrike las intrusiones en la nube han aumentado un 75 % en el último año y las víctimas de robo de datos en la darkweb han crecido un 76 %. Las empresas urgen contratar profesionales especializados en ciberseguridad: el 31 % de las empresas admite que sus departamentos de ciberseguridad carecen de personal suficiente según el último estudio de Kaspersky.

La FP y los perfiles digitales

El mercado laboral demanda perfiles profesionales TIC hiperespecializados, y la Formación Profesional, FP, da una respuesta formativa de calidad aportando la incorporación de los perfiles digitales que buscan las empresas.

La clave está en ofrecer una formación oficial de calidad que dé respuesta a las demandas de las empresas tanto en certificaciones, de la mano de partners, como de habilidades y experiencia práctica en colaboración con las empresas. La oferta formativa en España afronta, sin embargo, un gran desafío, remediar el abandono de los estudios sobre todo en materias STEM donde se incluye tanto la rama sanitaria como la tecnológica.

Según nuestra experiencia uno de los motivos principales de este abandono es la ausencia de seguimiento de los alumnos durante los primeros meses de estudios universitarios o de FP. En este sentido la OCDE ha subrayado en repetidas ocasiones la importancia de contar al menos con un orientador por cada 250 estudiantes.

En nuestro país estamos lejos de alcanzar esta cifra ya que, de media, existe un orientador por cada 750 alumnos por eso en centros de formación profesional como mope creemos que debemos centrar nuestro esfuerzo en acompañar y guiar al alumno en todo momento y por eso hemos mejorado la cifra de la OCDE de 250 a 90 porque queremos atender de una manera personalizada a cada estudiante. Actualmente tenemos un tutor para cada 90 alumnos junto con un equipo multidisciplinar y coordinado que incluye además de a los tutores, a profesores especialistas y a asesores pedagógicos.

Combinar la formación teórica con el aprendizaje práctico es otro de los retos que demandan las empresas a los que los centros de formación hemos de dar respuesta. La experiencia práctica es un pilar fundamental en la formación profesional tecnológica.

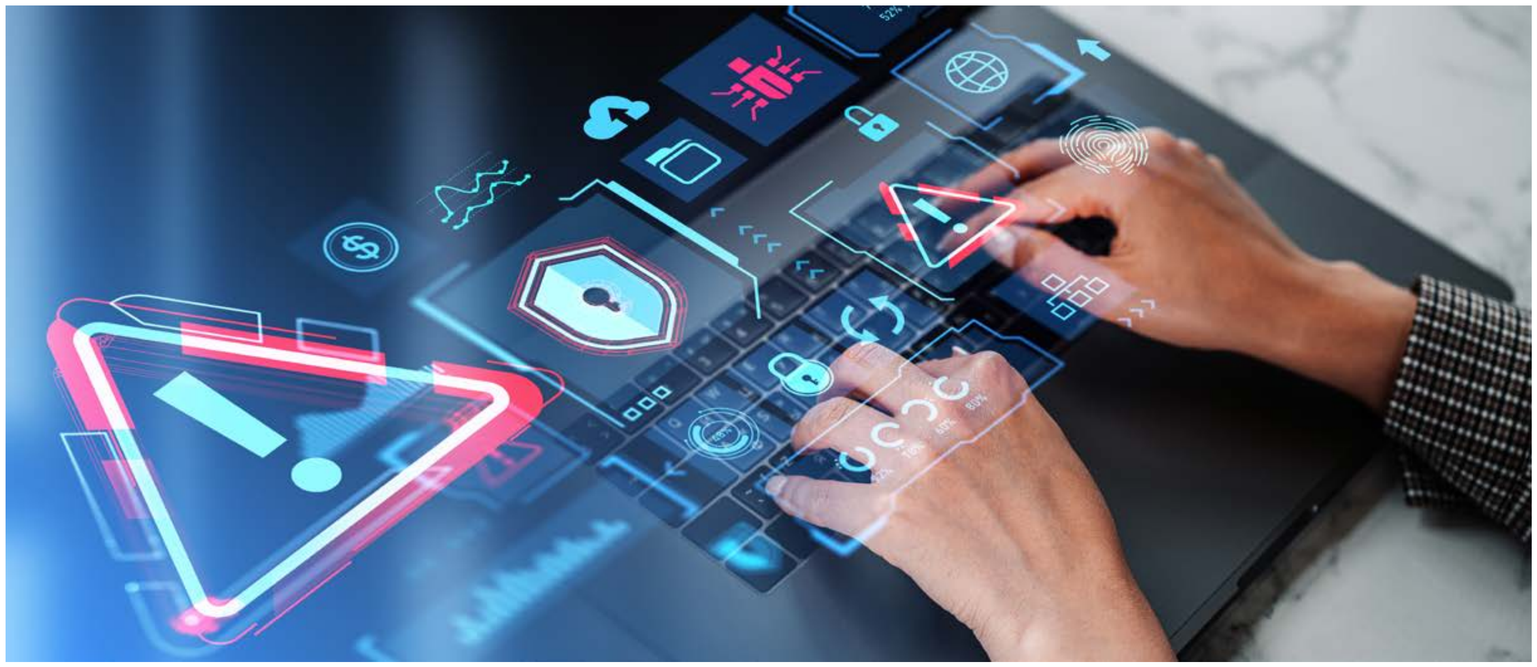
En nuestro caso, tras la experiencia de más de una década formando a más de 2.500 alumnos nacionales y extranjeros con títulos oficiales, propios y cursos de certificación, tanto en la rama sanitaria de farmacia, parafarmacia y audiología protésica como en la tecnológica, apostamos por un modelo de aprendizaje interactivo a través de clases online, pero con seminarios presenciales y prácticas en empresas que no solo ofrezcan una experiencia valiosa, sino que también complementen su formación académica con habilidades prácticas relevantes para el sector.

La Formación Profesional especializada en tecnología es la respuesta que está demandando la transformación digital que afronta la empresa hoy. Formar a profesionales de forma ágil en las competencias y habilidades tecnológicas que demanda el mercado es imperativo si no queremos quedarnos atrás en la transformación digital de nuestro país. El análisis de datos, la ciberseguridad, la inteligencia artificial y el desarrollo de aplicaciones son fundamentales para el futuro de las organizaciones, y es vital formar a profesionales preparados para estos desafíos.

Tendencias

Gestión de riesgos: medidas de ciberseguridad en NIS 2

Álvaro García Abarrio, country manager de WatchGuard



La Unión Europea ha dado un paso importante para reforzar la ciberseguridad de los Estados miembros y ha introducido la segunda versión de la Directiva sobre Redes y Sistemas de Información, también conocida como NIS 2. Esta legislación actualizada amplía la Directiva NIS original, con el objetivo de crear un enfoque más sólido y unificado de la ciberdefensa. La NIS 2 se aplica a un mayor número de organizaciones, obliga a tomar medidas de seguridad más estrictas y da prioridad a la mejora de la notificación de incidentes y el intercambio de información.

El nuevo reglamento representa una piedra angular en materia de ciberseguridad, al imponer requisitos estrictos a los sectores de infraestructuras críticas. Para garantizar la resiliencia del nuevo reglamento europeo, se han impuesto medidas específicas de gestión de riesgos de ciberseguridad. Mediante la aplicación diligente de estas medidas, las organizaciones pueden mejorar significativamente su postura de ciberseguridad y mitigar los riesgos de ciberataques. El cumplimiento de NIS 2 no consiste únicamente en evitar sanciones, sino también en proteger a una organización, a sus clientes y su reputación.

Gestión de vulnerabilidades y contención de daños: NIS2

Las empresas deben identificar, analizar y evaluar las amenazas y vulnerabilidades potenciales en materia de ciberseguridad, y también es importante comprender la exposición al riesgo de su organización y priorizar los esfuerzos de mitigación.

Mediante la identificación proactiva de las amenazas potenciales, las organizaciones pueden aplicar medidas para prevenir las brechas y minimizar su impacto.

Además de identificar una amenaza, es importante identificar y corregir las vulnerabilidades de los sistemas y el software. Esto ayuda a evitar que los atacantes exploten los puntos débiles. Mantenerse al día con los parches de software es crucial para protegerse contra las vulnerabilidades conocidas. Sin embargo, este cuidado y vigilancia pueden no ser suficientes para prevenir un ciberataque. Es esencial tener un plan bien definido para detectar, responder y recuperarse de los incidentes cibernéticos. Este plan debe incluir procedimientos de contención, eliminación y recuperación. Una respuesta rápida

y eficaz a un ciberincidente puede limitar los daños y restablecer rápidamente las operaciones.

Seguridad, control de acceso y cifrado

Dada la creciente complejidad de las cadenas de suministro, es esencial gestionar los riesgos de ciberseguridad de los proveedores evaluando sus prácticas de seguridad y aplicando controles.

Un eslabón débil en su cadena de suministro puede comprometer a toda su organización. Implantar controles de acceso sólidos garantiza que solo las personas autorizadas puedan acceder a los sistemas y datos, por lo que es una forma válida de garantizar que no haya puntos débiles en las cadenas de suministro.

Las empresas deben optar por medidas de autenticación de usuarios, autorizaciones y revisiones de acceso, ya que limitar el acceso a la información confidencial reduce el riesgo de divulgación o modificación no autorizada.

La protección de datos, mediante cifrado, es vital para mantener la confidencialidad: impide el acceso no autorizado a información sensible, incluso si los datos se ven comprometidos.

Probar, evaluar y comunicar

En el panorama actual de la ciberseguridad, la prevención y la evaluación continua ayudan a detectar puntos débiles y a mejorar la postura de seguridad de las empresas.

Medidas preventivas como el análisis de vulnerabilidades, las pruebas de penetración y las auditorías de seguridad pueden evitar que las organizaciones se conviertan en las próximas víctimas de un ataque.

Dada la nueva normativa europea, es obligatorio informar de los incidentes informáticos a las autoridades competentes. Una comunicación clara y transparente permite hacerse una idea global del panorama de las amenazas y facilita el intercambio de información. Una comunicación oportuna permite responder adecuadamente a las ciberamenazas.

Continuidad de negocio y concienciación sobre ciberseguridad

Un plan de continuidad de negocio y un marco sólido de gestión de riesgos garantizan la resistencia operativa de una organización en caso de ciberataque. Una organización bien preparada puede recuperarse más rápida y eficazmente de cualquier perturbación o incidente.

Parte del proceso de preparación en materia de ciberseguridad consiste en formar a los equipos y a todos los empleados sobre los temas de ciberseguridad más comunes: phishing, ingeniería social y seguridad de contraseñas, entre otros. Los expertos en ciberseguridad han demostrado que el error humano suele ser un factor importante en los incidentes cibernéticos y, por este motivo, la prevención y preparación ante nuevas amenazas cibernéticas depende de sus empleados y de su concienciación sobre los peligros a los que están expuestos.

En el marco de octubre, mes en el que se celebran iniciativas de concienciación sobre ciberseguridad, queremos llamar la atención sobre la necesidad de concienciar a las organizaciones y a sus equipos de que la ciberseguridad es una responsabilidad compartida que no se limita solo al mes de octubre.

Tendencias

Gestión de datos de la Industria 4.0 para optimizar las cadenas de producción

Youssef Nadiri, Product Manager Edge AI Solutions en PNY Tenchnologies

La integración de las tecnologías digitales en la industria ha alcanzado en los últimos años un nivel sin precedentes con la irrupción de la Industria 4.0. Gracias a los sensores inteligentes, la maquinaria conectada y los sistemas de gestión avanzados, las empresas tienen acceso a una ingente cantidad de información que puede ser utilizada para mejorar la producción y tomar decisiones estratégicas con mayor rapidez.

Uno de los principales retos ante una enorme disponibilidad de datos es poder extraer de ellos el valor adecuado para aprovechar todo su potencial.

Para ello, es necesario recurrir a la ayuda de tecnologías digitales avanzadas, como la inteligencia artificial (IA) y el análisis predictivo, para transformar la información en decisiones operativas. De hecho, los datos recopilados pueden utilizarse de diversas maneras: desde el mantenimiento predictivo hasta la optimización de los procesos de producción para reducir el tiempo y los costes de producción.

El potencial de los datos de la Industria 4.0

Los datos recopilados a través de la Industria 4.0 pueden utilizarse de diversas formas para mejorar numerosos aspectos del proceso de producción. Entre ellos, una de las áreas estratégicas en las que puede marcar la diferencia es el mantenimiento predictivo. Mediante el análisis de los datos de la maquinaria en tiempo real, es posible conocer el estado de las instalaciones, recopilando información sobre diversos indicadores como temperatura, vibración, presión y desgaste.

Esto permite predecir cuándo es probable que falle una máquina, de modo que se pueden planificar las tareas de mantenimiento antes de que se produzca el fallo. De este modo, no sólo se reducen los tiempos de inactividad imprevistos, sino que también aumenta la vida útil de los equipos y se reducen los costes de mantenimiento al intervenir sólo cuando es necesario y evitar intervenciones no solicitadas y fallos repentinos que provocarían la parada de la planta.

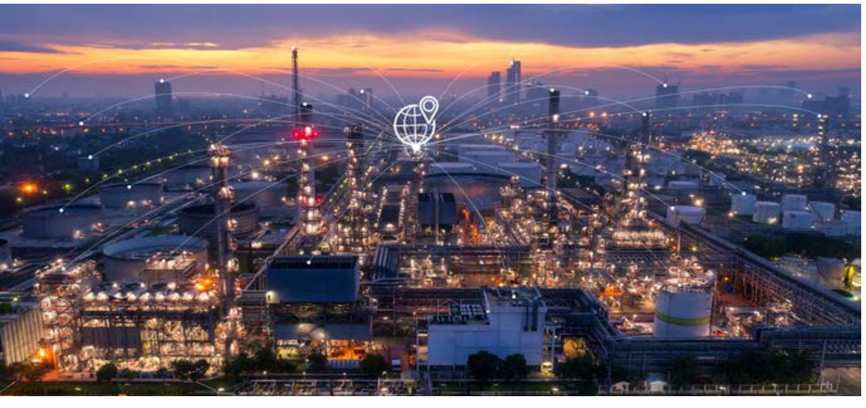
Otra aplicación útil de los datos es ayudar a optimizar los procesos de producción identificando cuellos de botella, ineficiencias y retrasos a

Gestión de datos de la Industria 4.0 para optimizar las cadenas de producción

lo largo de la cadena de producción. Por ejemplo, analizando el flujo de materiales y el comportamiento de las máquinas es posible optimizar la asignación de recursos, equilibrar las líneas de producción y mejorar la coordinación entre los distintos departamentos.

Además, el uso de datos permite realizar simulaciones para probar cambios en los procesos, como la reconfiguración de una línea o la introducción de nueva maquinaria, sin interrumpir la producción real. Las simulaciones permiten comprobar la eficacia de estos cambios antes de implantarlos físicamente, lo que minimiza el riesgo de errores.

El control de calidad en tiempo real es otro ámbito de aplicación de los Datos 4.0: gracias al uso de la analítica avanzada y la inteligencia artificial, es posible detectar inmediatamente los defectos de producción y rechazar o corregir los productos defectuosos durante el propio proceso.



Esto reduce significativamente las tasas de rechazo y garantiza que los productos finales cumplan las normas de calidad sin necesidad de un exhaustivo control de calidad al final de la producción. En lugar de realizar pruebas por muestreo, las empresas pueden supervisar cada una de las piezas producidas, lo que mejora la fiabilidad y la satisfacción del cliente.

Por último, otro ámbito estratégico es la optimización de la cadena de suministro. Gracias al seguimiento en tiempo real de materiales y productos, las empresas pueden gestionar los flujos logísticos con mayor eficacia. El seguimiento de las existencias y las entregas, por ejemplo, permite reducir los tiempos de espera, evitar el exceso o la falta de existencias y mejorar la planificación de la producción en función de la disponibilidad de materias primas.

Además, el análisis predictivo permite prever la evolución de la demanda y optimizar los pedidos y la producción en función de las tendencias del mercado. Esto garantiza que los recursos se utilicen de la forma más eficiente posible, reduciendo los costes operativos y mejorando la puntualidad de las entregas.

Una de las herramientas más avanzadas para aprovechar al máximo estas tecnologías es NVIDIA Omniverse, un entorno virtual que, junto con el uso de GPU (unidades de procesamiento gráfico), permite simular y analizar las cadenas de producción en tiempo real, reduciendo así los tiempos de inactividad y los costes de mantenimiento.

Omniverse es una plataforma de colaboración y simulación 3D que permite a equipos de ingenieros, diseñadores y técnicos trabajar juntos en un espacio virtual compartido. Gracias a la potencia de las GPU, esta plataforma permite ejecutar simulaciones complejas en tiempo real, lo que se traduce en una importante ventaja para las empresas de fabricación. Las simulaciones permiten probar y optimizar procesos sin tener que detener las líneas de producción físicas, lo que reduce los tiempos de inactividad y los costes asociados.

El uso combinado de plataformas avanzadas como Omniverse, las capacidades de cómputo de las GPU y la enorme cantidad de datos que genera la Industria 4.0 representa una auténtica revolución para las empresas. La optimización de las cadenas de producción no se limita a la fase de diseño o a la supervisión pasiva: gracias a la simulación en tiempo real y al análisis predictivo, las empresas pueden ahora anticiparse a los problemas, reducir los tiempos de inactividad y mejorar continuamente el rendimiento.

Entrevista

Igor Amantegi Vegas, responsable de Tecnología e I+D de FINNK

“La IA debe de ir jugando cada día un papel más relevante y ayudarnos a ser óptimos y eficientes”

Finnk ha lanzado una plataforma de inversión 100% digital que ofrece acompañamiento personalizado mediante algoritmos y el uso de Inteligencia Artificial. La plataforma incluye tres modelos de gestión para carteras diversificadas: IAvanzada, Sostenible y Tendencias, ideales para maximizar inversiones a largo plazo. Para profundizar sobre esto y más, contamos con Igor Amantegi Vegas, responsable de Tecnología e I+D de FINNK.

VANESA GARCÍA

¿Qué es Finnk y qué ofrece?
Finnk es una innovadora plataforma financiera, especializada en carteras de fondos de inversión, diversificadas y a largo plazo. Es una plataforma que facilita a los ahorradores y ahorradoras la posibilidad de diversificar sus inversiones

Entrevista

Igor Amantegi Vegas, responsable de Tecnología e I+D de FINNK

sin requerir conocimientos financieros y ofrece un seguimiento digital único que permite monitorizar el progreso de los objetivos en todo momento. En Finnk ofrecemos tres modelos diferenciados de gestión, aplicados a carteras con elevado peso de renta variable, óptimas para maximizar una inversión a largo plazo y dirigidas a perfiles arriesgados y/o decididos:

Avanzada: modelo de inversión, cuantitativo y automatizado, basado en un modelo algorítmico de última generación, creado por Inteligencia Artificial, en la selección de los activos y su peso dentro de la cartera

Sostenible: modelo de inversión orientado a la promoción de la sostenibilidad ambiental, social y de gobierno corporativo

Tendencias: modelo de gestión activa, basado en la inversión en tendencias globales destinadas a transformar el mundo

¿En qué se diferencia de otros competidores?

Creemos firmemente que la sociedad necesita afrontar sus metas con herramientas que permitan realizar una buena gestión de su economía. Sabemos también que muchos inversores no tienen conocimientos profundos de los mercados. Sabemos lo importante que es para cada cliente cada pedacito de su ahorro. Finnk da respuesta a estas cuestiones, de forma que nuestros clientes, con inversiones de un mínimo de 1.000 euros, pueden ponerse en manos de grandes expertos, y sentirse en todo momento acompañados en la persecución de sus objetivos de forma 100% digital.

¿Qué función desempeña la IA en su oferta?

Finnk cuenta con un amplio abanico de gestoras y fondos de inversión. Para la elección de cuáles son los mejores instrumentos para cada momento se deben de tener en cuenta muchos factores: diversificación, optimización, predicción, sostenibilidad... y ahí es donde la IA ayuda en la toma de decisiones y en la contención de los riesgos. Por otro lado, tenemos claro que en cada puesto de trabajo del equipo Finnk, la IA debe de ir jugando cada día un papel más relevante y ayudarnos a ser óptimos y eficientes.

¿Cómo es el proceso de alta de clientes? ¿Qué papel juega la tecnología?

El proceso de OnBoarding cuenta con herramientas que digitalizan el proceso cumpliendo todos los requerimientos regulatorios, que en nuestro sector son muy exigentes. Contamos con la tecnología de vanguardia para captación de los datos del DNI y del cliente de forma que el proceso se pueda realizar en cualquier momento, en cualquier lugar, con la mejor experiencia posible y la mínima introducción de datos por el cliente. Todo ello tutelado por un servicio de atención que se vuelca para que éste se encuentre acompañado desde el principio.

En un sector tan regulado, entiendo que garantizar la seguridad es fundamental. ¿Cómo lo han hecho?

En Finnk la seguridad lleva siendo desde su nacimiento la piedra angular de nuestro Sistema de Gestión de los sistemas de información, preocupándonos en todo momento de garantizar la confidencialidad, integridad, seguridad, y continuidad de negocio. Se han cubierto las nuevas exigencias regulatorias con el máximo rigor, tanto por nuestra área de cumplimiento normativo como por todos los departamentos involucrados.

¿Consideran que el mercado está maduro para un servicio como Finnk?

Eso es lo que dicen nuestros estudios; hay un importantísimo nicho de clientes potenciales a los que enamorar. Además, los datos demuestran que todavía hay mucho más camino por recorrer. Si nos comparamos con respecto a EEUU y Europa, en nuestra sociedad existe un importante gap en cuanto a conocimiento de herramientas de inversión y de conceptos como salud financiera.

Cibercotizante

José Joaquín Flechoso
Presidente de Cibercotizante

El crecimiento de perfiles en inteligencia artificial

Aunque parezca contradictorio, no tenemos claras cuáles son las demandas y los puestos concretos que el sector digital está buscando pues se da la paradoja de que con unas tasas de empleo joven todavía muy altas en España y a la vez con una fuerte demanda de sectores buscando profesionales, deberíamos tener claro cuáles son los profesionales que se están buscando y en qué puestos en concreto.

Es evidente que la demanda de ingenieros está cada vez más presente en nuestro sector, pero la de contrataciones de nivel técnico procedente de la formación profesional es cada vez más alto, según se desprende del informe de DigitalES “Radiografía de empleos y sectores emergentes” publicado recientemente por la mencionada patronal del sector tecnológico español, donde se afirma que las principales empresas están casi en el 30% de contrataciones procedentes de la FP.

Destaca el informe de DigitalES el gran empuje del mercado de las Open RAN donde se prevé un crecimiento a nivel mundial del 42 % hasta 2030 y también de tecnologías como el gemelo digital o la supercomputación, pues recordemos en 2018, se creó la Empresa Común Europea de Computación de Alto Rendimiento (EuroHPC Joint Undertaking) una iniciativa de colaboración público-privada a nivel continental que tiene como objetivo posicionar a Europa como un líder mundial en supercomputación.

En una reciente entrevista, Miguel Sánchez Gallardo director general de DigitalES afirmaba: "España necesita incorporar al sector digital 1,5 millones de personas", dato muy relevante que coincide con una llamada de atención muy importante que destaca el informe, en lo relativo a la demanda de profesiones en tecnología, que evidentemente ha estado siempre en un constante crecimiento y ahora no se produce, es cierto que esa ralentización se concreta al periodo 2023-2024, tras aquel momento de brutal crecimiento marcado por la pandemia, que cambió totalmente la forma de trabajar, de comunicarnos e incluso la forma de reunirnos.

Realmente no quiere decir que se esté destruyendo empleo, a pesar de algunos despidos masivos en grandes empresas multinacionales del sector que aprovecharon el COVID-19 como momento álgido para contratar personal. Es una evidencia que el crecimiento se está ralentizando, no solo en el sector digital, sino en toda la economía. Estamos en tiempos de ajuste y debemos ir con cautela.