

# ¿CÓMO GESTIONAR DE FORMA EFICAZ LA EMPRESA Y SUS CLIENTES?



- LA ERA DEL BANKING AS A SERVICE
- EL TRABAJO HÍBRIDO, ¿EMPIEZA A SER UN MITO?

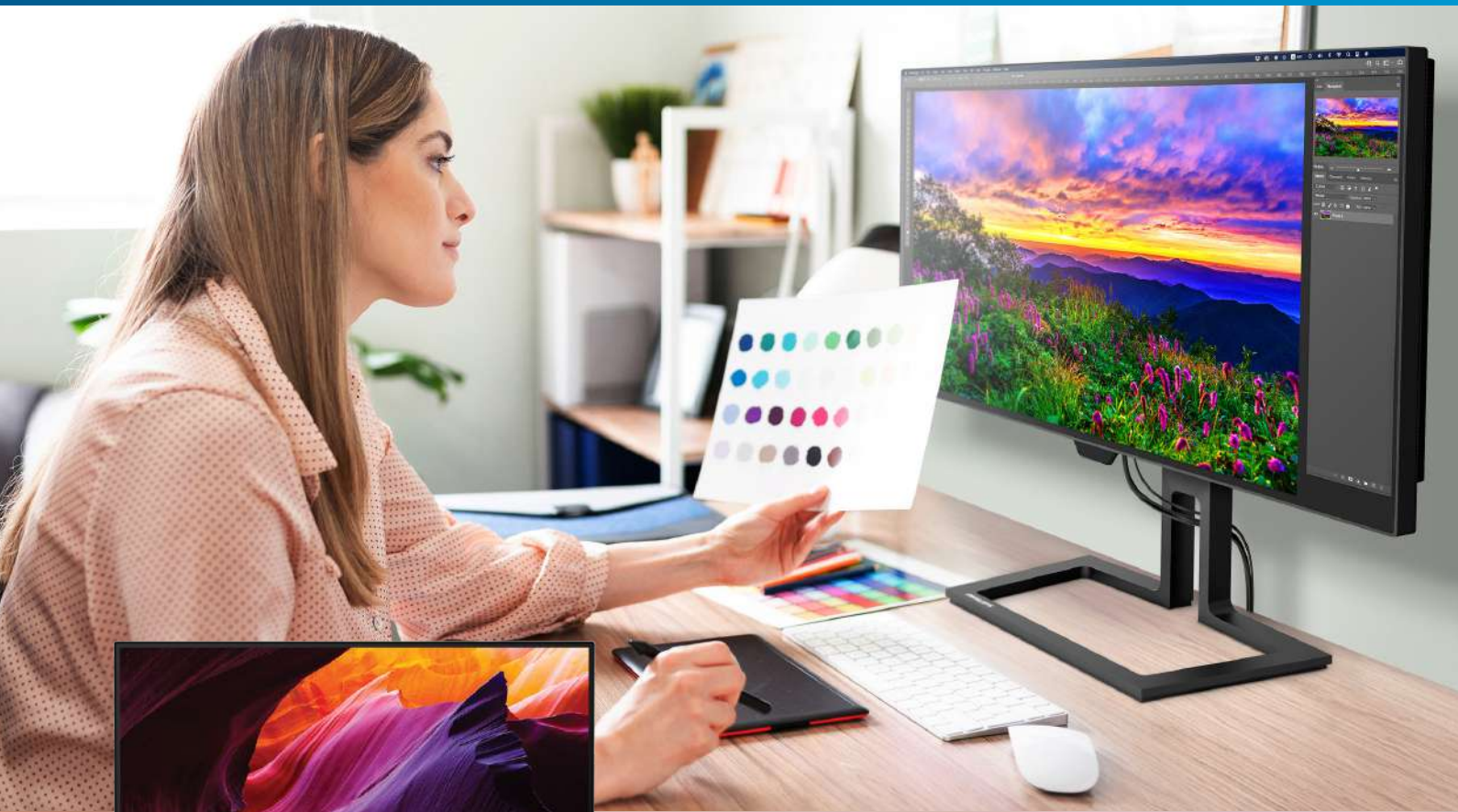
**COMPARATIVA**  Soluciones de ciberseguridad cloud

# PHILIPS

Monitores

## Sencillemente brillante

### MiniLED con Thunderbolt docking



Brilliance 7000  
27" (68.6 cm) | Mini LED | Thunderbolt 4 | 4K UHD

27B1U7903/00

innovation  you





# ¿Y si las sanciones no afectan a Huawei?



Manuel Navarro Ruiz  
Director de BYTE TI

Una de las características de la presidencia de Donald Trump fue su animadversión hacia todo lo que llevase el nombre de China. En esa guerra silenciosa, que Joe Biden sigue manteniendo, la tecnología sigue jugando un papel más que importante.

Una de las acciones que más impacto tuvo en las políticas estadounidenses fue el veto a Huawei. Desde el año 2019, la multinacional china tiene el acceso limitado a herramientas de fabricación de chips esenciales que le permiten producir los modelos de teléfonos más avanzados. Con esa limitación, la firma que hasta esa fecha podía competir con los líderes Apple y Samsung, vio como no tenía capacidad para fabricar smartphones de última generación ya que no tenía acceso a los chips 5G y sólo pudo utilizar aquellos chips que ya tenía almacenados.

Esas mismas limitaciones hicieron que muchas operadoras dejaran a la multinacional china a un lado en sus desarrollos de redes 5G. La razón en ambos casos era que Huawei representaba un serio riesgo para la seguridad de las democracias occidentales.

Los sucesivos vetos, llevaron a la división de móviles de Huawei a la hecatombe en los mercados occidentales, donde en la actualidad no se encuentra ni entre los 10 primeros fabricantes de smartphones. No pareció importarle mucho, toda vez que cuenta con uno de los mercados más importantes del mundo como es el chino para seguir vendiendo ter-

minales. Eso y, por supuesto, el apoyo que le presta el régimen de Xi Jinping. Sin embargo, a pesar de todos los obstáculos que se le han ido poniendo por delante, este mes Huawei ha anunciado un nuevo móvil que parece que ya está a la altura de los mejores modelos 5G del mercado actual. Se trata del Huawei Mate 60 Pro que los medios chinos han calificado como la prueba del fracaso de la estrategia occidental.

Y es que, algunas pruebas que se han realizado sobre el nuevo modelo, alcanzan incluso velocidades superiores a algunos de los mejores modelos de las empresas con más tradición en el mundo de los smartphones.

La duda que queda con este nuevo teléfono es que si Huawei y China son capaces de producir sus propios procesadores 5G, marcaría un avance significativo en las capacidades de la industria tecnológica china a la que se suponía que se le había dado un gran golpe del que tardaría años en recuperarse. En poco tiempo veremos que esconde el nuevo smartphone.

# SUMARIO

TEMA DE PORTADA

## La evolución

# del ERP y el CRM

# 44

N.º 318 • ÉPOCA IV

**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**

Javier Palazon

**Colaboradores**

R. de Miguel, I. Pajuelo, O. González,  
M. López, F. Jofre, A. Moreno, M<sup>a</sup>J. Recio,  
J.J. Flechoso, D. Puente, A. Herranz, C.  
Hernández.

**Fotógrafos**

P. Varela, E. Fidalgo

**Ilustración de portada**

Javier López Sáez

**Diseño y maquetación**

El Palíndromo Comunicación S.L.

**WebMaster**

NEXICA

www.nexica.es

**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

**PUBLICIDAD**

Directora comercial: Isabel Gallego  
(igallego@mkm-pi.com)

Tel.: 91 632 38 27

Natalie Awe (nawe@mkm-pi.com)

**DEPARTAMENTO DE SUSCRIPCIONES**

Tel. 91 632 38 27

Fax.: 91 633 25 64

e-mail: suscripciones@mkm-pi.com

Precio de este ejemplar: 5,75 euros

Precio para Canarias, Ceuta y Melilla:

5,75 euros (incluye transporte)

**Impresión**

Gráficas Monterreina

**Distribución**

DISPAÑA

Revista mensual de informática

ISSN: 1135-0407

**Depósito legal**

B-6875/95

© Reservados todos los derechos

Se prohíbe la reproducción total o parcial por ningún medio, electrónico o mecánico de los artículos aparecidos en este número sin la autorización expresa por escrito del titular del Copyright. La cabecera de esta revista es

Copyrightsafdsfcdscsdagtdhgvakjbsdvckjbcksdscj-baskcjbksdcjbsdclbt de Publicaciones Informáticas MKM. Todos los derechos reservados. Publicado con la autorización de Publicaciones Informáticas MKM. La reproducción de cualquier forma, en cualquier idioma, en todo o parte sin el consentimiento escrito de Publicaciones Informáticas MKM, queda terminantemente prohibida. Byte TI es una marca registrada de Publicaciones Informáticas MKM.

SEPTIEMBRE 2023

Printed in Spain



**EDITA**

Publicaciones Informáticas MKM



ACTUALIDAD



6

3 CARTA DEL DIRECTOR

6 ACTUALIDAD

22 WEBINARS y  
ENCUENTROS BYTE TI

34 COMPARATIVA

44 TEMA DE PORTADA

52 MUJERES TIC

54 UN CIO EN 20  
LÍNEAS

56 LEGALIDAD TIC

58 TENDENCIAS

64 ENTREVISTA

66 CIBERCOTIZANTE

COMPARATIVA



32

TENDENCIAS



58

# Estos son los finalistas a mejor CIO del año de los Premios Byte TI

El próximo 28 de septiembre se celebrarán los tradicionales Premios Byte TI 2023. Entre los galardones se encuentran el de "CIO del Año". Estos son los finalistas de esta edición y los proyectos que se han valorado

### FINALISTAS AL PREMIO CIO DEL AÑO



Teresa Capella,  
CIO de Banca March

Banca March aspira a ser referencia en banca privada y asesoramiento a empresas apoyándose en la mejor tecnología como punto clave de su estrategia de crecimiento.



Mónica González Arrebola,  
South West Europe CIO at PepsiCo

El proyecto ha consistido en el desarrollo y despliegue de una app para nuestros clientes del canal tradicional que les permite realizar sus pedidos de forma digital.



Rubén Andrés Priego,  
CIO de EVO Banco

La hipoteca 100% digital Open Banking se destaca por su enfoque API First, permitiendo la integración sencilla de prescriptores digitales a través de APIs



José Antonio Pérez,  
CIO de Bergé

Transformación del proceso operativo de operaciones portuarias de producto agroalimentario granel basada en la gestión centralizada de todas las operaciones de los puertos.



Mercedes Barreiro, Directora de Sistemas y Transformación Digital de Grupo Vithas

La hipoteca 100% digital Open Banking se destaca por su enfoque API First, permitiendo la integración sencilla de prescriptores digitales a través de APIs



Sergio Peinado,  
CIO de Correos

Proyecto de Voto-Elecciones Municipales y Generales. Tres ejes: Transformación Canal Digital; Evolución de Backoffice Canal Físico; Transformación de sistema analítico.



Carlos Garriga,  
CIO de IE University

Creación y despliegue de un ecosistema dentro de IE University para enseñar a través de tecnologías VR/AR



Beatriz Marco,  
CIO de Cantabria Labs

Mejorar la experiencia de clientes en farmacia, a través de una nueva plataforma de farmacias; Mejorar la experiencia de los empleados a través de un Programa de capacitación



David Vaquero,  
director de tecnología de Nationale-Nederlanden

Creación de un espacio que favorezca el desarrollo de skills necesarias para entender y poder adoptar un nuevo abanico de nuevos paradigmas de soluciones, integración y operación



Manuel Tarrasa,  
CIO y CTO de Prosegur

Desarrollo del proyecto Cyclone a fin de superar retos de escalabilidad, eficiencia y ciberseguridad, logrando satisfactoriamente sus expectativas.



# Y estos, los finalistas a mejor CISO del año de los Premios Byte TI

Como novedad y, dada la importancia que está teniendo la ciberseguridad en las organizaciones, en las que cada vez más apuestan por la creación de un departamento específico, los Premios Byte TI incorporan la candidatura de "CISO del Año"

## FINALISTAS AL PREMIO CISO DEL AÑO



Esther Muñoz,  
subdirectora general de tecnología de Madrid Digital

Con el Centro de Operaciones de Ciberseguridad de Madrid Digital – SOCMD, se ha conseguido centralizar y fortalecer las capacidades de ciberseguridad de la organización.



Gabriel Moliné,  
CISO de Leroy Merlin

Crear una sinergia entre las medidas de seguridad que teníamos implementadas entre nuestra ámbito físico y nuestro ámbito digital, a través de la estandarización de alertas y respuestas



Manuel Asenjo,  
director TIC de Broseta Abogados

Transformación total de la estrategia de ciberseguridad de la compañía: contratación de SOC, encriptación de sistemas, creación de Comité de Seguridad, etc.



Javier Torres,  
CISO de Allfunds

Implementación de un nuevo modelo tecnológico para agilizar el on-boarding de empleados, asegurar la autenticación, el control de acceso remoto y la navegación de usuarios.



Enrique Rubio-Manzanares,  
CISO de SegurCaixa Adeslas

Mejorar el nivel de madurez de seguridad, evolucionando las capacidades ya existentes. Se crearon cuadros de mando para ver el impacto de las acciones realizadas.



Carlos Asún,  
CISO de Food Delivery Brands

Implementación de diferentes herramientas de Seguridad, ayudar en la transformación digital y mejorar las herramientas de Seguridad existentes.



Daniel Puente,  
CISO de CIRSA

Integración de los procesos de DAST y SAST (Dynamic and Static Code Analysis) en la compañía.



Iván Sánchez,  
CISO de BUPA

Definir una estrategia y un equipo de Ciberseguridad que diera cobertura a todas las entidades del Grupo en Europa y Latinoamérica, en total 7 países y más de 30.000 empleados



Ángel Luis Gálvez,  
Global CISO de Dufry

Estandarización de procesos y tecnologías de seguridad para alinear los servicios de seguridad con el nuevo modelo de negocio o la adecuación a legislaciones en 80 países.



María Viader,  
CISO y DPO de Volkswagen Group

Campaña de concienciación de ciberseguridad donde se han realizado distintas actividades durante lo que hemos denominado la Cibersemana.

### LA OPINIÓN DE Fernando Jofre

## La fiebre de la IA generativa

La Inteligencia Artificial generativa está totalmente de moda, por su capacidad para producir gran variedad de nuevos contenidos. Desde imágenes, vídeo, música y voz, hasta redactar textos, picar código fuente y diseñar productos. La eclosión del tema ha sido relativamente reciente por “culpa” de ChatGPT, si bien la consultora Gartner viene realizando su seguimiento en su Hype Cycle para la IA ya desde 2020 y la identificaba entre sus principales tendencias tecnológicas estratégicas para 2022. Precisamente y según Gartner, el tema no está afectando en estos momentos a las previsiones de gasto de TI de las empresas.

De tal manera que la incorporación de la IA generativa se está llevando a cabo lentamente, a través de actualizaciones de herramientas que ya forman parte de sus presupuestos: embebida en el hardware, software y servicios que ya se están utilizando.

Pero eso no evita la necesidad de planificar una estrategia de adopción. Y la consultora reconoce que la fiebre entorno a la IA generativa se acabará traduciendo en un aumento en la inversión de TI.

Es precisamente la publicidad de ChatGPT la que ha conseguido que el 70% de las organizaciones haya iniciado investigaciones en torno a la IA generativa, y que el 19% haya puesto en marcha pilotos o la tenga en producción.

Es más, estas encuestas revelan también que el 68% de los ejecutivos considera que sus beneficios superan los riesgos, mientras que tan sólo el 5% que opina que son mayores los riesgos que los beneficios.

Las encuestas de Gartner a más de 2.500 ejecutivos indican que el 38% centrará sus inversiones en experiencia y retención del cliente, seguida del crecimiento de los ingresos (26 %), la optimización de costes (17 %) y la continuidad del negocio (7 %).

## Valero Marín, presidente de IndesIA



### ¿Qué es IndesIA?

IndesIA es una asociación creada para impulsar el uso de los datos y la inteligencia artificial la industria española, promovida por Repsol, Gestamp, Navantia, Técnicas Reunidas, Telefónica, Microsoft, Airbus, Ferrovial e Inditex y de la que forman parte grandes empresas y pymes industriales. Además, contamos con el apoyo del Basque Artificial Intelligence Center (BAIC) y Accenture. También colaboran con nosotros instituciones académicas y proveedores tecnológicos, gracias a todos ellos pretendemos lograr nuestro objetivo que es posicionar a España como referente en el uso de los datos y la inteligencia artificial en el ámbito industrial e impulsar el desarrollo de la economía del país.

### ¿En qué proyectos está inmersa ahora IndesIA?

Desde que creamos la asociación, hace poco más de un año, no hemos parado de poner en marcha proyectos a los que vamos dando continuidad y con los que pretendemos facilitar la adopción de la IA en las empresas, sobre todo en las py-

mes. Por eso hemos creado una guía de casos de uso de la IA, nuestra propia plataforma de espacio de datos y hemos desarrollado un caso de uso propio, sobre el valor de la analítica de datos y la IA para detectar anomalías en los equipos industriales. Recientemente también hemos presentado una guía para que las empresas apliquen inteligencia artificial de manera responsable. Y todo esto, lo estamos realizando mientras ponemos en marcha nuestros datatones, una iniciativa dirigida especialmente a las pymes para acelerar casos digitales, de la que estamos a punto de celebrar su segunda edición, en la que encontramos una solución a un problema de negocio gracias a los datos y la IA.

### De la asociación forman parte varias de las principales empresas españolas, ¿qué aportan a IndesIA?

Las empresas que han promovido IndesIA son líderes en sus respectivos ámbitos, todos ellos sectores industriales muy relevantes y llevan años utilizando los datos y la inteligencia artificial. Esto nos ha permitido beneficiarnos de su amplio conoci-

*Sigue en página 10*



# solmicro

erp6

¡El ERP con el  
que tu empresa  
estará **OK!**

El Software de gestión para la era digital 4.0



Personalizable



Rentable



Usable

**Premio Innovación**

XXXIII Premios Dirigentes a la Excelencia Empresarial



**PREMIOS  
Dirigentes**

{ XXXIII EDICIÓN }



# ZUCCHETTI

El software que te acerca al éxito

## LA OPINIÓN DE Manuel López

### ¿Hacia una Edad Media Digital?

Vivimos un mundo sumido en el caos. La desinformación está llegando a todos los rincones del mundo, vivimos destruyendo nuestro maravilloso planeta, en una polarización indescriptible. Se ha perdido el concepto de verdad, todo es opinable, nada es real, todo es relativo. La irrupción de la IA en nuestras vidas ha desatado un torbellino de emociones y preocupaciones. Aparece un periodo en el que la humanidad se enfrenta a lo desconocido, al temor y a las amenazas. En relación con la IA y la tecnología avanzada, nos encontramos en una situación similar a la existente en la Edad Media. Ambos son conceptos abstractos y poco comprendidos por la mayoría de las personas y esto ha creado una brecha entre los que entienden y controlan esta tecnología y aquellos que se sienten intimidados y confundidos por ella.

Sufrimos un mundo donde los señores feudales de la tecnología nos imponen sus ideas y visiones, mientras la mayoría de la gente se siente perdida en un mar de información contradictoria y sensacionalista, que nos lleva a la negatividad más oscura: “la IA me va a quitar el trabajo”, “la IA va a dominar el mundo”, “la IA va a destruir la humanidad”, ... Suena a que estamos entrando en una etapa parecida a la Edad Media, pero que en nuestra época lleva el apellido de “Digital”.

Pero creo que no todo es tan oscuro y hay espacio para la esperanza. Está empezando a desarrollarse el concepto de “Augmented Humanity”, como una visión positiva, que quiere ser realista y que desarrolla la idea de mejorar la experiencia humana mediante la integración de la IA en nuestra vida cotidiana.

En lugar de reemplazar a los humanos con máquinas, el enfoque es crear una simbiosis entre la tecnología y la humanidad, de manera que ambas se potencien mutuamente. Es un rayo de esperanza en medio de la oscuridad tecnológica.

miento y experiencia en estas áreas y ahora queremos compartirlo con las compañías que forman parte de nuestra cadena de valor. Nos sentimos comprometidos en actuar como motores e impulsores, ayudando a otras organizaciones a aprovechar las ventajas que ofrece el uso de los datos y la IA. Nuestro objetivo es contribuir a que estas empresas avancen y sean más eficientes, fomentando una actividad empresarial moderna y competitiva. Creemos firmemente que esto no solo beneficia a las grandes empresas, sino que también contribuye al progreso de toda la sociedad en general.

#### **En los últimos meses la IA ha cobrado especial protagonismo ¿cree que las empresas conocen realmente lo que les aporta la IA?**

Estamos en un momento en el que la Inteligencia Artificial generativa está despertando un gran interés, pero la inteligencia artificial viene de muchos años atrás. Ahora se están viendo las oportunidades que supone para las empresas, pero aún queda recorrido por delante y debemos seguir avanzando en su implantación y uso en las pymes. Y ese es nuestro objetivo principal. Trabajamos para demostrar lo que la IA puede aportar a cualquier negocio y lo hacemos explicando casos de uso y cómo se puede aplicar esta tecnología de diversas formas. Para ello realizamos informes y estudios y para acercarnos a las pymes, celebramos nuestros propios datatones, en los que ayudamos a pymes industriales a encontrar soluciones a sus retos reales de negocio gracias a algoritmos que se basan en IA. De hecho, hace unos días celebramos la segunda edición del Datatón IndesIA en el que uno de nuestros asociados, la empresa Cosentino, resultó ganadora.

#### **¿Tienen acuerdos firmados con Universidades para potenciar el conocimiento de la IA? ¿En qué consisten esos acuerdos?**

Tenemos acuerdos con varios centros universitarios como la Universidad de Navarra, la de A Coruña y la de Santiago de Compostela. Con ellos vamos a impulsar la formación en nuevas tecnologías, a través de la realización de diversas actividades formativas como cursos, seminarios o programas educativos y la creación de Cátedras en materia de inteligencia artificial. Además, las empresas asociadas a IndesIA están colaborando para la realización y presentación de casos de uso en los estudios relacionados con big data e IA. Todos estos estudios además se han certificado con el “sello IndesIA”. También participamos en los planes de estudio de másteres y asignaturas específicas y formamos parte de actividades y proyectos de investigación conjunta. En este sentido, los alumnos de estos centros podrán beneficiarse de la tutorización de proyectos fin de grado y másteres y la realización de prácticas en las empresas que forman parte de IndesIA.

#### **¿Qué metas se ha fijado IndesIA para el medio-largo plazo?**

Queremos apostar por nuestra industria, porque es lo que genera un tejido económico y social moderno, lo que arrastra la innovación y la competitividad y por lo tanto el bienestar social. Y en esta apuesta tenemos el reto de atraer a las pymes. Nuestra meta es sumar cada día a más compañías del tejido industrial, porque si queremos promover un cambio, una evolución, debemos contar con ellas. El uso de la inteligencia artificial se ha popularizado durante el último año, pero los datos apuntan a que todavía no es suficiente su implantación en las pymes, si queremos una industria eficiente y moderna.







# Expertos en transformaciones a S/4 HANA



[www.commonms.com](http://www.commonms.com)

[comercial@commonms.com](mailto:comercial@commonms.com)

+34 916 368 535



### LA OPINIÓN DE Daniel Puente

## El vuelo del Cóndor

Hace muy pocas fechas conocimos la muerte de Kevin Mitnick, probablemente uno de los mayores hackers de la historia, así como un ciber delincuente (recordemos que ambos términos no son sinónimos). En muchos artículos ya se habrá comentado lo importante que ha sido para el mundo de la informática, pero me gustaría si se me permite, hablar de lo que ha supuesto para mucha gente que hoy en día nos dedicamos a la ciberseguridad. Aún recuerdo cuando en la grupeta que nos reuníamos a cacharrear con el Comodore Amiga de un compañero y el flamante 386 de otro, nos llegó, años más tarde eso sí, el libro de Tsutomu Shimomura, Takedown, allá por 1997-1998. Fue realmente un impacto, y una constatación de que nos queríamos dedicar a esto, que queríamos algún día poder ser el protagonista de una novela parecida, sin tener claro aún qué papel jugar, pero queríamos que esas cosas pasaran, y ser nosotros actores de esa realidad.

Años más tarde, y después de sentencias cumplidas, Mitnick pasó a ser un gran profesional de la ciberseguridad, participando en empresas de gran renombre con alguna de las cuales he llegado a trabajar. Podríamos decir que es uno de los muchos ejemplo que hay de reinserción, y más en el mundo de la ciberseguridad, pero ni siquiera esto está en fuera de polémica, y es que cualquier cosa relacionada con Mitnick ha tenido casi la misma cantidad de detractores que de partidarios. Lo que no podemos negar es que con él muere uno de los grandes iconos del hacking y un auténtico profesional que ha inspirado a muchas personas.



## La IA acelera la contratación



Las empresas que utilizan herramientas de IA para agilizar sus procesos de contratación tienen una ventaja competitiva significativa. Estas herramientas pueden emular comportamientos humanos y procesar grandes cantidades de información, lo que les permite completar tareas en cuestión de segundos o minutos, que llevarían horas. Esta herramienta se ha convertido en parte fundamental del día a día de departamentos de RRHH para optimizar procesos, hacer más eficiente la toma de decisiones y para eliminar cualquier sesgo de comportamiento, favoreciendo así la inclusión durante los procesos de reclutamiento y selección.

Y es que, teniendo en cuenta que hoy en día el 31% de las búsquedas de empleo se realizan a través de un smartphone, habilitar un canal de comunicación a través de WhatsApp acerca a las empresas mucho más a los usuarios.

“Los procesos que antes se llevaban a cabo de forma manual ya los puedes hacer automatizando tus

conversaciones a través de un bot que vive en canales como WhatsApp”, explica Paulina Castañón, Directora de Recursos Humanos en GUS.

### IA EN EL DEPARTAMENTO DE RR.HH.

Prosegur ha contratado la tecnología de GUS para digitalizar y mejorar la comunicación con los candidatos en sus procesos de selección.

Las herramientas de inteligencia artificial en recursos humanos permiten a los profesionales centrarse en tareas complejas como capacitaciones y planificación del desarrollo del talento. También han demostrado ser cruciales para ahorrar costos y aligerar la carga de trabajo de los reclutadores.

Un ejemplo es Jobandtalent, que al integrar WhatsApp en su flujo de trabajo, logró ahorrar un 36% en puestos del Call Center, reducir llamadas en un 42% y aumentar la carga de documentos en un 150% durante el proceso de reclutamiento.



# Un gran viaje necesita de un gran compañero...



En **Viewnext** conocemos todos los caminos hacia la nube y cómo superar sus retos y desafíos. Siéntete seguro de emprender un viaje con la confianza que te da un compañero con experiencia.

## ¿Te acompañamos?

# La clave oculta en el éxito de los proyectos ERP - CRM



La implementación de sistemas ERP y CRM se ha convertido en una necesidad para que las empresas impulsen su eficiencia operativa y mejoren la experiencia del cliente. Sin embargo, el camino hacia el éxito en estos proyectos puede ser complejo y lleno de desafíos. Aquí es donde entra en juego el papel esencial del partner tecnológico.

Y es que, un partner tecnológico adecuado puede marcar la diferencia en el desarrollo e implementación de este tipo de proyectos. Carlos Esteve, director de Desarrollo de Negocio de Aitana, destaca que "el partner tecnológico adecuado es mucho más que un simple proveedor de servicios. Se convierte en un socio estratégico que comprende las necesidades específicas de la empresa y ofrece soluciones personalizadas para optimizar sus procesos y maximizar su eficiencia."

### UNA VISIÓN HOLÍSTICA DEL PROYECTO

Uno de los principales beneficios de colaborar con un socio tecnológico es su capacidad para ofrecer una visión holística del proyecto. Los partners experimentados como Aitana no solo poseen un profundo conocimiento de las tecnologías ERP - CRM, sino que también entienden las particularidades del sector y los desafíos operativos a los que se enfrenta cada empresa.

"La visión holística que ofrecemos en Aitana nos permite evaluar las necesidades empresariales desde una perspectiva amplia y global. Esto nos ayuda a ofrecer soluciones integrales, alineadas con los objetivos estratégicos de nuestros clientes", comenta Carlos Esteve.

### EXPERIENCIA Y CONOCIMIENTO TÉCNICO

Otro factor clave que distingue a un socio tecnológico de excelencia es su know how y conocimiento técnico. La implementación de sistemas ERP - CRM puede ser compleja y desafiante, pero un partner con experiencia ha superado múltiples obstáculos en proyectos anteriores y aprendido lecciones valiosas en el camino.

Según Carlos Esteve, "la experiencia es fundamental en este ámbito. Nuestro equipo ha trabajado en numerosos proyectos y, además, contamos con una metodología probada y exitosa, que nos otorga una ventaja competitiva frente a otros socios tecnológicos."

### ACOMPañAMIENTO DURANTE TODO EL PROCESO

Desde la fase inicial de análisis y planificación hasta la puesta en marcha y el seguimiento posterior, un partner valioso se mantiene a la vanguardia, brindando asesoramiento y soporte técnico en cada etapa.

"Nuestra relación con los clientes no termina con la implementación del proyecto. Nos comprometemos a ofrecer un soporte continuo y estar disponibles para cualquier consulta o ajuste que se requiera en el futuro. Nuestro objetivo es garantizar que nuestros clientes obtengan el máximo valor de sus inversiones en tecnología y logren un crecimiento sostenible a largo plazo", asegura el director de Desarrollo de Negocio.

### AITANA, TU PARTNER TECNOLÓGICO

En conclusión, la colaboración con un partner tecnológico adecuado se revela como un factor imprescindible en el éxito de los proyectos ERP - CRM. La consultora tecnológica Aitana es partner Gold de Microsoft y partner Platinum de Sage, cuenta con más de 40 años de experiencia y más de 2.400 empresas, y su propósito es impulsar el crecimiento de las empresas y su digitalización.



# La ciberseguridad en el centro de la estrategia del negocio



**Por Carlos Manero**  
Digital & Managed Services  
Manager de HP

Cada vez resulta más importante para las empresas contar con las estrategias adecuadas de seguridad para prevenir, detectar y contener las ciberamenazas actuales. Un plan básico de seguridad permite hacer frente a los ciberataques que están en constante evolución y que generan complejas amenazas. Según el último Estudio de Defensa Digital de Microsoft, se estima que las compañías que disponen de un buen sistema de seguridad se encuentran protegidas frente al 98% de los ataques.

Además, uno de los retos actuales para la seguridad empresarial es la transición hacia una cultura laboral caracterizada por el trabajo híbrido. Tener una protección adecuada en este tipo de entornos resulta más complicado porque el perímetro y el radio de acción de los empleados traspasa los límites de las oficinas (y por tanto, el perímetro tradicional de seguridad). Para proteger los nuevos espacios de trabajo es clave garantizar la seguridad en todos los dispositivos incluyendo PCs e impresoras, ya que se han convertido en el objetivo preferido por los ciber-delincuentes y representan la "zona cero" en un alto porcentaje de los ataques.

## TENDENCIAS ACTUALES DE LA CIBERDELINCUENCIA

Del mismo modo que en el entorno laboral se adoptan nuevos estilos de trabajo híbrido, los riesgos en ciberseguridad para las empresas también se transforman. En HP revelamos cuáles son las últimas técnicas a destacar en ciberdelincuencia gracias al informe trimestral HP Wolf Security Threat Insights. De entre los múltiples hallazgos, encontramos cuatro tendencias destacadas.

De entrada, es especialmente relevante la distribución del malware ChromeLeader que incentiva a la instalación de una maliciosa extensión llamada Chrome Shampoo.

La extensión puede redirigir las búsquedas hacia sitios web no seguros incluso hacer ganar dinero a la banda criminal a partir de campañas publicitarias. En segundo lugar, OneNote es otra vía por la cual los delincuentes aprovechan para insertar archivos dañinos detrás de falsos iconos. Accediendo a ellos, consiguen activar el acceso sin permiso al dispositivo de los usuarios.

Por otro lado, también han sido frecuentes los ataques que aluden a las políticas de macros. Se utilizan dominios de confianza, comprometiendo las cuentas fiables de Office 365, a partir de configurar correos electrónicos nuevos para distribuir archivos maliciosos. El informe también evidencia la diversificación de los métodos de ataque, destacando un notable incremento de un 37% en el contrabando de HTML (HTML smuggling) o el aumento de 4 puntos este trimestre del malware en formato PDF respecto al anterior analizado.

## CONTAR CON EL ADECUADO SISTEMA DE SEGURIDAD

Desde HP ponemos al servicio de nuestros clientes HP Wolf Security, que proporciona una perspectiva exclusiva de las técnicas más utilizadas por los criminales en el cambiante panorama de la ciberdelincuencia. De este modo, garantiza la resiliencia en todas las capas, desde el hardware hasta la nube. Gracias a la tecnología de aislamiento de aplicaciones, se aíslan aquellos riesgos que podrían pasar como desapercibidos. Gracias a ello, los clientes de HP Wolf Security han abierto ya más de 30.000 millones de adjuntos sin que se hayan ocasionado infracciones.

En definitiva, considerar las últimas conductas de los ciberdelincuentes, como también la adaptación de soluciones a las actuales tendencias del mundo laboral, son dos aspectos que deberían estar interconectados. Es fundamental para las empresas lograr la contención de las amenazas, localizar y poder bloquear los dispositivos perdidos, o bien asegurar la resiliencia de los equipos frente a comportamientos anómalos. Un entorno profesional seguro se convierte en un elemento determinante, ya que la información son uno de los activos más apreciados por parte de las compañías.



# Impresión segura: una tarea para no poner en riesgo tu empresa



La impresión es una de las tareas más comunes en cualquier empresa, y a menudo se subestima la importancia de su seguridad. Sin embargo, si no se toman las precauciones necesarias la impresión puede ser una puerta de entrada para los ciberdelincuentes que buscan infiltrarse en una red empresarial.

Según el último estudio de la firma de investigación de mercados Quocirca, realizado sobre una muestra de 531 responsables de TI en cuatro países, el 68% de las empresas han experimentado algún problema de seguridad relacionado con la impresión en 2022. Además, el estudio muestra que el 64% de las organizaciones no tiene ninguna política de seguridad para responder a este tipo de incidentes y sólo el 26% confían plenamente en la seguridad de su infraestructura de impresión.

La falta de atención a la seguridad de la impresión puede resultar en una serie de riesgos de gran trascendencia para una empresa, pudiendo llegar incluso a la interrupción de su negocio.

La primera línea de defensa

Uno de los principales riesgos de seguridad asociados con la impresión es el robo de información, como por ejemplo, contratos, informes financieros y datos de los clientes. Los piratas informáticos pueden explotar vulnerabilidades en la red para acceder a las impresoras y robar esta información, al igual que pueden utilizarlas para lanzar ataques cibernéticos. Si estos documentos caen en manos equivocadas, pueden causar daños reputacionales muy significativos.

Además, la pérdida de datos confidenciales puede re-

sultar en costosos pleitos y multas regulatorias. Según el mismo estudio de Quocirca, las pérdidas de datos relacionadas con la impresión supusieron un coste medio de más de 700.000 euros para las empresas.

Para protegerse contra el acceso no autorizado a las impresoras, las compañías deben implementar políticas de seguridad y medidas concretas tanto a nivel de red como de dispositivos y documentos.

Seguridad en tres capas: red, dispositivos y documentos

Una forma común de mejorar la seguridad de la impresión es implementando firewalls y sistemas de autenticación de usuario. Esto significa que los usuarios deben ingresar sus credenciales para imprimir un documento, lo que ayuda a prevenir que información confidencial caiga en las manos equivocadas. Este tipo de herramientas permiten también restringir ciertas funciones a usuarios específicos para evitar el mal uso de los dispositivos.

Además, las empresas pueden utilizar soluciones de gestión de impresión que permiten a los administradores de la red supervisar el uso de las impresoras y detectar cualquier actividad sospechosa. Estas soluciones pueden ayudar a identificar y mitigar cualquier riesgo de seguridad antes de que se convierta en un problema grave.

Como último aspecto importante, destacamos el cifrado. Los documentos confidenciales que se imprimen deben ser cifrados durante la transmisión para garantizar que no sean interceptados por ciberdelincuentes. Los dispositivos de impresión profesionales, más modernos, están equipados con esta capacidad y deben configurarse para que los trabajos de impresión se transmitan de forma segura.

No está de más recordar que mantener los dispositivos y softwares actualizados es prioritario, y no sólo para obtener su mejor rendimiento. Las actualizaciones a menudo incluyen correcciones de seguridad para vulnerabilidades conocidas.

Para conocer cómo Brother te puede ayudar a mejorar la seguridad de tus soluciones de impresión, tienes toda la información **en este enlace**.

# Los retos de modernizar los sistemas sanitarios



El sanitario es uno de los sectores que más está impulsando sus procesos de transformación digital ya que tienen que abordar una complejidad creciente. La modernización tecnológica es imprescindible para afrontar éstos y otros desafíos que permitan reducir las interrupciones parciales que está sufriendo el 40% de los servicios sanitarios esenciales de Europa.

## PRIORIDADES ESTRATÉGICAS

Para atajar esta serie de problemas, los responsables de TI que lo conforman consideran que es necesario abordar una serie de prioridades estratégicas, tal y como queda reflejado en un informe llevado a cabo por la consultora IDC. Entre esas prioridades estratégicas se encuentra, para un 63% de profesionales, la ciberseguridad. Asimismo un 41% de los encuestados también señala como prioritario el cumplimiento de la normativa y un 28% señala la necesidad que tiene el sector de cumplir con las expectativas que tienen puestas en él los ciudadanos. En este sentido, la nube (entendida como una experiencia y no como un destino) aparece como un elemento esencial para poder afrontar esta serie de retos ya que les permite cubrir tanto los apartados de la ciberseguridad, reducir de forma sensible las interrupciones y todo ello con una gran facilidad para gestionar los diferentes entornos y aplicaciones.

Un 79% de las empresas que conforman el sector asegura tener un alto nivel de madurez de los datos procesados y en este aspecto, el modelo *as a service* o de tecnología como servicio está jugando un papel cada vez más relevante en los procesos de digitalización de las organizaciones sanitarias. Los profesionales de TI del sector sanitario valoran muy positivamente las

ventajas de este modelo. Y es que, al optar por la tecnología como servicio, el departamento de TI puede combinar hardware, software y otros servicios complementarios a través de este modelo basado en suscripciones lo que les permite acceder a la última y mejor tecnología, a la vez que pueden optimizar su presupuesto y a simplificar su facturación. El hecho de que, con este modelo, la tecnología se renueve de forma constante, permite disponer de los últimos avances en seguridad, lo que redundará en una reducción de los riesgos informáticos.

Además, gracias al modelo de suscripción flexible, se reduce el exceso de aprovisionamiento y de esta forma las organizaciones tienen acceso a la tecnología que realmente necesitan y evitando malgastar recursos económicos.

La adopción de un modelo de tecnología como servicio, va a permitir a las instituciones sanitarias abordar la transformación de la asistencia sanitaria, donde los dispositivos médicos conectados, la telemedicina, la eficacia clínica o la medicina de precisión van a jugar un papel cada vez más relevante. Y serán las tecnologías del tipo nube las que posibiliten todo ello.

## COMPUTACIÓN DE ALTO RENDIMIENTO

La nube es el gran aliado de la computación de alto rendimiento (HPC) necesaria para la modernización de los entornos sanitarios. HPE tiene una de las soluciones de HPC más reconocidas por los profesionales del sector ya que proporciona ventajas clave para las necesidades del sector como son la agilidad, la sencillez y la rentabilidad gracias al uso de tecnologías de nube, métodos operativos, modelos empresariales, análisis de datos de alto rendimiento, inteligencia artificial y aprendizaje profundo. Una de las grandes ventajas es que la propuesta de HPE brinda un centro de datos más eficiente. Con la HPC híbrida de HPE, con la que se obtiene lo mejor de ambos mundos para el aprovisionamiento de soluciones locales o no locales. Además, la solución HPC híbrida incrementa las capacidades de HPC local con opciones basadas en la nube, ampliando los sistemas HPC locales conocidos a una infraestructura de nube privada flexible.

En definitiva, la infraestructura como servicio para HPC permite que el departamento de TI sea capaz de ofrecer servicios de aplicaciones e infraestructura de alto rendimiento incluso para los requisitos de HPC más exigentes.

# Guido Petillo, Director de Ventas de Zoom para el sur de Europa y Oriente Medio y Norte de África



### **Zoom se ha hecho muy popular en los últimos años. ¿Qué opina de la situación actual?**

Los dos últimos años han sido un boom para el mundo de la videoconferencia. Hoy nos centramos en la difusión de esta plataforma de videoconferencia unificada. De hecho, eso es lo que siempre hemos hecho desde el principio, desde que Zoom nació hace diez años.

### **¿Cuáles son las últimas novedades?**

Estamos introduciendo nuevas funciones de telefonía IP. Se trata de ayudar a las empresas a consolidar algo que tradicionalmente era complicado de gestionar. Servicios como el contact center, la pizarra interactiva avanzada para que los equipos trabajen de forma ágil, y luego desarrollos innovadores como las salas de conferencias multisala o las integraciones con soluciones de mercado.

### **¿Y en el ámbito del consumo?**

Zoom for Home es una solución de oficina en casa para videoconferencias, llamadas telefónicas y pizarras. Esta nueva realidad del teletrabajo, que hemos visto crecer, no es un fenómeno pasajero, sino que está destinada a perdurar. Hemos creído en esta evolución desde el principio y nuestras soluciones se centran en esta nueva normalidad.

### **¿Por qué Zoom fue el gran fenómeno del teletrabajo en la pandemia?**

Hay tres aspectos que creo que son importantes para los usuarios hoy en día. Me refiero a la facilidad de uso, la calidad de la experiencia de usuario y la seguridad: siempre hemos trabajado en estos tres puntos. La facilidad de uso y la capacidad de la plataforma para funcionar de manera sencilla y fiable creo que fueron los elementos que convencieron a la gente en un momento en el que todo el mundo se vio obligado a comunicarse por vídeo debido a la pandemia. Este cambio nos hizo mirar con nuevos ojos el entorno corporativo al que siempre habíamos estado acostumbrados y, al mismo tiempo, sacó a la luz nuevas formas de comunicarnos con compañeros, familiares y amigos.

### **¿Cómo se unen estos dos mundos, el empresarial y el del consumidor?**

Los une la sencillez funcional, la seguridad, la calidad de la experiencia, los elementos que marcan la diferencia, tanto en casa como en la oficina. Los servicios que hemos desarrollado, aunque en su mayoría nacen para el usuario empresarial, luego son consumidos por un público que puede ser consumidor.

### **¿Por ejemplo?**

Zoom Events es una plataforma para organizar eventos a los que se puede asistir de forma virtual o híbrida, con total libertad. Por otro lado, un servicio más puramente empresarial, como Zoom Contact Centre, permite a una empresa comunicarse con sus clientes de forma multicanal.

### **Un buen ahorro de tiempo y dinero.**

Si trabajo en atención al cliente, por ejemplo, vivo dentro de un entorno de comunicación Zoom, recibo una llamada de un cliente, la cojo, hablo con él, tengo una reunión por vídeo si necesito enseñarle algo, incorporo, por ejemplo, la firma de documentos mediante la introducción de DocuSign, añado notas, paso a CRM... Es una forma de simplificar las operaciones, garantizando una experiencia completa. Esa es la idea: llevar esa experiencia de trabajo híbrida y la optimización que conlleva, tanto al entorno corporativo como en beneficio del consumidor final.



# El futuro del espacio de trabajo: la conexión humana en un mundo híbrido



No es un secreto para nadie que la forma de trabajar ha cambiado, la pandemia ha acelerado un cambio que, desde nuestro punto de vista, era inminente y nos ha mostrado nuevas formas de ejecutar tareas, cumplir objetivos y aumentar la productividad de los equipos.

El trabajo híbrido no tiene por qué ser el próximo gran disruptor. Puede considerarse una evolución natural de herramientas y enfoques que han servido a equipos de trabajo durante décadas. Pero al garantizar una colaboración sin fisuras entre los que están en la sala y los que trabajan a distancia todos pueden estar incluidos, conectados y lograr un mayor impacto.

Google Workspace ayuda a los equipos híbridos de cualquier tamaño a conectarse, crear y colaborar, desde cualquier lugar y en cualquier dispositivo, sin embargo el trabajo híbrido es más que el lugar desde el cual se trabaja.

- ¿Cómo se mantienen conectadas las personas que trabajan a remoto con los que están en la oficina?

- ¿Cómo pueden todos los empleados gestionar mejor su tiempo y atención?

- ¿Cómo puede la tecnología contribuir al bienestar para que todos puedan maximizar su impacto?

Aunque el trabajo híbrido presenta algunos retos únicos, Google Workspace se ha centrado en la colaboración en cualquier momento y lugar durante más de una década.

La colaboración híbrida es ágil y fluida. No solo ocurre en reuniones programadas que abarcan diferentes lugares; ocurre en innumerables momentos cotidianos, desde discusiones espontáneas por chat hasta la colaboración en documentos compartidos. Las herramientas deben ser lo suficientemente flexibles para respaldar tanto la colaboración híbrida en tiempo real como la asincrónica. La capacidad de moverse sin problemas entre los modos de comunicación, como cambiar entre un documento com-

partido en Espacios y una videollamada con un solo clic, es crucial.

Establecer una mentalidad "hybrid first" no sucederá de la noche a la mañana. Pero al reconocer la necesidad de adaptar las normas de trabajo actuales y abrazar estas medidas fáciles de implementar, la colaboración híbrida eventualmente se convertirá en algo natural.

Un lugar de trabajo híbrido debe fomentar la productividad y la creatividad, fortalecer las conexiones y el sentido de pertenencia, así como aumentar la salud y el bienestar de todos los trabajadores. Considerar el diseño del futuro laboral híbrido como un viaje es clave, no se trata de una solución rápida para un solo momento en el tiempo. La prueba y experimentación son la parte clave de lo que ofrece GWS que continúa adaptándose en base a lo que aprende que funciona mejor para los empleados.

## ESTRATEGIAS PARA EL ÉXITO

**Tecnología inteligente y flexible:** utilizar soluciones de software y hardware para conectar equipos sin fisuras y reimaginar el espacio de trabajo para crear entornos inspiradores e integradores es esencial para promover la innovación y el trabajo en equipo dentro de cualquier organización.

**Construir una cultura de trabajo híbrida:** establecer prácticas que promuevan una mentalidad "hybrid first". El futuro del espacio de trabajo ya está aquí y es fundamental adaptarse para impulsar los flujos de trabajo y generar mejores sinergias entre empleados y equipos. Si quieres saber más sobre la implementación de Google Workspace habla con nosotros, como Premier Partner de Google desde hace más de 11 años, estaremos encantados de apoyarte en la modernización de tus espacios de trabajo.

### Más información

Sitio web: [www.incentro.com](http://www.incentro.com)

E-mail: [contacto@incentro.com](mailto:contacto@incentro.com)

Twitter: @IncentroES

Instagram: Incentro España

# Modelo SaaS o cómo descargar de responsabilidades a nuestro equipo IT



Vamos a coger una máquina del tiempo para viajar unos cuantos años atrás, donde la nube y todos sus términos no son ampliamente conocidos y en las empresas predomina el modelo de herramienta On-Premise, es decir, instalada en la infraestructura local de la red, ya sea en modo virtual o físico.

En este viaje que hemos hecho al pasado, entramos en una organización y hablamos con su responsable de IT. “¿Cuál es tu principal preocupación?” le preguntamos. Nos cuenta que su deber principal es asegurar la disponibilidad del servicio, y que intenta construir su red de acuerdo con esa meta. Añade que eso le supone un esfuerzo importante y que al tener tantas herramientas siempre hay algo que se le escapa, ya que tener una red 100% On-Premise requiere a la organización hacerse cargo la instalación y mantenimiento de las propias plataformas, incluyendo la redundancia de las mismas y las incidencias derivadas.

Pero, además, tiene que encargarse de que la plataforma sea segura y esté protegida, lo que le requiere estar al día y muy bien informado de nuevas actualizaciones y posibles vulnerabilidades que se puedan encontrar en sus herramientas, con la posible intervención que ello pueda necesitar.

## LA SOLUCIÓN A LOS PROBLEMAS

Para su tranquilidad, le decimos que dentro de unos años llegará la solución a sus problemas: El modelo SaaS.

Tener una plataforma en la nube en modo SaaS (software como servicio) supone, en resumen, descargar al equipo IT de toda la responsabilidad de gestionar la plataforma, poniendo ese trabajo en el tejado del fabricante. Y esto tiene todo el sentido del mundo, porque ¿quién mejor que el propio fabricante para mantener al día la plataforma y poder solucionar de la manera más rápida posible cualquier incidencia en la misma?

## UN EJEMPLO

Vamos a verlo con un ejemplo. Pongamos que tenemos una plataforma concreta en modelo On-Premise. Tras terminar el contrato decidimos llevarla a la nube e irnos a un licenciamiento SaaS. Esto supone que la organización se quita de encima todas las tareas de instalar, mantener, actualizar, monitorizar y proteger la plataforma, pudiendo además acceder a la misma desde cualquier lugar, sin necesidad de abrir ciertos puertos hacia el interior de la red local.

Aviso para navegantes, la inversión inicial siempre va a ser algo más alta para la modalidad SaaS, y si nos ceñimos a los números iniciales es posible que estemos tentados a quedarnos con el modelo On-Premise, pero en el momento de evaluar lo que supone tener la plataforma en local frente a tenerla en cloud, se puede asegurar que el modelo aquí descrito aporta una rentabilidad mucho mayor que el sistema tradicional.

En definitiva, lo que está claro es que el software como servicio ha llegado para quedarse, y eso es una gran noticia para todas las organizaciones.

### Más información

<https://omega-peripherals.com/>

# CLOUĐERA

## EL PODER DE LA IA GENERATIVA: POSIBILIDADES INFINITAS PARA TU EMPRESA

Ejecuta IA generativa y analítica a gran escala en un **data lakehouse abierto** y seguro.

Conéctate a cualquier fuente de datos, en cualquier lugar; procesa y entrega **a cualquier destino**.

Visita [cloudera.com](https://cloudera.com)





# Entrevista con Jorge Jiménez Molina, director general de Viewnext



**La sostenibilidad parece haberse convertido en un elemento esencial en las estrategias de las empresas, ¿qué es lo que ha cambiado?**

En los últimos años hemos vivido un cambio en las estrategias empresariales, pasando por tres fases: una original de convencimiento genuino integrando sostenibilidad en los valores corporativos, una segunda en que ese valor se convertía en un elemento diferencial de competitividad y por último, donde nos encontramos en este momento, una época de obligado cumplimiento, en que la sostenibilidad en las empresas es un elemento mandatorio para la supervivencia y capacidad de operar en los mercados. Esta evolución ha sido natural y más fácil en aquellas empresas como Viewnext que integraron el valor de la sostenibilidad en la estrategia de compañía desde el principio, involucrando al equipo directivo, empleados, proveedores y stakeholders. Aquellas que se han incorporado más tarde por necesidades de competencia o regulatorias están sufriendo para integrar las nuevas políticas en su día a día y en algunos casos caer en el llamado 'green washing'.

**¿Realmente la concienciación ha cambiado o han influido otros factores como la reducción de costes que ofrecen los**

**nuevos productos, soluciones y servicios que efectivamente son más sostenibles que los antiguos?**

La sostenibilidad se ha convertido en un elemento esencial en las estrategias empresariales resultado de varios factores. La creciente conciencia global es definitivamente el embrión, pero se ha visto catalizado por otras dinámicas confluyentes como: los cambios en la mentalidad de los consumidores que se traslada a los comportamientos como clientes o proveedores, la rentabilidad a largo plazo, las normativas más estrictas e incluso las exigencias de los potenciales inversores.

Y me gustaría añadir un elemento menos comentado y que en Viewnext estamos convencidos, que es la sostenibilidad como catalizador de la innovación tecnológica. En un círculo virtuoso, los retos a que nos enfrentamos las empresas por ser más sostenibles ponen a prueba la capacidad de respuesta de la tecnología. Para superarlos, se fomentan nuevos usos de la tecnología y su continuo desarrollo y evolución, y así nuevas tecnologías como el análisis de datos, los sistemas de gestión de la cadena de suministro o la inteligencia artificial puede ayudar a optimizar los procesos, reducir costos y minimizar el impacto ambiental. Las empresas que adoptan prácticas sostenibles están mejor posicionadas para enfrentar los desafíos, atraer y retener talento y aprovechar las oportunidades emergentes en un mundo cada vez más centrado en la sostenibilidad.

**¿Qué hace Viewnext como empresa para ser más sostenible?**

Lo primero y más importante es integrar el tema de sostenibilidad de forma integral, tanto en alcance cubriendo todas las áreas desde medioambiente a ética, buen gobierno, como en inclusión de todos los profesionales. Es un objetivo estratégico de máximo rango a nivel Comité de Dirección. Hemos definido un plan multianual, con 5 objetivos estratégicos e indicadores para el seguimiento del progreso de cada uno de ellos. Desde un punto de vista más pragmáticos hay varias acciones que estamos desarrollando como Eficiencia Energética (uso de equipos eficientes, optimización iluminación y edificios), Políticas de Reciclaje muy estrictas tanto en residuos electrónicos como de material, siendo una compañía en que nuestra huella de carbono principal proviene de los desplazamientos tenemos unas políticas de teletrabajo muy desarrolladas promoción de prácticas saludable con el personal animándoles a extender la concienciación más allá de Viewnext y en particular dos inicia-

tivas especiales Basuraless y Bosque Viewnext, este último dirigido a neutralizar y compensar la huella de carbono. Es un esfuerzo continuo y cada pequeña acción cuenta. Establecer metas claras, medir el progreso y comunicar los logros a los empleados y clientes también son pasos importantes para crear una cultura empresarial sostenible.

### ¿Cómo trabaja Viewnext con sus clientes para que sean más sostenibles?

Una compañía de servicios IT puede desempeñar un papel clave en ayudar a sus clientes a ser más sostenibles. Al trabajar en colaboración con nuestros clientes y ofrecer soluciones sostenibles, puedes ayudarles a reducir su impacto ambiental y lograr una mayor eficiencia en sus operaciones de TI. Esto no solo es beneficioso para el medio ambiente y la sociedad, sino que también puede generar ahorros de costos a largo plazo para tus clientes. Algunas formas de hacerlo son:

El progreso en la digitalización, que ayuda en el uso eficiente de recursos (como papel) pero también ayudándoles a evaluar y re diseñar la arquitectura IT y el mapa de aplicaciones. Migración a la nube que más allá de los beneficios puntuales de reducir servidores físicos por una consolidación global más eficiente, conlleva simplificar los procesos y consumo de IT. Proyectos de gestión eficiente de datos , que implica optimizar la eficiencia de la capacidad de almacenamiento evitando duplicidades, mantenimiento de datos obsoletos y costes de transmisión. Y también, educación y concienciación de las organizaciones, los proyectos anteriores requieren de una gestión de cambio en su adopción donde el componente de sostenibilidad es importante para nosotros incorporar por el impacto y la aceptación de la transformación , ayudando a vencer resistencias al cambio.

### ¿Dónde están los mayores retos? ¿En la gestión de residuos electrónicos,

### utilizar el centro de datos, utilizar energías renovables o emplear equipos más eficientes?

En el ámbito de la sostenibilidad en las empresas, existen varios retos importantes a abordar. Si bien todos los aspectos que mencionas son relevantes, para mí la clave es abordar todos estos desafíos de manera integral para lograr una mayor sostenibilidad en las empresas. Y no sólo desde una perspectiva medioambiental, si no también evaluando el impacto social y el ejemplo que como compañía transmites a tus empleados, clientes y proveedores. Uno de los retos también es fortalecer nuestra organización como un ejemplo de la mejor sociedad posible, donde cabe todo el mundo, con mejores índices de diversidad e inclusión, especialmente con más mujeres, personas LGBTIQ, personas de orígenes diversos, personas con discapacidad... y poniendo en marcha más políticas en contra de la discriminación y a favor de la igualdad entre todos nuestros profesionales.

De los que comentas, y en base a nuestra experiencia con clientes y colaboradores, la gestión de residuos electrónicos y la utilización de centros de datos eficientes y con energías renovables suelen considerarse como los mayores retos debido a su impacto ambiental y la complejidad asociada a su implementación. Pero seguramente el mayor reto es la credibilidad, continuidad y ambición de las acciones comprometidas.

### ¿Dónde están los principales errores que se cometen que impiden un mejor desarrollo de políticas sostenibles?

### ¿Son conscientes las empresas de estos errores?

Como comentaba en la primera pregunta cuanto más genuína es la concienciación y compromiso alrededor de la sostenibilidad más fácil es el desarrollo de políticas sostenibles. Los principales errores que cometen las

empresas está asociados a este punto y pueden variar según el nivel de madurez de cada empresa. Por ejemplo,

- Falta de compromiso de la alta dirección: Si la dirección no considera la sostenibilidad como una prioridad estratégica, es probable que no se asignen suficientes recursos ni se establezcan metas claras en este ámbito.

- Enfoque a corto plazo y priorización del beneficio económico o reputacional inmediato. Muchas empresas aún se centran principalmente en lo medioambiental sin considerar adecuadamente los impactos sociales, o lanzan programas a corto plazo que luego no tienen continuidad o no son integrados en los valores y estrategia de la compañía. Esto último lleva a otro error común

- Tratar la sostenibilidad como un aspecto aislado en lugar de integrarla en la estrategia y las operaciones diarias de la empresa. La sostenibilidad debe estar presente en todas las áreas de la organización, desde la toma de decisiones hasta la cadena de suministro y las relaciones con los stakeholders.

- Falta de medición y reporte adecuados: aquí también es muy aplicable ' lo que no se mide .. no se le presta atención ... no mejora ... no se comunica bien '

En cuanto a si las empresas son conscientes de estos errores, en general yo diría que sí. Cada vez más organizaciones están reconociendo la necesidad de adoptar prácticas sostenibles y están trabajando para corregir estos errores. La presión de los consumidores, los cambios en las regulaciones y las expectativas crecientes de los stakeholders están impulsando un mayor enfoque en la sostenibilidad empresarial. Pero eso no significa que haya organizaciones que por presiones económicas, modelos de negocio muy volátiles o simplemente falta de concienciación no tengan reconocido la sostenibilidad como prioridad plenamente.

# Seguridad de los datos en el sector sanitario



El sector sanitario es uno de los más preocupados por proteger los datos, tanto de los usuarios como de sus empleados. Para analizar cómo se pueden proteger esos datos, cómo establecer una correcta estrategia y cuáles son las herramientas más adecuadas para su protección, Byte TI organizó un encuentro, patrocinado por Commvault, que contó con la participación de José Antonio Ovejero, CIO de Insurama; Ángel Luis Sánchez, CTO del Sermas; Santiago Gil, Enterprise Account Manager de Commvault; Maite Ramos, Country Manager de Commvault; David Hernán Gallardo, Jefe de Riesgos e Inteligencia de Seguridad de Mapfre; Sergio Chicheri, Territory Account Manager de Commvault y Marek Nowosielski, Data Science Director de Liberty Seguros.

El encuentro comenzó analizando cuál es el grado de preparación que tienen las empresas para combatir y prevenir un ciberataque. En este sentido, David Hernán Gallardo, Jefe de Riesgos e Inteligencia de Seguridad de Mapfre, comentó que “en Mapfre montamos hace un tiempo un CERT (Equipo de

Respuesta ante Emergencias Informáticas) que era reactivo. En el año 2020 nos atacaron de la forma más fácil. Ese ciberataque, nos sirvió para transformar ese CERT. Ahora tenemos uno mucho más avanzado que tiene numerosas herramientas en el cloud, con analítica de comportamiento. La realidad es que,



## LOS PARTICIPANTES

en nuestro caso, desde el año 2008 estamos creciendo e invirtiendo cada vez más en ciberseguridad. A pesar de todos los desarrollos e inversiones creemos que tenemos que seguir trabajando para mejorar de forma constante. Hay que destacar que todo lo que hacemos en nuestro departamento lo hacemos a nivel global, de tal forma que lo que elegimos en España lo implantamos en el resto de subsidiarias. Esta homogeneización nos permitió ser mucho más ágiles y mejorar la securización y hacerlo de forma global. La gran ventaja es que ahora, con una plantilla de 20 personas, podemos gestionar todo y eso antes era imposible”.

### CLAVES DE LA DIGITALIZACIÓN

La realidad es que todas las organizaciones que trabajan en los entornos sanitarios están inmersas en proyectos de transformación digital. Tal y como aseguró Marek Nowosielski, Data Science Director de Liberty Seguros, “todas las empresas estamos en una constante digitalización. Sin esa transformación digital no podríamos sobrevivir ahora mismo. El COVID nos enseñó muchas cosas y gracias a la pandemia fuimos capaces de ver cómo podíamos cambiar. El futuro pasa por la transformación digital, y en ese proceso es muy importante ver qué se puede hacer y qué no se puede hacer con los datos. Este es uno de los aspectos más importantes que están cambiando. Hay que proteger los datos de forma local, pero también teniendo en cuenta que el perímetro es cada vez más difuso”.

Ante estas circunstancias de incremento de ciberataques, cada vez más sofisticados, las empresas que trabajan en el sector sanitario se enfrentan a diferentes retos. En este sentido, Ángel Luis Sánchez, CTO del Sermas (Servicio Madrileño de Salud), consideró que “uno de los principales retos del sector sanitario es la sostenibilidad del sistema público. En España tenemos un problema ya que tenemos una de las mayores esperanzas de vida y por otro lado, tenemos la desgracia de que nacen pocos niños. Esta pirámide va a suponer que vayamos a incurrir en más gastos y tengamos menos ingresos. Y todo ello en un entorno en el que la sociedad está cada vez más envejecida y por tanto, va a tener más problemas de salud. Por eso hay que digitalizar la Sanidad Pública: hemos avanzado bastante como con la historia clínica, pero falta la parte de la transformación digital porque no hemos transformado digitalmente la sanidad. Se trata de empezar a ver que esas nuevas tecnologías lleguen al sanitario para que tengan todas las tecnologías posibles que permitan una toma de decisiones mucho más rápida y eficaz. En mi opinión, creo que no le estamos sacando todo el beneficio que podemos a la tecnología, aunque es verdad que no es un tema sencillo”.

### PROTECCIÓN DE LA INFORMACIÓN

Uno de los grandes objetivos es proteger la información con la que trabajan las organizaciones. José Antonio Ovejero, CIO de Insurama explicó que su compañía “se diferencia del resto a través de esa faceta de la transformación digital. Nosotros tratamos de usar todas las facetas de la digitalización dentro de la oferta de



José Antonio Ovejero,  
CIO de Insurama



Ángel Luis Sánchez,  
CTO del Sermas



Maite Ramos, Country  
Manager de Commvault

## LOS PARTICIPANTES



Santiago Gil, Enterprise Account Manager de Commvault



David Hernán Gallardo, Jefe de Riesgos e Inteligencia de Seguridad de Mapfre



Marek Nowosielski, Data Science Director de Liberty Seguros



Sergio Chicheri, Territory Account Manager de Commvault

nuestro producto ofreciendo una serie diferencial y de forma personalizada para los clientes. Intentamos hacerlo a través de todos los mecanismos de ciberseguridad como auditoria de código o escaneos de vulnerabilidad, pero no tenemos información de nivel alto como otros entornos”.

### DISPERSIÓN DE DATOS

Otro de los retos en protección de datos reside en la dispersión de los mismos. Y es que, tal y como expresó Marek Nowosielski, “Lo que creo que nos debe preocupar son los datos que están en cada departamento aislados y no se comparten con otros departamentos. El problema de esos datos que no se comparten es que implican un cambio cultural y es clave, porque hay que implicar a todos los empleados en que la seguridad es una cosa de todos los usuarios”.

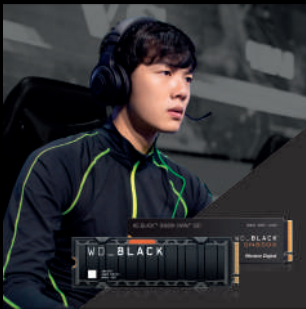
Para Sergio Chicheri, Territory Account Manager de Commvault, “Hoy en día, las organizaciones afrontan el reto de hacer frente a cada vez más amenazas y nuevos medios de ataque, pero con menos recursos y más datos en más lugares. En un mundo híbrido y multinube, que es en el que nos encontramos, es necesaria una solución capaz de asegurar, defender y recuperar los datos de forma rápida y sencilla. Y esto es lo que ofrece Commvault. Hemos integrado tecnologías de alerta temprana en nuestra plataforma, que ayudan a protegerse frente a las amenazas antes de que estas puedan causar daño, defender los datos si se origina una brecha en el entorno y garantizar la recuperabilidad para que los clientes y sus datos sigan siendo resistentes frente a las ciberamenazas, por mucho que estas evolucionen. Commvault es el único proveedor de protección de datos con alerta temprana, supervisión exhaustiva de amenazas y cyber deception para entornos de producción y backup, y puede detectar amenazas en tan sólo cinco minutos, frente a las 24 horas de media del sector. Y esto es importantísimo, ya que hay una gran diferencia entre el día cero y el día 1 de un ataque. Al sacar a la luz y neutralizar las amenazas internas y de día cero antes de que causen daños, la tecnología de Commvault ayuda a contener las brechas y a limitar el radio de explosión de los ciberataques”.

El backup es la principal herramienta para la recuperación, pero no es suficiente porque, tal y como expuso Maite Ramos, Country Manager de Commvault, “hoy en día las ciberamenazas también tienen como objetivo el backup. Por eso es necesario garantizar que los datos de backup permanezcan inmutables frente a alteraciones o cifrado por ransomware. Esto es crucial para recuperarse de un ataque. También es esencial que, en el caso de que se produzca un ataque, podamos asegurar que las copias de seguridad estén limpias antes de restaurarlas. Con nuestras soluciones de seguridad, estamos redefiniendo la protección de los datos, cubriendo todo su ciclo de vida y asegurándonos de proteger, defender y recuperar los datos. En resumen, lo que hacemos es facilitar la vida de nuestros clientes y darles la tranquilidad de saber que sus datos están protegidos durante todo su ciclo de vida y frente a cualquier problema”.

# Lleva tu dispositivo a otro nivel con los discos Western Digital® NVMe™



Las unidades NVMe™ suponen un enorme salto de rendimiento respecto a las unidades SATA, con velocidades de lectura hasta 13 veces superiores\*, ya que la interfaz y los protocolos SATA se basan en la tecnología de los discos duros. Todos los nuevos PCs y portátiles utilizan ahora unidades SSD M.2 PCIe® NVMe™ y Microsoft requiere un SSD NVMe™ para la compatibilidad con DirectStorage para juegos acelerados.



**WD\_BLACK™** con alto rendimiento para gamers y compatibilidad con DirectStorage para juegos de PC de próxima generación, unidades NVMe con licencia para PS5 y gran ancho de banda para aplicaciones exigentes.



**WD Blue™** para Creadores, el favorito para los profesionales DIY y creativos.



**WD Red™** para NAS, proporciona almacenamiento en caché rápido para un acceso acelerado y pools de almacenamiento de alto rendimiento para máquinas virtuales o edición de vídeo, manteniéndose al día con el creciente ancho de banda de la red.



**WD Green™** para mejorar las tareas informáticas cotidianas realizadas con tu PC, como navegar por Internet, estudiar y trabajar desde casa.

**JUEGA | CREA | COMPARTE | ACTUALIZA**

[westerndigital.com/solutions/internal-ssd](https://westerndigital.com/solutions/internal-ssd)

\*Comparación entre WD\_BLACK SN850X y WD Blue SATA SA510 1TB. Western Digital, el diseño de Western Digital, el logotipo de Western Digital, myWD, el logotipo de myWD, WD\_BLACK, WD Blue, WD Red y WD Green son marcas registradas o marcas comerciales de Western Digital Corporation o sus filiales en Estados Unidos y/o en otros países. Las marcas con las palabras NVMe y NVMe-oF son marcas comerciales de NVM Express, Inc. PCIe es una marca registrada de PCI-SIG Corporation. PS5 es una marca registrada de Sony Interactive Entertainment Inc. en los Estados Unidos y/o en otros países. Todas las demás marcas pertenecen a sus respectivos propietarios. Las imágenes mostradas pueden diferir del producto real. ©2023 Western Digital Corporation o sus filiales. Todos los derechos reservados.



# La Digitalización en el sector sanitario y farmacéutico



El sector sanitario y el farmacéutico son uno de los que más implicados están en sus procesos de transformación digital. Hospitales, laboratorios, farmacias, compañías de seguros, centros de realización, ambulatorios, entre otros, se están apoyando en la tecnología para mejorar sus procesos.

**Por Vanesa García**

Uno de los retos que tiene el sector es que son numerosas las tecnologías que se pueden aplicar. Además, al ser un sector con diferentes tipologías de empresas y organismos, las necesidades pueden variar mucho entre unas y otras. Para hablar sobre esto, Byte TI ha organizado una webinar, en colaboración con HP Enterprise y Common Management Solutions, que ha contado con la presencia de: Francisco José Sánchez, subdirector general, Sistemas Clínicos del servicio Andaluz de Salud; Julián Sánchez, partner de Common; Juan Carlos Peciña, Jefe del Servicio de Tecnologías de la Información de SACYL. Roberto Torres, HPE CTO Data Services, Marco Antonio García, Director Territorial de IT, de Quirón Salud y Josep Bardallo, CISO en Grupo Hospitalario Recoletas.

La ciberseguridad se ha convertido en una preocupación fundamental para las empresas y organismos sanitarios. Con la creciente dependencia de la tecnología y la digitalización de la información médica, surge la pregunta de si estas entidades tienen una estrategia adecuada para protegerse contra las cada vez más sofisticadas amenazas cibernéticas.

En respuesta a ello, Roberto Torres, HPE CTO Data Services explica que desde antes de la pandemia ya se sufrían continuamente ataques de ciberseguridad contra entidades, no solo sanitarias, sino empresas de todo tipo, a nivel nacional y internacional. “El famoso ransomware también ha hecho que los CEOs tengan su presupuesto ya reservado para este tipo de protecciones. Nosotros tratamos la ciberseguridad en los diferentes vectores de ataque: con tecnología zero-trust, en los cuales cualquier dispositivo que fabricamos, ya sea un servidor, una cabina de almacenamiento, un dispositivo... todos los dispositivos están firmados electrónicamente para que cualquier componente que se añade a él sea un componente reconocido por nuestra marca. Tenemos firmas digitales con todos los fabricantes de tarjetería y demás que se añaden a los componentes para verificar. Es importante también proteger el entorno de la red, los entornos wifi y hospitales. Y luego por supuesto protección contra la encriptación y el malware, el ransomware famoso que además entra desde dentro y es difícil de detectar”.

Para Julián Sánchez, partner de Common, la sanidad, igual que otros sectores, necesitaba un cambio radical antes de la pandemia, “ahora mismo hay más población, mucho más anciana, y más enfermedades tratables... Todos los responsables de sistemas o responsables de gestionar hospitales, tienen que llevar los servicios hacia lo digital. La telemedicina, la teleasistencia, la teleadministración de pacientes es el futuro. Al igual que introducir los servicios de seguridad adecuados para esta transformación digital”

## ESTRATEGIAS FUTURAS

Francisco José Sánchez, subdirector general, Sistemas Clínicos del servicio Andaluz de Salud explica que en los próximos meses seguirán una estrategia en la cronicidad y en los nuevos modelos de atención, gracias a un convenio con Red.es. “Nosotros, siempre que desarrollamos algo nuevo, intentamos alejarnos de aplicaciones monolíticas y tener muchos microservicios o herramientas base que nos permitan hacer muchas cosas con poco desarrollo. El principal cambio que venía en este proyecto de crónicos era el orquestador, el tener un orquestador que nos permitiera conectar todos nuestros módulos y empezar a hacer cosas sin necesidad de código, sino simplemente hacer el dibujo del BPMN y que los funcionales puedan directamente dibujar el proceso y no necesitar el tiempo que nos lleva, muchas veces, entregar versiones y cambiar”.

Por su parte, Josep Bardallo, comenta que desde Grupo Hospitalario Recoletas enfocan sus estrategias futuras en tres puntos globales, “uno es lo que tiene que ver con la experiencia de paciente digital. Otra de las estrategias que nos hemos marcado ya hace un par de años para soportar este crecimiento, esta velocidad que llevamos es la estandarización. Tenemos unos procesos internos que este año acabaremos de estandarizar. Otro punto importantísimo es el de ciberseguridad. Ya tenemos un cierto nivel, pero este año vamos a apretar muchísimo más, sobre todo en la parte de detección y respuesta. Asumimos que nos van a entrar todos los procesos internos para detectar muy rápidamente cualquier incidencia, cualquier problema que tengas y poder responder para que el impacto sea mínimo”.

## TECNOLOGÍAS COMO IA Y BIG DATA

La IA y el Big Data han unido fuerzas para transformar la atención médica, ofreciendo soluciones innovadoras y personalizadas. Con el inmenso poder de procesamiento y análisis de datos, estas tecnologías permiten a los profesionales de la salud obtener información valiosa en tiempo real. Desde análisis predictivos hasta diagnósticos más precisos, la IA y el Big Data se han convertido en aliados indispensables para tomar decisiones clínicas informadas.

En esta línea, Juan Carlos Peciña explica que en línea con la salud digital, los profesionales deben ser dotados con estas tecnologías para ayudar al diagnóstico. “Tradicionalmente había ya herramientas en el ámbito de la imagen, pero ha avanzado mucho la aplicación de inteligencia artificial en otros ámbitos. En nuestro caso también intentamos favorecer el trabajo en grupo, porque tenemos mucha dispersión, y aplicamos todas las técnicas de Big Data y Data Lake con otras comunidades y con el ministerio. Estas tecnologías también van a mejorar toda la parte de atención al ciudadano, la comunicación con profesionales y la parte administrativa, aunque ya está muy avanzada”.

Marco Antonio García, coincide con su compañero, y añade que las nuevas tecnologías como la inteligencia artificial, la realidad aumentada y el Big

## LOS PARTICIPANTES



Francisco José Sánchez,  
subdirector general, Sistemas  
Clínicos del Servicio Andaluz  
de Salud

“Vamos a seguir una estrategia de cronicidad”



Juan Carlos Peciña, Jefe del  
Servicio de Tecnologías de la  
Información de SACYL

“Intentamos favorecer el trabajo en grupo, porque tenemos mucha dispersión”



Julián Sánchez, partner de  
Common

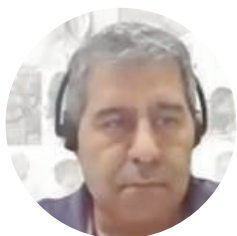
“Quienes gestionan hospitales, tienen que llevar los servicios hacia lo digital”

### LOS PARTICIPANTES



Roberto Torres,  
HPE CTO Data Services

*“Los CEOs tienen un presupuesto reservado para el ransomware”*



Marco Antonio García,  
Director Territorial de IT de  
Quirón Salud

*“Desde Quirón Salud realizamos programas de liderazgo y de formación”*



Josep Bardallo,  
CISO en Grupo Hospitalario  
Recoletas

*“Una de nuestras estrategias se ha basado en la estandarización”*

Data, aportan bastantes mejoras y retos. “Tenemos que acompañar la tecnología en cada uno de los centros a la utilización de toda esta nueva tecnología. Estos algoritmos avanzan mucho más rápido que la tecnología que podemos tener en los distintos centros. Para nosotros es un reto bastante grande adecuar toda la equipación de los centros a estos nuevos requerimientos. Y luego otro valor es la comunicación y la formación a los diferentes equipos médicos o servicios. Por eso, desde Quirón Salud realizamos programas de liderazgo y de formación, que sean interdisciplinarios para que todos puedan trabajar de la misma manera. Y luego también disponemos de unos KPIs que nos permitan medir el grado de implantación, el grado de uso de todas estas nuevas tecnologías”.

Roberto Torres comenta que en HP están haciendo una inversión muy fuerte, en todo el ciclo de vida del dato, “hemos montado una unidad de negocio nueva que es de software ,donde dentro de ahí tenemos lo que llamamos nosotros los Delta Lakes que es una versión más moderna del Data Lake donde se puede ingestar información tanto estructurada como desestructurada. De hecho, estamos lanzando al mercado tecnologías de inteligencia artificial federada para poder compartir información, entre diferentes sedes y entre diferentes hospitales que no están ni siquiera en el mismo país y así, poder cumplir el GDPR”.

#### UNA CORRECTA ESTRATEGIA DE ATENCIÓN AL CLIENTE

Establecer una correduría de estrategia de atención al paciente implica diseñar un enfoque integral para optimizar el proceso de atención, desde el primer contacto hasta el seguimiento posterior al tratamiento. Aquí es donde la Inteligencia Artificial y los chatbots juegan un papel crucial. La IA permite analizar grandes volúmenes de datos de pacientes, historiales médicos y patrones de enfermedades para mejorar la toma de decisiones clínicas y ofrecer tratamientos personalizados.

Mientras que los chatbots actúan como asistentes virtuales que pueden brindar información, responder preguntas frecuentes, programar citas y brindar seguimiento a los pacientes de manera instantánea y eficiente.

En opinión de Julián Sánchez, no solo se debe mejorar la experiencia del paciente, sino también mejorar cómo el personal clínico, cómo los recursos del hospital se enfocan a prestar ese servicio. “Por otro lado, todos los pacientes son diferentes. Entonces, personalizar la atención es importantísimo y a través del conocimiento al paciente y conociendo el procedimiento y el diagnóstico, podemos enlazarlo y hacer que esta gestión sea más rápida”.

Y es que, los datos en el sector sanitario son primordiales, así lo destaca Josep Bardallo, que dice que hoy en día ya no solo son los datos de la historia clínica del paciente, sino todos los procesos, todas las mejoras, todo lo que se hace va en la línea y cruza todo tipo de datos, “es un crecimiento constante, pero al final lo que se está buscando es que todos esos datos sirvan para mejorar la experiencia del paciente, también sirvan para mejorar los procesos, o cómo los utilizan los profesionales para diagnosticar”.

“Utilizar el dato más allá de la parte de investigación, es aplicar todas estas nuevas tecnologías de Big Data e Inteligencia Artificial para casos más concretos y del día a día. El reto es que efectivamente es un área nueva, es un área que está en plena audición, hay carencias de profesionales cualificados, lo cual es un hándicap”, añade Juan Carlos Peciña.



# Digital workplace: el reto del nuevo trabajo



Desde la pandemia los procesos de digitalización de los entornos de trabajo se han acelerado. En la actualidad, la apuesta por los entornos híbridos ha obligado a las compañías a avanzar en la transformación del puesto de trabajo.

Para tratar cuál es la evolución Byte TI organizó un encuentro, patrocinado por Kyocera, Incentro y Zoom, que contó con la participación de José Manuel Medina, CTO de LaborMatters Abogados; Raquel Pinillos Gil, Business Solutions Director de Kyocera; Manuel Tarrasa Sánchez, CIO de Prosegur; Miguel Ángel Ramos, Responsable Digital Workplace en Leroy Merlin; Manuel Asenjo, Director IT y Ciberseguridad en Broseta Abogados; Daniel Damas, IT Security Manager de Nationale-Nederlanden; Rafael Corrales, CIO de Nuubo; Raúl Belber, IT Director de Northgate; Néstor Cortés, Google Workspace Technical Lead de Incentro; Antonio Gómez, Enterprise Account Manager de Zoom; José Morales, Director TIC de Acciona y Diego Carbajales, IT Workplace & Service Delivery Manager de Dufry.

El encuentro lo comenzaron las tres empresas patrocinadoras que dieron a conocer cuál es su punto fuerte en esta materia. Así, Néstor Cortés, Google Workspace Technical Lead de Incentro, explicó que su compañía “es una consultora de Transformación Digital que es partner de Google con 14 oficinas alrededor de todo el mundo y especialistas en solucio-

nes cloud. Somos especialistas en la modernización de entornos de trabajo”. Por su parte, Antonio Gómez, Enterprise Account Manager de Zoom comentó que “además de lo que somos conocidos por la mayoría del público, nos dedicamos a implementar proyectos de Digital Workspace y también estamos posicionado en los ámbitos de telefonía o Contact Center”. Finalmente, Raquel Pinillos Gil, Business Solutions Director de Kyocera, explicó que uno de los puntos fuertes de esta multinacional “es haber recogido la experiencia que tenemos en lo referente a la gestión documental en la nube y hemos desarrollado una plataforma API low code que nos sirven para modernizar aplicaciones que tienen que ver con el puesto de trabajo”.

## FORMA DE TRABAJO

Tras ello, fueron los diferentes representantes los que explicaron cómo han transformado el puesto de trabajo. Así, Manuel Tarrasa Sánchez, CIO de Prosegur explicó que “nosotros llevábamos un camino de teletrabajo antes de la pandemia, pero ésta nos ha servido para acelerarlo mucho. Con esto,

la cantidad de viajes se ha reducido mucho por el uso de estas herramientas y hemos realizado grandes inversiones en apostar por esta transformación del puesto de trabajo. Ha cambiado mucho la cultura de trabajo y la forma en la que se colabora. Ahora que casi todo el mundo teletraba, la posibilidad de participación es mucho más democrática porque la relación se hace mucho más simétrica”.

Raúl Belber, IT Director de Northgate explicó que “a nosotros se nos complica ya que hay puestos en los que es imposible implementar el teletrabajo y maridar los puestos que sí y los que no. El puesto de trabajo trasciende de la tecnología a otros atributos que no habíamos tenido en cuenta. Hemos puesto herramientas que nos han dado la posibilidad de dar continuidad de negocio, pero todavía estamos lejos de esa hibridación. Está muy bien el teletrabajo, por ejemplo para la retención del talento, pero todavía tenemos que aprender a diferenciar entre los puestos que tienen posibilidad de teletrabajo y aquellos en los que no”.

En el encuentro quedó clara la diferencia que existe entre las compañías y cómo la implementación del digital workspace depende mucho del sector en el que opere. Para Miguel Ángel Ramos, Responsable Digital Workplace en Leroy Merlin, “la mayoría de nuestros colaboradores son de atención al público. A todos ellos, les ofrecemos escritorio y también movilidad en lo que se refiere a digital workplace. Así hemos conseguido adaptar las tiendas. Justo antes de la pandemia empezamos a trabajar con escritorios virtuales. Al principio hubo cuellos de botella porque la mayoría de los equipos no eran portátiles. Superado el cuello de botella, hemos retirado los sobremesa y todo trabajador que necesita un equipo trabaja con un portátil”.

Antonio Gómez de Zoom explicó lo que están viendo en las diferentes empresas: “Nosotros vemos lo que necesitan las empresas que tienen que gestionar grandes volúmenes de trabajo y quieren hibridar lo híbrido. Los fabricantes tenemos que dar soluciones a todas las tipologías de empresa y a sus necesidades. Para mí es difícil saber cuál va a ser la evolución en los próximos 4-5 años, porque la vuelta a la oficina se ha basado en utilizar las instalaciones que ya tengo pagadas. Al final, las soluciones son más complejas. Por ejemplo, en

una sala de reuniones ya no vale con una webcam. Por otro lado, tenemos la gestión de los espacios físicos de trabajo, que cambian de usuario y que no tienen un puesto de trabajo físico fijo y eso hay que adaptarlo. Estoy viendo también que hay tipos de gran cuenta de un entorno familiar que quiere volver a lo anterior e implementando las herramientas que tenían antes. El objetivo, al final, debe ser ofrecer la productividad total”.

### LA IMPORTANCIA DE LA PANDEMIA

Lo que está claro es que la pandemia cambió la forma en la que trabajaban las organizaciones. En este sentido, José Morales, Director TIC de Acciona explicó que “a nosotros la pandemia nos pilló con un presupuesto muy grande para hacer Campus Acciona. Justo nos pilló cuando empezábamos a establecer el proyecto de construcción. En aquel momento, salvo el equipo TIC, nadie teletrabajaba. Dos semanas antes del estado de alarma previmos lo que podría pasar y nos pusimos a trabajar y no tuvimos problema. Transcurrida la pandemia seguimos trabajando en el Campus y tan buena experiencia hemos tenido que lo vamos a exportar a otras localizaciones. Nosotros seguimos planificando lo que teníamos antes y estamos en la continuación de los proyectos que teníamos y ahora trabajamos de otra manera: el trabajador tiene que reservar su mes, una sala, y todo lo hace a través de su móvil. Esto ha requerido una reorquestación de diferentes proveedores pero somos muy potentes en TIC para hacer una infraestructura robusta. Los empleados están encantados con esta nueva experiencia. Lo que no sé es en que quedará el teletrabajo porque las filosofías de las empresas son diferentes: hay empresas que solo quiere el presencial y otras que tienen el teletrabajo implementado de forma total”.

Para Manuel Tarrasa Sánchez, CIO de Prosegur, “es curioso porque la gente joven que ha salido de la facultad se pierde muchas cosas, también en su formación, si hacen todo en remoto. Nosotros intentamos hacer un mix entre lo físico y lo remoto. Es



verdad que no está nada claro donde va a ir el teletrabajo, aunque creo que si la fuerza laboral es escasa y demanda teletrabajo, iremos hacia allí. Está cambiando todo a tanta velocidad que es difícil predecir a dónde vamos”.

Diego Carbajales, IT Workplace & Service Delivery Manager de Dufry tiene, además de su labor habitual, una tarea extra: “A primeros de año compramos Autogrill. Esto nos ha movido toda nuestra planificación y básicamente nuestro esfuerzo se basa en integrar a la nueva compañía. Tenemos muchas oportunidades para trabajar de forma más sencilla. Tenemos la premisa de que cualquier aplicación tiene que ser cloud first, pero es que ahora también lo tienen que ser las integraciones. Tenemos una estrategia de 3-2 en cuanto a ir a la oficina. Tenemos demanda de gente que quiere ir a la oficina y gente que quiere solo teletrabajo. El tema de seguridad también es muy importante y lo estamos cubriendo con tecnologías de virtual desktop”.

Manuel Asenjo, Director IT y Ciberseguridad en Broseta Abogados cree que “la feria va a ir por barrios. Yo represento a un despacho pequeño de abogados y nosotros, por las diferentes ubicaciones geográficas, tenemos que tener un workplace para poder trabajar en esas ubicaciones o en casa de los clientes, a pesar de que no tengamos implementado el teletrabajo de forma total. Hacemos mucho foco en la seguridad y todos nuestros equipos son portátiles salvo los de las personas de recepción”.

Por su parte, Rafael Corrales, CIO de Nuubo explicó que en su compañía, “ahora mismo estamos inmersos en implantar un ERP. Hay cosas que no podemos hacer en un entorno físico al tener presencia en diferentes localizaciones y países. Por eso, es importante para nosotros tener un digital workspace. Ahora mismo no nos planteamos un cambio de modelo que es hiperflexible ya que cada uno va a la oficina cuando quiere y cuando lo necesita. Tenemos también hiper-



flexibilidad en el horario y ya tenemos casi 5 ó 6 grupos de horarios de diferentes”.

Para Raquel Pinillos Gil, Business Solutions Director de Kyocera, la clave del éxito en la implementación del nuevo puesto de trabajo radica en el departamento de Recursos Humanos. Tal y como explicó la portavoz de la multinacional nipona “es fundamental que el departamento de RR.HH. trabaje de forma conjunta con el departamento de tecnología. La implementación del digital workspace no es sólo un asunto de implementar determinadas soluciones o de dotar a los trabajadores con un equipamiento específico. Hablamos de formas de trabajar, en las que las personas cobran un papel imprescindible. Por eso, una transformación del puesto de trabajo sólo es efectiva si se cuenta con ese trabajo conjunto entre ambos departamentos”

Por su parte, Néstor Cortés, Google Workspace Technical Lead de Incentro aseguró que “desde la pandemia vemos un cambio radical. Ahora observamos que cada empresa tiene filosofías diferentes. En nuestro caso tenemos flexibilidad total. Nos dimos cuenta que los espacios de trabajo digitales habían venido para quedarse. Creemos que hay una serie de características a tener en cuenta: accesibilidad para no depender de estar en un lugar físico. Colaboración en tiempo real que, en nuestro caso, ha permitido reducir los viajes. La organización de la estructura, que permite la organización de los archivos y los proyectos. La integración de las aplicaciones para facilitar que no haya ninguna caída del trabajo. La seguridad y la privacidad es otro de los elementos importantes. Y todo ello apostando por la nube”.

Pinillos explicó, por su parte que “la madurez de un negocio depende de la capacidad para medir que tienen las empresas. La parte del digital workspace tiene que ver con las aplicaciones y los procesos. Si los procesos en el back office no están alineados con el front office entonces hay una congestión importante. Eso es lo que ofrecemos desde Kyocera: la descongestión. En la parte que tenemos en conversaciones con CIOs lo que vemos es que hay una preocupación por descongestionar ciertas áreas o procesos que hacen que la tecnología no fluya para dar determinados servicios.”



# Ciberseguridad

## cloud

Las organizaciones utilizan cada vez más la nube y para hacer frente a los posibles riesgos, necesitan una solución de ciberseguridad que atienda a sus demandas. En este artículo, recogemos 13 propuestas. La primera es Barracuda Email Protection que reúne un conjunto de herramientas para la seguridad de Microsoft Office 365. Le sigue CrowdStrike Falcon Cloud Security ofrece una solución integrada y unificada desde el endpoint hasta la nube en una plataforma de protección de aplicaciones nativa en cloud tanto con o sin agente.

Mientras, CyberArk Secure Cloud Access proporciona acceso de privilegio permanente cero en entornos multi cloud, pero con los permisos suficientes para cumplir con el principio de acceso con privilegios mínimos. ESET participa con PROTECT Elite, una solución integral para empresas que necesitan una mayor visibilidad de sus redes y Fortinet con Security Fabric, una plataforma diseñada para abarcar la superficie extendida y el ciclo de ataque digital.

En el caso de Palo Alto Networks, su solución Prisma Cloud protege las aplicaciones en la nube desde el código para ayudar a implementar aplicaciones nativas de forma segura en menos tiempo. Le siguen Sophos Cloud Native Security que blinda cargas de trabajo, datos, aplicaciones y accesos en la nube frente a vulnerabilidades y amenazas a través de la plataforma Sophos Central.

Junto a la participación de Trend Vision One-Cloud Security, encontrarán más soluciones en nuestra web [www.revistabyte.es](http://www.revistabyte.es) donde también se encuentran las soluciones Veeam Data Platform, Netskope Intelligent Security Service Edge, Proofpoint Cloud App Security Broker, Bitdefender GravityZone Cloud y WatchGuard AuthPoint Total Identity Security, que añade funciones avanzadas de gestión de contraseñas y de supervisión de la dark web para proteger las credenciales corporativas.







# Barracuda Email Protection



Proporciona una seguridad completa a Microsoft Office 365. Las empresas, en función de sus necesidades, cuentan con tres versiones entre las que elegir.

Para las organizaciones que deseen proteger su negocio frente a las amenazas más avanzadas contenidas en los correos electrónicos, Barracuda Email Protection es una solución que permite la defensa de la puerta de enlace, defensa de la bandeja de entrada basada en API, respuesta ante incidentes, protección de datos y posibilidades de cumplimiento normativo.

Para bloquear el correo no deseado, el malware y las amenazas de día cero, Barracuda emplea técnicas avanzadas y ofrece también continuidad del correo electrónico, junto con el filtrado de correo saliente y el cifrado para evitar la pérdida de datos. Mientras, su tecnología integrada de Advanced Threat Protection utiliza los análisis de cargas y sandboxing para detectar malware de día cero. La protección de enlaces redirige las URL sospechosas y con errores tipográficos deliberados, al igual que 'Seguridad Web' bloquea el acceso a dominios maliciosos para evitar que los destinatarios descarguen malware sin darse cuenta.

Barracuda Email Protection dispone, por otro lado, de una arquitectura que permite que su motor de inteligencia artificial estudie los correos electrónicos históricos y aprenda los patrones de comunicación únicos del usuario. Después puede identificar anomalías en los metadatos y el contenido del mensaje para encontrar y bloquear los ataques de ingeniería social en tiempo real. La solución se encuentra también preparada para detectar comportamientos de correo electrónico anómalos y enviar alertas a los departamentos de TI de las empresas; a continua-

FUNCIONES	ADVANCED	PREMIUM
Protección de correo no deseado y antimalware	✓	✓
Protección de adjuntos	✓	✓
Protección de enlaces	✓	✓
Continuidad del correo electrónico	✓	✓
Cifrado de correo electrónico	✓	✓
Prevención de la pérdida de datos	✓	✓
Protección frente a Phishing y suplantación de identidad	✓	✓
Protección frente a la usurpación de cuentas	✓	✓
Reparación automática	✓	✓
Protección del fraude de dominio		✓
Seguridad Web		✓
Búsqueda y respuesta ante amenazas		✓
Flujos de trabajo automatizados		✓
Integración de SIEM/SOAR/XDR		✓
Archivado en la nube		
Cloud-to-Cloud Backup		
Inspector de datos		
Simulación de ataques		
Security Awareness Training		

ción, encuentra y elimina todos los correos electrónicos fraudulentos enviados desde cuentas comprometidas.

En el caso de que una organización desee asegurar sus datos y garantizar el cumplimiento normativo, Email Protección permite disponer de backups en la nube para los datos de Office 365 incluidos los buzones de correo electrónico de Exchange Online, SharePoint Online, OneDrive para la empresa y Teams. Con una opción de recuperación puntual rápida en caso de borrados accidentales o maliciosos, el archivado en la nube ayuda a cumplir con los requisitos de cumplimiento normativo con la exhibición de documentos electrónicos, las políticas de retención personalizadas, y el almacenamiento y retención ilimitados.

Con un acceso basado en Zero Trust que verifica continuamente la identidad y la confianza de los empleados y los dispositivos, la solución de Barracuda incluye otras características de interés como formación en seguridad y vídeos de microaprendizaje, e informes y paneles personalizados. Es posible elegir entre tres planes: Advanced, Premium y Premium Plus.

## Barracuda

Web: Aqua eSolutions

Tel: +44 118 338 4600

Web:

www.barracuda.com





# CrowdStrike Falcon Cloud

Una solución que incorpora, entre otros, protección de cargas de trabajo, gestión de posturas de seguridad cloud y gestión de responsabilidades de identidad cloud.

Seguridad integrada y unificada desde el endpoint hasta la nube en una plataforma de protección de aplicaciones nativa en cloud (CNAP) tanto con o sin agente. Así se presenta la solución CrowdStrike Falcon Cloud Security, con la que se pueden consolidar herramientas fragmentadas para proteger todos los activos en la nube, incluyendo protección de cargas de trabajo (CWP), gestión de posturas de seguridad cloud (CSPM) y gestión de responsabilidades de identidad cloud (CIEM).

En el caso de la gestión de posturas de seguridad cloud, ofrece visibilidad multi cloud, monitorización continua y detección de amenazas. De la misma manera, simplifica las políticas de cumplimiento gracias al despliegue de aplicaciones de forma rápida sin importar el entorno en el que se trabaja. Por su parte, para las cargas de trabajo, la solución de CrowdStrike facilita su protección completa en cualquier entorno, desde el endpoint a la nube, con herramientas de descubrimiento de amenazas automatizadas y con protección de todas las cargas de trabajo; se integra, además, con los equipos de DevOps para proporcionar un soporte de entrega e integración continuas (CI/CD).

Falcon Cloud Security dispone también de funciones de seguridad basadas en identidades, la visibilidad y la gestión de accesos con privilegios simplificada, de modo que el rendimiento de la remediación en las fases de test mejora los resultados de despliegue e integración. Se brinda,



por otro lado, seguridad para contenedores en Amazon Web Services, Microsoft Azure y Google Cloud, identificando las vulnerabilidades desde el desarrollo a la producción en cualquier cambio en las políticas de seguridad o en la estrategia cloud. Todo este enfoque le permite ofrecer un 100 % de visibilidad unificada, protección y compliance para entornos híbridos y multi cloud. Además, minimiza los riesgos producidos por errores de configuración y por exposición accidental, así como otros fallos humanos gracias a la presencia de indicadores de configuración errónea. De esta manera, se asegura una rápida respuesta y se limitan las superficies de ataque de los criminales. De igual forma, la solución de CrowdStrike proporciona una res-

puesta ante incidentes end-to-end en la nube, threat hunting, despliegue en plataformas y detección y respuesta gestionada 24 x 7 en entornos cloud. Para finalizar, añadir que como plataforma unificada de ciberseguridad identifica y detiene brechas mediante una serie de indicadores de ataque que detectan cualquier amenaza sin importar si surge en el endpoint o en la nube.

**CrowdStrike**

**Tel:** +1 (888) 512 8906

**Web:**

**[www.crowdstrike.com/es](http://www.crowdstrike.com/es)**

**Precio:** a consultar

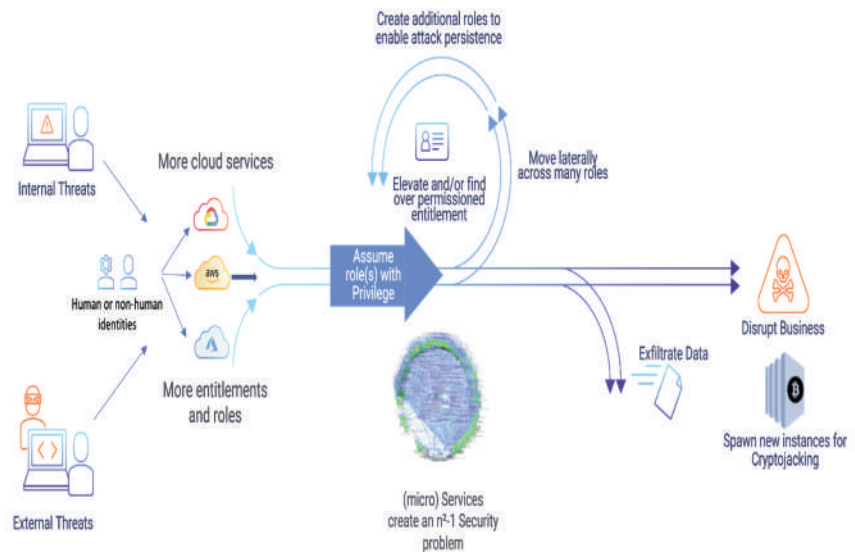
# Cyberark Secure Cloud Access

Entre sus características, incluye el aprovisionamiento just-in-time, que reduce el riesgo de robo de credenciales y secuestro de navegadores en entornos de nube pública

La solución CyberArk Secure Cloud Access se caracteriza por proporcionar acceso de privilegio permanente cero en entornos multi cloud, pero con los permisos suficientes para cumplir con el principio de acceso con privilegios mínimos. Además, la solución SaaS, parte de la plataforma de Seguridad de las Identidades de CyberArk, permite eficiencias operativas para los equipos de IAM y seguridad que implementan Zero Trust.

Esto mejora la seguridad al eliminar cualquier acceso permanente cuando no esté utilizándose, mientras que la combinación de elevación just-in-time y permisos para privilegios mínimos reduce el riesgo en las sesiones más confidenciales en la nube pública, es decir, aquellas que implican configuraciones de entornos de nube. Por otro lado, Secure Cloud Access proporciona experiencias de usuario nativas a los equipos de Cloud Engineering y DevOps permitiéndoles acceder, de forma nativa y segura, a la capa de administración de la nube.

Destacan cuatro beneficios principales. El primero es la reducción medible del riesgo cibernético. A través del aprovisionamiento just-in-time, la solución reduce el riesgo de robo de credenciales y el secuestro de navegadores en entornos de nube pública. Aquí, las políticas de acceso con privilegios mínimos limitan el radio de actuación de cualquier acceso comprometido, lo que reduce aún más el riesgo. El segundo beneficio es que Cyberark Secure Cloud Access permite habilitar la eficiencia operativa. En este caso, proporciona una solución única para



asegurar el acceso a la capa de administración de la nube en entornos multi cloud: como resultado, se elimina la necesidad de parchear varias herramientas y procesos. Además, los clientes pueden integrarla con sus chatOps, flujos de trabajo y sistemas ITSM.

El tercero de los beneficios está relacionado con asegurar la transformación digital. Esto significa que Secure Cloud Access permite a las organizaciones federar el acceso necesario a sus usuarios finales para completar las operaciones de gestión de la nube, con aprovisionamiento just-in-time para reducir el riesgo de identidades comprometidas. Mientras, las capacidades de automatización permiten a las organizaciones garantizar que cada vez que creen un nuevo entorno en la nube (cuenta de AWS, suscripción de Azure

o GCP Project), el acceso just-in-time con privilegios mínimos se aprovisiona automáticamente.

El último beneficio es el de la auditoría. Al supervisar las sesiones de consola basadas en web, se agiliza la revisión de la auditoría. Secure Cloud Access también ayuda a las organizaciones a demostrar el estricto cumplimiento del principio de privilegios mínimos.

## Cyberark

**Web:**

[www.cyberark.com/es](http://www.cyberark.com/es)

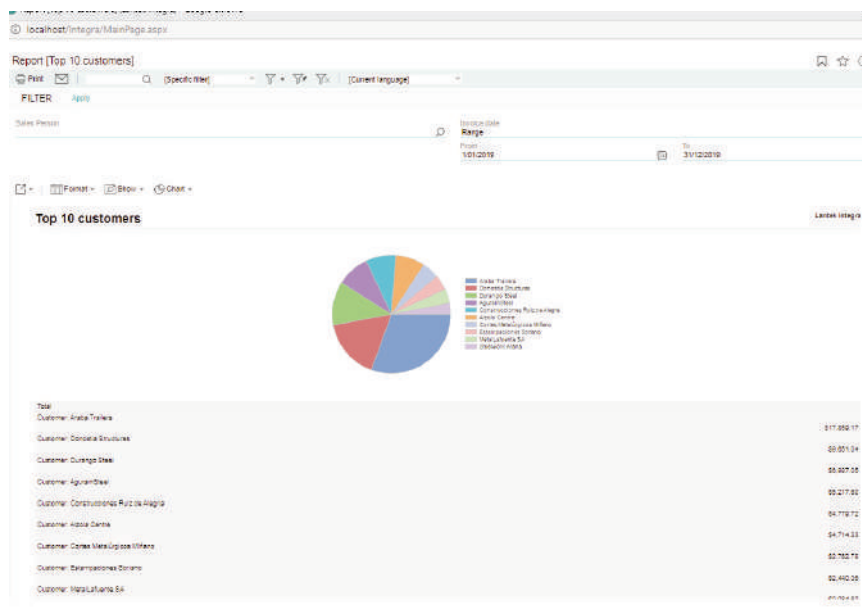
**Teléfono:**

+44-203-728-7074

# ESET PROTECT Elite

Su sistema de detección proporciona a los equipos de seguridad de las empresas información en tiempo real recopilada por más de 100 millones de equipos.

El XDR para empresas de esta solución integral garantiza que las amenazas emergentes, el comportamiento imprudente de los empleados y las aplicaciones no deseadas no pongan en riesgo la reputación o los beneficios de la organización. Dentro de este contexto, responde de forma proactiva al entorno de amenazas en constante evolución y brinda a las ciberdefensas capas de protección en constante innovación que protegen: endpoints, correo electrónico, aplicaciones en la nube y almacenamiento de datos. Ofrece, asimismo, evaluación continua de vulnerabilidades con priorización y remediación basadas en riesgos para reducir la exposición a los ataques; cifrado de disco completo; y autenticación multifactor para mejorar la protección de los datos y las identidades. Entre las herramientas que integra se encuentra ESET Cloud Office Security, que proporciona protección avanzada para aplicaciones de Microsoft 365 mediante una consola en la nube. También una combinación de filtrado de spam, análisis antimalware y antiphishing que ayuda a proteger las comunicaciones y el almacenamiento en el entorno cloud. Por su parte, ESET Full Disk Encryption es una característica propia de la consola ESET PROTECT que permite la implementación y el cifrado de datos para los equipos Windows y macOS conectados. ESET Full Disk Encryption ayuda, igualmente, a cumplir con las normativas de protección de datos gracias, entre otros, al cifrado de discos del sistema, particiones o unidades enteras, e implementación, activación y cifrado de



dispositivos en una sola acción. Mientras, ESET Endpoint Security brinda prevención de control contra el malware y los exploits, y puede detectar malware antes, durante y después de su ejecución. Ahora también dispone de una tecnología contra la detección de contraseñas.

Para evaluar y corregir activamente las vulnerabilidades de los endpoints, se encuentra ESET Vulnerability & Patch Management: efectúa un seguimiento activo de las vulnerabilidades en sistemas operativos y aplicaciones comunes y permite la aplicación automatizada de parches en todos los endpoints gestionados a través de una plataforma unificada. Con ella, además es posible personalizar las políticas de aplicación de parches; filtrar, agrupar y clasificar las vulnerabilidades en fun-

ción de su gravedad; y elegir entre las opciones de parcheo manual y automático. También destaca ESET Secure Authentication, una solución de autenticación multifactor (MFA) desde el dispositivo móvil que protege a las empresas de las vulnerabilidades causadas por contraseñas débiles e intentos de acceso no autorizados: notificación push y claves de hardware existentes.

**ESET**

**Tel:** 962 913 348

**Web:** [www.eset.com/es](http://www.eset.com/es)

**Precio:**

A consultar

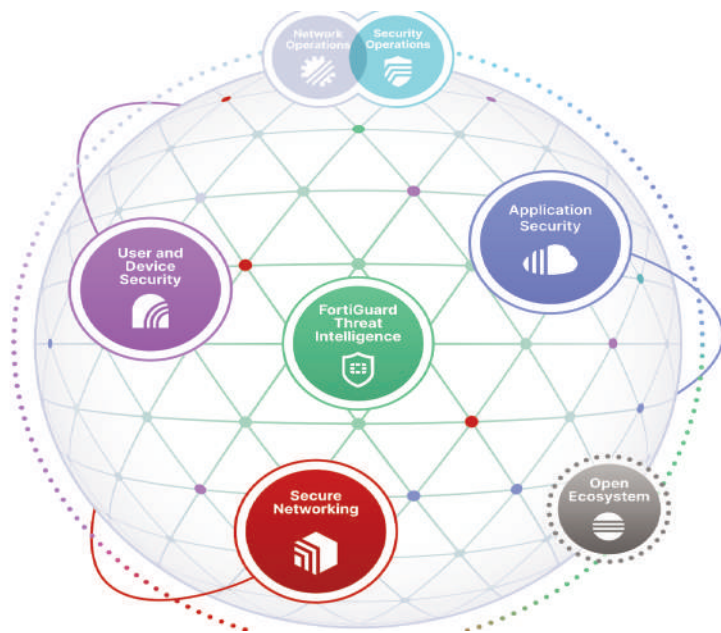


# Fortinet Security Fabric

Aúna los conceptos de convergencia y consolidación para ofrecer una protección integral de la ciberseguridad en tiempo real, desde los usuarios hasta las aplicaciones

Impulsada por el sistema operativo de Fortinet, FortiOS, se trata de una plataforma de ciberseguridad diseñada para abarcar la superficie extendida y el ciclo de ataque digital, lo que permite disponer de seguridad y redes de recuperación automática para proteger dispositivos, datos y aplicaciones. Además, ofrece diversos modelos de implementación (entornos físicos, virtuales, en la nube y todo como servicio) y comprende un ecosistema y cartera de productos donde tienen cabida endpoints, redes y nubes.

Teniendo en cuenta que para romper la secuencia de ataques las organizaciones deben ajustar rápidamente su postura de seguridad para defenderse de forma cohesiva, Fortinet Security Fabric proporciona un enfoque amplio, integrado y automatizado. Amplio porque detecta amenazas, hace cumplir la seguridad en todas partes y permite una detección coordinada de estas amenazas en tiempo real con la aplicación de políticas en toda la superficie de ataque digital y el ciclo de vida. En cuanto a su enfoque integrado, comentar que contribuye a cerrar las brechas de seguridad y que cuenta con un análisis impulsado por inteligencia artificial y prevención automatizada para ofrecer una seguridad uniforme y coherente, así como operaciones simplificadas en distintas tecnologías, ubicaciones e implementaciones. Respecto a su enfoque automatizado, Fortinet Security Fabric considera el contexto y brinda automáticamente una protección coordinada en toda el área a proteger, desde el usuario a las aplicaciones casi en tiempo real.



Mientras, la automatización de procesos simplifica las operaciones para implementaciones a gran escala y libera a los equipos de TI.

Los pilares sobre los que se sustenta son la integración nativa de todos los servicios de inteligencia de amenazas y seguridad de FortiGuard, lo que permite una detección y aplicación coordinada en toda la superficie de ataque. Estos servicios se basan en los modelos de Machine Learning e inteligencia artificial de FortiGuard Labs, el área de investigación de amenazas de Fortinet; por su parte, Fortinet Secure Networking aborda los desafíos de aceleración digital al integrar estrechamente la infraestructura de red con seguridad avanzada en todos los perímetros. Esto permite desplegar políticas de seguridad coherentes y proporcio-

nar una mejor experiencia de usuario para los trabajadores híbridos. Respecto al acceso de confianza cero, conecta de forma segura las aplicaciones alojadas en cualquier lugar con los usuarios que trabajan desde cualquier lugar. Ofrece así una seguridad consistente y sin problemas en todas las aplicaciones y usuarios, ajustándose automáticamente a los riesgos percibidos sobre la BBDD.

**Fortinet**

**Tel:** 91 133 21 00

**Web:**

[www.fortinet.com](http://www.fortinet.com)

**Precio:** consultar

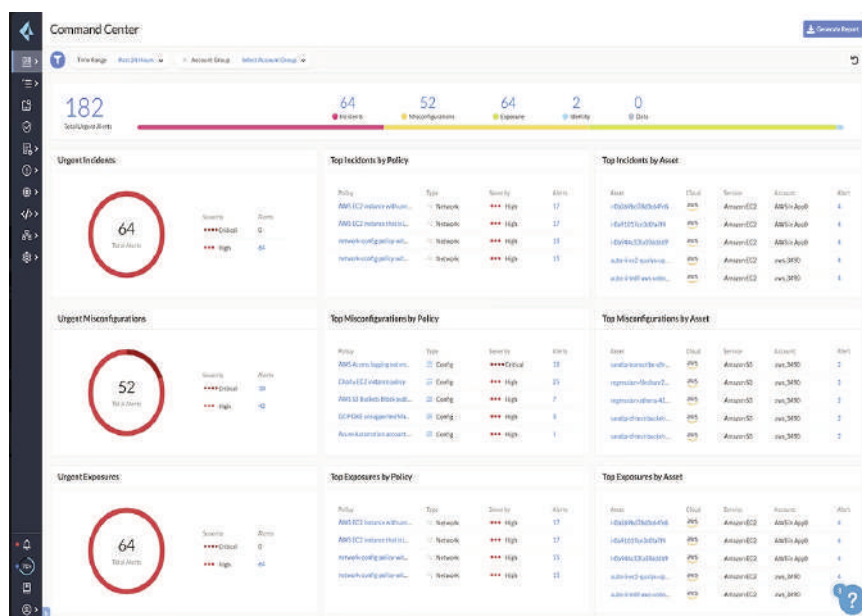
# Palo Alto Networks Prisma Cloud

Protege las aplicaciones en la nube desde el código para ayudar a las organizaciones a implementar aplicaciones nativas de forma segura en menos tiempo.

A medida que continúa la adopción y expansión de la nube, las organizaciones necesitan apostar por un enfoque de plataforma que asegure el ciclo completo de vida de las aplicaciones, desde que se escribe el código hasta que la aplicación se encuentra en producción en cualquiera de los entornos de nube pública, privada o híbrida. A este respecto, los servicios de seguridad en nube de Palo Alto Networks están integrados de forma nativa y ofrecen capacidades similares de protección en todos los entornos; unas capacidades que no solo cuentan con el respaldo de la Unit 42, un importante equipo de investigación de amenazas, sino que además se nutren de la inteligencia extraída de más de 85.000 clientes internacionales que generan una inteligencia procedente desde todos los vectores de ataque para detener tanto las amenazas conocidas como las desconocidas.

Prisma Cloud es un servicio de seguridad y cumplimiento que descubre dinámicamente recursos y datos confidenciales en la nube, y posteriormente detecta configuraciones de riesgo, amenazas de red, comportamientos sospechosos de usuarios, malware, filtración de datos y vulnerabilidades de host en GCP, AWS y Azure. Además, la plataforma proporciona un enfoque integrado que permite a los equipos de operaciones de seguridad y DevOps colaborar y acelerar el desarrollo seguro de aplicaciones nativas en la nube.

Prisma Cloud también protege y se integra con arquitecturas y conjuntos de herramientas nativos de la nube para



garantizar una cobertura de seguridad completa a la vez que rompe los silos operativos de seguridad en todo el ciclo de vida de la aplicación. Fundamentalmente, permite la adopción de DevSecOps y una mayor capacidad de respuesta a las cambiantes necesidades de seguridad de las arquitecturas nativas de la nube. Del mismo modo, elimina los puntos ciegos y detecta amenazas para brindar a los usuarios una visibilidad completa, una detección continua de las amenazas y una respuesta automatizada.

Las organizaciones tienen a su disposición otras características a destacar como la posibilidad de proteger los hosts, los contenedores y las funciones sin servidor en todo el ciclo de vida de las aplicaciones; o prevenir amenazas no solo en la

propia infraestructura sino en APIs y datos en tiempo de ejecución en la nube pública mientras se protegen también las máquinas virtuales y los kubernetes. Se integra de igual modo con las herramientas y el entorno de la empresa para identificar vulnerabilidades, errores de configuración y riesgos de seguridad durante las fases de código y compilación.

## Palo Alto

Tel: 866 320 4788

Web:

[www.paloaltonetworks.es](http://www.paloaltonetworks.es)

Precio: A consultar

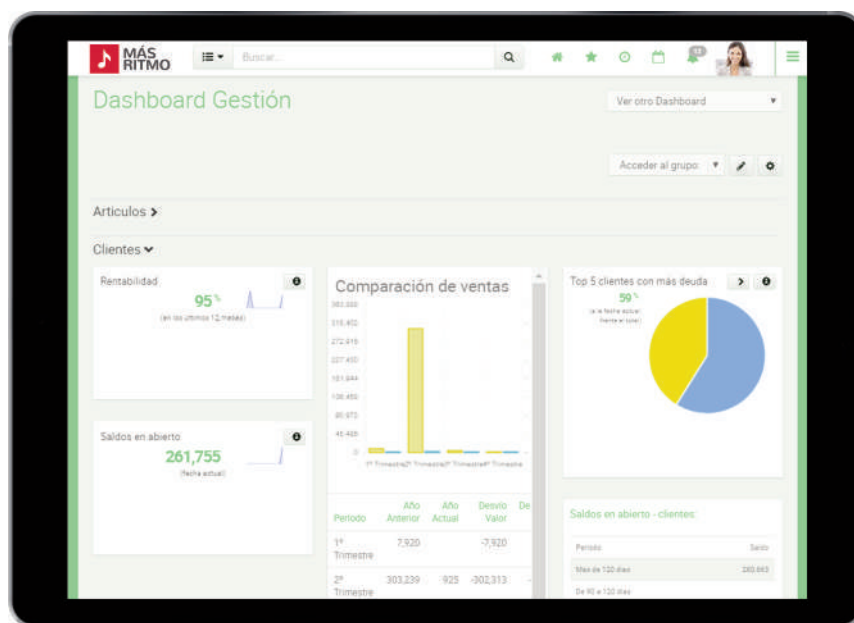
# Sophos Cloud Native Security



Protege cargas de trabajo, datos, aplicaciones y accesos en la nube frente a vulnerabilidades y amenazas a través de la plataforma de ciberseguridad Sophos Central.

Sophos Cloud Native Security es una solución que proporciona una completa cobertura de seguridad multi nube en todos los entornos, cargas de trabajo e identidades de Amazon Web Services, Microsoft Azure y Google Cloud Platform, a fin de detectar y de remediar los riesgos de seguridad y mantener el cumplimiento. Como plataforma integrada de seguridad, unifica también la gestión de derechos para garantizar los mejores resultados de visibilidad, protección y cumplimiento; y todo ello integrado con herramientas SIEM, de colaboración, de flujo de trabajo y de DevOps para incrementar la agilidad en todas las organizaciones.

Su tecnología le permite, en otro orden de cosas, identificar y detener el malware, así como los exploits, los errores de configuración y los comportamientos anómalos mediante herramientas de detección y respuesta ampliadas (XDR). Además de buscar amenazas, las empresas reciben detecciones priorizadas y se benefician de los eventos de seguridad conectados automáticamente en los entornos de AWS, Azure y GCP para optimizar los tiempos de investigación y respuesta. Mientras, las herramientas de remediación y seguridad en la nube disponibles en Cloud Native Security pueden ser gestionadas por los propios equipos de seguridad de cada compañía, a través de un partner de Sophos o el servicio Sophos Managed Threat Response para acelerar su ciberresiliencia y hacer frente a los incidentes de seguridad actuales. Sophos Cloud Native Security se pue-



de complementar con Sophos MTR. Este servicio de detección y respuesta gestionadas puede trabajar con los propios equipos de las organizaciones, monitorizar su entorno las 24 horas del día los 7 días de la semana a lo largo de los 365 días del año, responder a posibles amenazas, buscar indicadores de peligro y proporcionar análisis detallados sobre los eventos que incluyen lo que ha ocurrido, dónde, cuándo, cómo y por qué para evitar que las amenazas se dirijan contra sus datos y sus sistemas. También destaca la presencia de una consola de gestión unificada para todas las tecnologías de ciberseguridad en la nube híbrida de Sophos, incluida la protección para endpoints, dispositivos móviles, servidores, firewalls, switches, redes inalámbricas,

correo electrónico y acceso seguro. En este sentido, Sophos Central hace que la ciberseguridad resulte más fácil, pero a la vez efectiva gracias a la información compartida en tiempo real entre sus productos, XDR Data Lake, y los paneles de control y alertas consolidados. La protección de las cargas de trabajo en la nube se extiende tanto a entornos Windows como Linux.

**Sophos**

**Tel:** 91 375 67 56

**Web:** [www.sophos.com/es](http://www.sophos.com/es)

**Precio:**

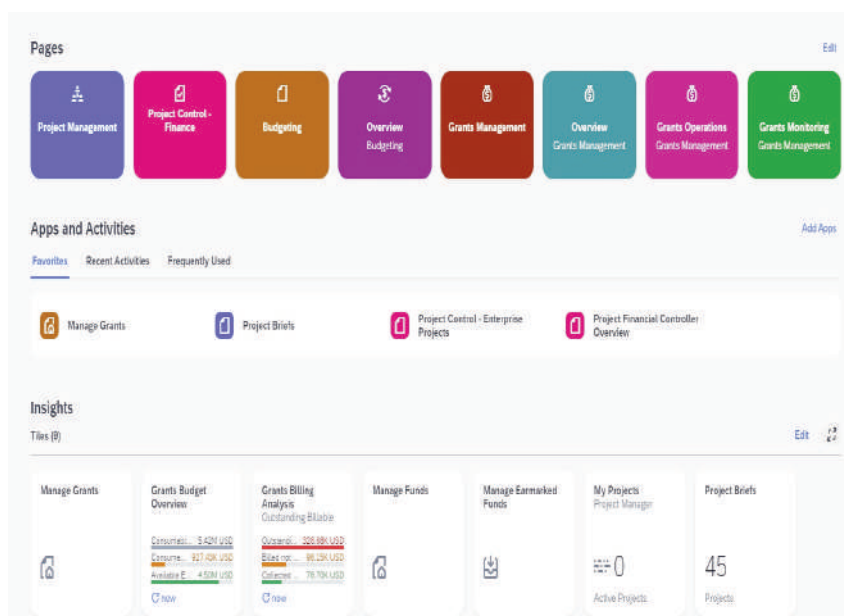
A consultar



# Trend Vision One-Cloud Security

Abarca una gestión de riesgos de la superficie de ataque, protección multicapa en entornos híbridos y XDR de nueva generación

Dentro de la plataforma Trend Vision One se integra la solución Trend Vision One - Cloud Security, o Cloud Security, que reúne un conjunto de servicios de seguridad para creadores de nubes con los que proteger las infraestructuras disponibles en este entorno. Estos servicios son: Workload Security, que ofrece protección en tiempo de ejecución para cargas de trabajo (virtuales, físicas, cloud y contenedores); Container Image Security, para el escaneo de imágenes en el canal de compilación; File Storage Security, seguridad para servicios de almacenamiento de objetos y ficheros en la nube; Application Security, seguridad para funciones, API y aplicaciones sin servidor; Network Security, seguridad IPS de la capa de red en la nube; Conformity, para la gestión de la postura de seguridad y conformidad de la nube; y Open Source Security by Snyk que se enfoca a la visibilidad y la supervisión de vulnerabilidades de código abierto y riesgos de licencia. Entrando en detalle, Trend Cloud Security proporciona soluciones para la migración hacia la nube, automatizando el descubrimiento y la protección de los entornos de nubes públicas, privadas y virtuales, a la vez que protege la capa de red. Esto garantiza flexibilidad y simplicidad para asegurar la nube a lo largo de todo el proceso de migración y expansión: así, las empresas pueden tener una mayor visibilidad y seguridad consistente en todos sus entornos de nube con la mayor cantidad de controles de seguridad e integraciones dentro



de sus conjuntos de herramientas existentes.

Ofrece, por otro lado, soluciones para aplicaciones nativas en la nube. Con CI/CD, contenedores, plataformas sin servidor y otras prácticas y tecnologías de desarrollo modernas, las organizaciones necesitan una seguridad para las aplicaciones nativas de la nube que les brinde una protección conectada a lo largo de su ciclo de vida; y con la garantía de que sus servicios cumplen con las prácticas recomendadas de seguridad mientras permiten que sus desarrolladores hagan su trabajo. Trend Cloud Security les permite crear y ejecutar aplicaciones a su manera con seguridad integrada. En otro orden de cosas, es posible evaluar automáticamente cómo los servicios en la nube se alinean con

las mejores prácticas de configuración y los estándares de cumplimiento de normativa de la industria. Esto facilita incorporar una cultura de DevSecOps en las empresas dándole el poder a sus equipos para desarrollar una mejor arquitectura y aplicaciones en la nube, a la vez que tienen la seguridad necesaria para crecer y escalar su negocio sin sobresaltos.

## Trend Micro

**Tel:** 913 69 70 30

**Web:** [www.trendmicro.es](http://www.trendmicro.es)

**Precio:**

A consultar

# La evolución del ERP y CRM



A pesar de ser herramientas con años de antigüedad, el CRM y el ERP siguen siendo esenciales para las organizaciones. La nube o la IA están transformando estas herramientas

Vanesa García



La planificación de recursos empresariales (ERP) y la gestión de relaciones con los clientes (CRM) son las dos soluciones a las que las empresas dan prioridad en su inversión tecnológica. Son la base de la transformación digital de cualquier organización, pues su uso no solo implica la implementación de una herramienta útil sino un cambio en los procesos, en las formas de trabajar y en las capacidades de las personas que lo usan, aportando agilidad, eficiencia, transversalidad y ahorro de tiempo y costes.

Además, nos encontramos en la era de los datos y estas soluciones brindan la oportunidad de albergar todos ellos en un solo sistema, así como integrar todos los procesos empresariales. Cuestiones clave tanto para ofrecer la mejor experiencia de cliente como para tomar las mejores decisiones de negocio, sustentadas por datos.

Para Pablo Serna, Director de Product Management para Pymes, Asesorías y Despachos profesionales de Cegid en España, en la situación actual del mercado del ERP y el CRM

todavía hay mucho por hacer, “en un estudio reciente que llevamos a cabo entre nuestros clientes del sector asesorías y despachos profesionales, nos encontramos que más del 50% aún no disponían de



## TEMA DE PORTADA

---

ERP para la gestión integral de su despacho. Y, lamentablemente, ese sector no es un caso aislado. Como muestran datos del Observatorio Nacional de Tecnología y Sociedad (ONTSI), el uso de ERP es del 52% en empresas TIC, pero en otros sectores es aún más bajo: un 50% en el industrial, un 47% en el sector servicios y un 30% en el de la construcción. Es necesario analizar el sector tecnológico para verlo subir hasta un 65%”.

Eva Mirás, Directora Comercial de Zucchetti Spain incide en que, tecnologías como la Inteligencia Artificial, el Big Data, el Cloud o el Internet de las Cosas están planteando nuevos desafíos, “hace falta abordar la necesidad de una mayor automatización y una transformación digital inteligente con soluciones de gestión de última generación. Un alto porcentaje de empresas siguen trabajando con herramientas obsoletas y no existe una integración adecuada con otras soluciones que utilizan en su día a día, como el software TPV, de gestión de RRHH, MES, eCommerce..”.

### ERRORES COMUNES

Muchas veces las empresas no son conscientes de lo que necesitan. Un error habitual es tomar la decisión de implantar un ERP sin considerar la evolución futura de la empresa, por lo que en un corto espacio de tiempo pueden verse limitados si han elegido una herramienta poco flexible y que no facilita la integración.

“Es muy importante contar con el asesoramiento de un partner tecnológico, que pueda concienciar a la dirección de la empresa sobre la tecnología, etapas y procesos que se van a llevar a cabo para lograr el máximo beneficio para la empresa. En Zucchetti Spain somos conscientes de esta necesidad y nos diferenciamos por actuar como un socio tecnológico de nuestros clientes, adaptándonos y a sus nuevas necesidades y anticipándonos a los cambios del mercado para brindarles siempre las soluciones más vanguardistas con las que garantizar su proyecto de futuro”, dice Eva Mirás, Directora Comercial de Zucchetti Spain.

Profundizando en los errores más comunes, Francesc Núñez, ERP Product Manager, Wolters Kluwer Tax & Accounting España incide en que antes de iniciar una implementación de una solución ERP o CRM, deberíamos reflexionar sobre tres preguntas básicas. ¿Qué quiero conseguir? ¿Estoy dispuesto a conseguirlo? ¿Puedo conseguirlo?.

“La primera pregunta debe responderse con unos objetivos claros. Es fundamental para el éxito del proyecto que las expectativas estén claras y alineadas. Además, los objetivos marcados deben ser posibles, alcanzables y, por supuesto, medibles y acotados en el tiempo. La segunda

pregunta reflexiona sobre la implicación en la implementación. Toda la compañía debe estar dispuesta al cambio, y esto es fundamental, pero al mismo tiempo complicado. Los bloqueos internos en muchas ocasiones son la causa del fracaso total o parcial de una implementación. Un cambio de este tipo siempre tiene que ser impulsado por la dirección de la compañía, y se debe involucrar a todos los miembros, analizando, sobre todo, el liderazgo del cambio y la necesidad de nuevo talento. Y una vez claros objetivos y motivación al cambio, otra reflexión es si la empresa dispone o no de los recursos para esta implantación, y normalmente, el recurso más importante (salvado el económico) es el tiempo. La dedicación en tiempo al cambio es fundamental”.

Pablo Serra aboga por la participación activa de los empleados para conseguir una buena implementación de estas soluciones, “esto suele variar según el tamaño de la empresa. Las grandes empresas sí que suelen tener una idea mucho más exacta de lo que necesitan



implementar, precisamente, porque ya suelen contar con un ERP u otra solución de gestión empresarial y, a menudo, el cambio es para cubrir nuevas necesidades que su proveedor actual no puede satisfacer o disponer de nuevos módulos para ofrecer más ventajas a sus clientes. Sin embargo, en el caso de las pymes y micropymes, nos encontramos con un nivel de digitalización mucho menor. Un error común, a menudo, es que no cuentan con una estructura ni procesos de trabajo claros, ni haber involucrado a los usuarios clave desde el principio, lo que suele ayudar a evitar la habitual resistencia al cambio. Por ello, el proceso de formación y onboarding aquí debe ser mucho más meticuloso e incluso, contar con la posibilidad de ofrecer un servicio de consultoría”.


Carlos Esteve, director de desarrollo de negocio de Grupo Aitana, asegura que hay varios elementos en los que se cometen errores. En su opinión, “el problema es que todavía quedan compañías que comienzan procesos de implantación de ERPs y CRMs guiándose sólo por el precio, no por lo que les va a ayudar a mejorar. También hay CEOs que

no lideran el cambio y que no consideran estos proyectos como estratégicos, por lo que destinan escasos recursos a su éxito y como consecuencia no lo priorizan frente a otros. Y el tercer error más habitual sería la falta de concreción y de medición de los objetivos. Si no enfocamos el proyecto de digitalización adecuadamente, en vez de una inversión habremos hecho un gasto”.


### **BENEFICIOS DE LA NUBE EN EL ERP Y EL CRM**

El papel de la nube en el mercado juega un papel fundamental. La adopción de la nube ha transformado la forma en que las empresas implementan y utilizan sus soluciones ERP y CRM. Por un lado, este modelo permite el acceso a los usuarios desde cualquier dispositivo con conexión a Internet y por tanto desde cualquier lugar aportando flexibilidad para aquellos equipos que precisen de esta movilidad o simplemente trabajen fuera de la oficina.

Además, a nivel de costes evitar la necesidad de invertir en infraestructura de servidores y equipos costosos, así co-



La analítica que  
incorporan estas soluciones  
está acelerando la toma  
de decisiones



mo exige a las compañías de tareas técnicas y les permite enfocarse en actividades más estratégicas para el negocio ya que son los propios proveedores los que se encargan de las actualizaciones, parches de seguridad o el mantenimiento.

En palabras de Gonzalo Valle, director de preventa de IFS, la nube permite escalar fácilmente los recursos de la solución ERP o CRM según las necesidades de la empresa, “si se requiere más capacidad de almacenamiento, potencia de procesamiento o usuarios adicionales, se puede lograr con facilidad lo que garantiza que la solución pueda crecer junto con el negocio. De hecho, facilita la integración con otras aplicaciones y servicios, lo que permite una colaboración más fluida entre diferentes sistemas y departamentos mejorando así la visibilidad de la información para una mejor toma de decisiones”

En esta misma línea, para Eva Mirás proporciona una mayor accesibilidad, seguridad y escalabilidad a las empresas que no cuentan con su propia infraestructura, “supone también un ahorro de costes significativo, al poder delegar este área en el proveedor de software. Las empresas pueden así contratar soluciones como servicio y optar por herramientas que permiten el pago por uso. Esto ayuda a adaptarse mejor ante cualquier tipo de circunstancia”.

Y es que, “trabajar en un entorno cloud facilita la integración de todos los datos y su actualización en tiempo real, pues es capaz de recoger todos los datos de distintos usuarios trabajando a la vez desde distintos lugares. Otra gran ventaja de los software en la nube es que permite que estén siempre actualizados a la normativa aplicable por parte del proveedor y sin necesidad de que el cliente tenga que descargarse nada proactivamente. Además, la nube permite la escalabilidad, es decir, que estos sistemas pueden adaptarse a las nuevas necesidades de la empresa a medida que crece: agregar usuarios, funciones..”, comenta Pablo Serna, director de Product Management de Cegid.

### EL ROI EN LA NUBE

El objetivo de un software en la nube es transformar los procesos de las empresas para que haya más automatización, productividad y eficiencia. Pero también es una ayuda esencial para mejorar la toma de decisiones. Para analizar el ROI de una solución de gestión, Eva Mirás explica que es necesario dejar un margen de al menos un año hasta que se hayan consolidado todas las transformaciones. “A partir de ahí, se podrá observar una mejora de la productividad y la eficiencia del personal, con una mejor relación coste/beneficio, por un lado, y por otro, una mejora en la toma de decisiones permitirá comparar la evolución de los ingresos desde que empezó a utilizarse la nue-



va solución ERP en la nube”

“La medición del ROI implica varios ejercicios. Por un lado, está el cambio de modelo de inversión: en lugar de un gran proyecto de inversión en infraestructura se pasa a un gasto operativo recurrente. Por otro lado, se reducen los costes y necesidades internos de gestión y mantenimiento de infraestructura. Para calcular el ROI hay que cuantificar muy bien cuánto sería ese gasto de gestión y mantenimiento en igualdad de condiciones (calidad de servicio, seguridad, accesibilidad...)”, resalta Toni Parada, Head of Digital Business & Customer Engagement, de aggity.

Pablo Serna resume en dos, las consideraciones a tener en cuenta para el ROI: “En primer lugar, es necesario cuantificar los beneficios esperados al implementar la solución: en cuánto se reducen los costes de gestión, en cuánto aumenta el % de productividad de los equipos, etc. Bien es cierto que muchos parámetros, como la mejora en la toma de decisiones o la excelencia del servicio al cliente, no se pueden medir de forma cuantitativa sino solo cualitativamente. En segundo lugar, habrá que determinar los costes de la inversión: la licencia del propio software, su infraestructura, la migración de los datos, la consultoría del producto o la propia formación para los empleados”.

## EL IMPACTO DE LA ANALÍTICA Y LA IA

La analítica ayuda a tomar decisiones que tienen un mayor grado de éxito, porque están asentadas en datos que proporcionan información de valor para la organización. Por lo que, a la hora de evaluar estrategias, una empresa que apuesta por el análisis de datos comprenderá el entorno en el que se desenvuelve, siendo más competitiva y como resultado de esto aumentando sus ingresos.

“Una de las herramientas para gestionar el gran volumen de datos que manejan las empresas es el Big Data. Esta herramienta es clave a la hora de analizar el rendimiento de las soluciones de gestión empresarial, porque los datos necesitan ser moldeados para interpretarlos de manera óptima. Por ello, el software empresarial se ha convertido en una solución fundamental para las empresas porque permite la recopilación de un gran volumen de datos y su posterior análisis gracias a herramientas que incorporan como el machine learning o la inteligencia artificial”, interpretan desde IFS.

Por su parte, la inteligencia artificial está cambiando la manera de gestionar las empresas. Hablamos de una tecnología disruptiva que ha venido para quedarse e incluso hacernos la vida más fácil. La IA puede automatizar tareas rutinarias y repetitivas que normalmente requieren tiempo



y esfuerzo humano y ayuda a liberar tiempo para que los empleados se centren en actividades más estratégicas y creativas.

En cuanto a las soluciones de gestión empresarial, Gonzalo Valle dice que esta tecnología tiene el potencial de revolucionar la forma en que las organizaciones operan, mejorando la eficiencia, reduciendo costes y permitiendo una toma de decisiones más informada y estratégica, “sin embargo, también es importante abordar los desafíos éticos y de privacidad asociados con el uso de la IA y asegurarse de que se implemente de manera responsable y transparente”.

Mientras que, Carlos Esteve, director de Desarrollo de Negocio de Grupo Aitana, hace hincapié en sus capacidades de automatización y del análisis de datos, “gracias a la Inteligencia Artificial, por ejemplo, se pueden predecir, con un alto grado de precisión, los resultados de ventas e ingresos para el siguiente trimestre; y se pueden elaborar pronósticos de demanda y consumo”.

Para Pablo Serna lo esencial es reconocer la IA como una herramienta de apoyo para el equipo humano y el desarrollo del trabajo, por lo que no debe verse como una amenaza, “debemos entenderla como un complemento para permitir que las personas dediquen su tiempo a la aportación de valor al negocio; dejando las tareas repetitivas y de poco valor a las herramientas tecnológicas. En Cegid, todas nuestras soluciones aplican la IA de una manera u otra. Un buen ejemplo es el caso de los software GMAO (Gestión de Mantenimiento Asistido por Ordenador) en el sector industrial. Gracias a la IA podemos realizar un mantenimiento preventivo y predictivo de los activos implicados en cualquier fábrica, evitando un problema mayor en el futuro”.

### SEGURIDAD EN LA NUBE

La seguridad es un factor fundamental a la hora de escoger una solución u otra. Desde luego, más allá de la encriptación de datos y el monitoreo de la solución para el análisis de posibles amenazas que el proveedor de software debe hacer, será muy interesante saber si realizan auditorías periódicas (como por ejemplo la ISO 27001 para la ciberseguridad), o si cumplen con la normativa vigente de cada país en cuanto a la seguridad.

Según datos del ‘Balance de Ciberseguridad 2022’ del Instituto Nacional de Ciberseguridad de España (INCIBE), se han incrementado un 9% los incidentes de ciberseguridad respecto al año anterior. En concreto, más del 50% de ellos afectaron a empresas y ciudadanos, y los fraudes online, como el phishing y el malware, fueron los más fre-

cuentes. Por eso es tan importante la propuesta de seguridad de las soluciones y la formación de los empleados en las compañías.

De ahí que desde cecig, opten por “conocer si ofrecen fórmulas de recuperación de la información en caso de pérdida o, por ejemplo, si cuentan con doble autenticación a la hora de acceder a la aplicación, por mencionar algunas cuestiones esenciales”.

La seguridad es uno de los aspectos más importantes a la hora de elegir una solución cloud, y quizá, al que menos importancia se da. En Wolters Kluwer ven la seguridad como parte del ciclo de vida de la solución. “Esto quiere decir que se tiene en cuenta en todas las fases de la ideación, creación y entrega del producto. La seguridad en el código, la seguridad perimetral, la seguridad en la autenticación y la política de privacidad deben ser robustas y estar bien gestionadas. Todos estos aspectos de la seguridad tienen sus certificados oficiales correspondientes y deben estar a disposición del cliente. Elegir un fabricante que gestione correctamente la seguridad es fundamental”.

A la hora de elegir una solución de software, Zucchetti recomienda, “asegurarse de que la herramienta cumple con los requisitos de la normativa europea de protección de datos, ya que en un software ERP-CRM se van a almacenar datos de personas que debemos proteger. Por otra parte, es esencial que podamos tener el control en la creación de usuarios y permisos de acceso asignados a cada área del programa, de manera que se pueda prevenir y rastrear cualquier problema de seguridad. La nube aporta unas mayores ventajas que las soluciones on-premise, ya que los datos están cifrados y distribuidos en múltiples máquinas, y sus medidas de seguridad son altamente superiores a numerosas implementaciones on-premise, especialmente en las pymes”.

### TENDENCIAS ACTUALES

La evolución y el desarrollo de herramientas de gestión empresarial ha experimentado un impulso en los últimos años gracias a la aparición de tecnologías emergentes más eficientes y seguras.

Gonzalo Valle reitera que la adopción de estas tendencias es fundamental para seguir marcando la diferencia y, sobre todo, para seguir siendo competentes. Precisamente en esta área cobran especial importancia:

- La inteligencia artificial. Las empresas estamos aprovechando esta tecnología para optimizar procesos y favorecer la toma de decisiones. De hecho, según datos de IDC el 55% de las organizaciones europeas ya están explorando potenciales casos de uso de la IA generativa y un 21% tienen previsto invertir en este tipo de tecnología durante el año 2023



- El Internet de las cosas y Edge Computing, que permiten mejorar la eficiencia operativa y aumentar la seguridad
- La ciberseguridad, clave en la era actual del software empresarial
- El Low Code y No Code, esto permite a los usuarios desarrollar aplicaciones sin necesidad de tener grandes conocimientos en programación, lo que facilita la toma rápida de soluciones

En palabras de Pablo Serna, cada vez más, también se prefieren aquellas soluciones que cuenten con herramientas que permitan la integración con otros software, ya sean propios o de proveedores y clientes, para nuevamente facilitar y agilizar la comunicación entre equipos y demás actores, “Otra tendencia al alza, sobre todo en empresas con una complejidad mayor, es la posibilidad de adquirir soluciones que, pese a ser estandarizadas, permitan módulos y personalizaciones para adaptarse al core business de cada empresa. En cuanto a la sostenibilidad ha emergido como una poderosa tendencia que está conmoviendo a prácticamente todos los sectores. Con la creciente conciencia sobre el impacto ambiental y social de las operaciones comerciales, las organizaciones buscan cada vez más incorporar prácticas sostenibles en sus procesos y estrategias”.



## Áurea Rodríguez, Autora de “Antes muerta que analógica”

Fecha de nacimiento: 7/2/1977

Hijos: dos

Hobbies: Escribir, mi playa

Estudios: Varios

### ¿Cómo llegaste al mundo de las TIC?

A la industria TIC llegué por mi profesión como gerente de un centro tecnológico en donde se aplican las tecnologías TIC de manera transversal a todos los sectores y más tarde como directora de innovación en la administración en donde era responsable de la puesta en marcha del programa de Industria 4.0 de apoyo a la pyme.

### En su opinión ¿qué es lo que falla para que las mujeres no apuesten más por el estudio de carreras STEM?

Las mujeres en carreras STEM (ciencia-tecnología-ingeniería y matemáticas) son solo el 28% y si le añadimos el componente empresa o cargos de responsabilidad, la cifra se desploma. Tenemos una cultura que estereotipa las personas y la percepción que tenemos de ciertas profesiones. Hay que educar, visibilizar, cambiar el lenguaje, empoderarlas, abrirles puertas y tener más referentes de todo tipo. La tecnología no tiene género por tanto la tecnoeconomía tampoco debería.

### ¿Cree que existe el “techo de cristal” en las empresas TIC?

#### ¿Cuál debería ser la solución?

El techo ya no es de cristal, ahora es de bits y pronto de qubits. Como todo en este siglo, el patriarcado se ha digitalizado y se manifiesta en forma de menor presencia en las redes (invisibilidad) pero sobre todo por el sesgo de los algoritmos controlados por inteligencias artificiales o la propia industria. Un sesgo por género en un algoritmo puede significar acceder o no a un trabajo o a un crédito así que, si no ponemos remedio,

tendremos una nueva fuente de discriminación.

### ¿Una política de cuotas puede resolver el problema?

No podemos arreglar un problema digital analógicamente ni uno cultural solo con cuotas. Existe un componente cultural desde que el mundo es mundo, de hecho, en el 2023 aún no existe ningún país de los 197 de la tierra que sea 100% igualitario. Mejoramos sí, pero seguimos con el sesgo por omisión así que de la misma manera que hemos llegado a la conclusión que hay que prohibir fumar o que debemos conseguir los objetivos de descarbonización del planeta, deberíamos tener la misma contundencia con la igualdad y más específicamente, tecnológica. Ahora esto se extiende al mundo digital, ya no solo en la poca representación de la mujer en las profesiones digitales sino en la subrepresentación en los algoritmos que dirigirán las decisiones del mundo y por tanto sesgos y brechas más acentuadas.

### ¿Qué dificultades se encontró usted para llegar a la posición que tiene actualmente?

En mi caso, al estar en un entorno empresarial empiezas a tomar conciencia que la presencia de la mujer en tecnología o industria debería ser normal pero no es lo común. Además, cuanto más tecnología, poder o riqueza, menos mujeres. Sean en traje o corbata en el caso de las grandes empresas o en tejanos y zapatillas en el caso de startups, las fotos de quien representa esta economía son ellos. Para mí, hoy en día la igualdad es digital y el feminismo es tecnológico y va de que con-

troleamos los algoritmos y en general la Inteligencia Artificial.

**¿Qué es lo que más valora de su empresa con respecto a la integración de la mujer?**

Es una empresa igualitaria con buenas políticas de teletrabajo y conciliación que siempre favorecen la integración.

**Un 35% de alumnos no logra ni acabar el bachillerato ni la FP equivalente, ¿está en la educación el problema de la falta de perfiles especializados?**

Hay una desintonía entre las necesidades de las empresas y los contenidos formativos actuales, pero también en los perfiles que ya están en las propias empresas porque las necesidades cambian más rápido. Además los conocimientos también los adquirimos con el autoaprendizaje en grandes plataformas, las nuevas universidades en red con puntos de prácticas y donde la información está en grandes repositorios mundiales.

**¿Le han servido los estudios que hizo para realizar su labor actual?**

Me han servido para aprender a aprender, que es una de las cosas más importantes que puede uno saber y siempre

mejora con la práctica. Los boomers y X éramos de ciencias o letras, pero eso es parte de la historia del siglo pasado. Ahora debemos adquirir conocimientos híbridos entre las ciencias y las humanidades – STEAM- y desde una perspectiva de la tecnología humanística y a la inversa del humanismo tecnológico.

**Solucione el problema de la educación en España.**

Los 193 Estados Miembros de la UNESCO han aprobado la primera recomendación mundial sobre ética de la inteligencia artificial y que aconseja a todos los países preparar sus sistemas educativos promover la adquisición de “competencias previas” para la educación en materia de IA, como la alfabetización básica, la aritmética elemental, las competencias digitales y de codificación y la alfabetización mediática e informacional, así como el pensamiento crítico, el trabajo en equipo, la comunicación, las aptitudes socioemocionales y las competencias en materia de ética. La mejor política de igualdad sería formar masivamente a todo el mundo en estas competencias, como sociedad no nos podemos permitir ningún analfabeto digital.

**Si tuviera que aconsejar a un**



**joven qué estudiar de cara a obtener un futuro laboral estable, ¿por dónde le orientaría?**

Le diría que haga aquello que le haga feliz como profesión y por el resto que procure aprender durante toda la vida y sobre la vida y sobre todo que piense que querer es poder.

**¿Hacia dónde cree que va el sector TIC? En su opinión, ¿cuáles van a ser las tendencias que realmente van a transformar la sociedad?**

Creo que el sector TIC va a crecer a través de sus casos de uso como la movilidad autónoma, la salud personalizada o el audiovisual por poner unos ejemplos, pero sobre todo se verá retado como el resto por las potencialidades de la inteligencia artificial, la cuántica y las regulaciones de la propia IA, las criptomonedas o la propia identidad digital. Confío en que la tendencia prevalente sea utilizar la tecnología para el bien de las personas en todos esos campos y no al revés.

## UN CIO EN 20 LÍNEAS



“Uno de los mayores retos es reducir la complejidad de nuestro ecosistema IT”

### **¿A qué están dedicando en la actualidad la parte principal del presupuesto de TI de Nationale-Nederlanden?**

El principal propósito es hacer lo necesario para que la Compañía esté preparada para el futuro con la premisa inamovible de ofrecer la mejor experiencia de cliente convirtiéndonos en referentes dentro del mercado de protección español. Así que, partiendo de esa base, la mayor parte de los recursos están dirigidos a transformar y evolucionar nuestro mapa de infraestructura, aplicaciones y servicios. Sin embargo, no es algo nuevo, sino que llevamos años inmersos en esa transformación digital recorriendo un mapa de proyectos que posicionan a Nationale - Nederlanden a la cabeza de la industria gracias a tres facilitadores: la tecnología, el dato y las personas. En primer lugar, uno de los mayores re-

tos tecnológicos es reducir la complejidad de nuestro ecosistema IT eliminando y sustituyendo componentes y aplicaciones por nuevas tecnologías; así como modernizar los sistemas legacy para romper su aislamiento y abrirlos al resto del ecosistema tecnológico. Algo que nos servirá para ofrecer el mejor servicio al cliente partiendo de procesos internos más eficientes, ágiles y flexibles a partir de, también, la incorporación de nuevas capacidades digitales.

En paralelo, siguiendo con los facilitadores estratégicos, el dato se posiciona como un elemento fundamental en el desarrollo de esa transformación de la que hablo. Por ejemplo, trabajamos en una nueva plataforma de datos que maximiza su valor al servicio de la eficiencia y las mejores decisiones en el momento necesario y que, sin duda, nos

convertirá en una verdadera compañía data-driven. Además, tenemos el objetivo de alcanzar una mayor resiliencia, elasticidad y escalabilidad aprovechando todo el potencial de las tecnologías en la nube.

Por último, aunque primordial para todo lo anterior, confiamos en las personas, en nuestros equipos. Por eso, creamos y fomentamos una cultura de ingeniería entre nuestra comunidad de IT, para potenciar la especialización y el desarrollo de nuevas skills, así como ser un empleador atractivo para la incorporación de nuevo talento.

### **Llevan tres años desarrollando un proceso de transformación digital importante, ¿en qué ha consistido?**

Es cierto es que este proyecto de transformación comenzó hace tres años con



la puesta en marcha de una nueva estrategia corporativa que persigue convertirnos en referentes en la prestación de esa experiencia de cliente de la que hablaba antes. Sin embargo, Nationale-Nederlanden siempre se ha distinguido por ser pionera y líder en innovación siendo una de las primeras aseguradoras tradicionales en conseguir grandes avances como la 100% venta digital o la incorporación de Agile como modelo de trabajo.

Dicho esto, en los últimos tiempos nos hemos esforzado en crear el espacio proclive a favorecer el desarrollo de skills necesarias para entender y poder adoptar un nuevo abanico de tecnologías y nuevos paradigmas de soluciones, integración y operación. Ha sido necesario atraer nuevo talento con nueva especialización y potenciar nuevas skills por parte de nuestra comunidad IT.

Un espacio que también tiene muy en cuenta el trabajo en equipo colaborando estrechamente con los departamentos de negocio de forma transversal para garantizar el alineamiento y que la estrategia de compañía está debidamente conectada con la estrategia tecnológica. Todo ello dedicando los esfuerzos oportunos a minimizar cualquier riesgo que pueda derivarse de los proyectos e iniciativas de transformación de renovación de plataformas, modernización de aplicaciones, etc. sin que afecten a la operativa diaria del negocio.

#### **¿Cuáles han sido los principales retos que se han encontrado durante todo el proceso?**

Como es lógico cuando estamos hablando de iniciativas que afectan directamente al negocio, uno de los principales retos es tener la capacidad de que los cambios se-

an ágiles y, por supuesto, no afecten a los planes previamente fijados. También destacaría la modernización del legacy que comentaba en la primera pregunta. Su integración con nuevas plataformas y soluciones es compleja y requiere una excelente puesta en escena tanto en recursos humanos, como materiales. En la misma línea, resulta complejo adoptar esas nuevas tecnologías, arquitecturas y paradigmas de desarrollo tecnológico que, en suma, requieren un esfuerzo extra en lo que se refiere a la captación y retención del talento.

#### **¿Qué ventajas y beneficios han obtenido?**

Siendo sinceros, la lista es extensa y no sólo referida a lo puramente tecnológico, sino a indicadores de negocio como las mejoras en SLAs y KPIs de experiencia y servicio a nuestros clientes. Además, y por destacar algunas más concretas, me quedaría con la eficiencia operativa que hemos conseguido en nuestros procesos ayudando a contener y/o reducir el coste de nuestras operaciones, la consecución de una mayor escalabilidad de nuestros sistemas buscando ser flexibles y ágiles ante aumentos de demanda en capacidad, el trabajo desarrollado para conseguir una mayor seguridad y resiliencia y la apertura a nuevos modelos de negocio y colaboración con partners y terceras partes.

#### **¿Qué pasos les queda por dar en ese proyecto? ¿En cuánto tiempo cree que estará acabado?**

El plan estratégico actual nació en 2021 con un horizonte a tres años, lo que significa que su previsión es completarlo en 2024. Tenemos buen ritmo, así que el objetivo sigue siendo cumplir con

David Vaquero,  
subdirector general y  
director de Tecnología  
en Nationale-  
Nederlanden

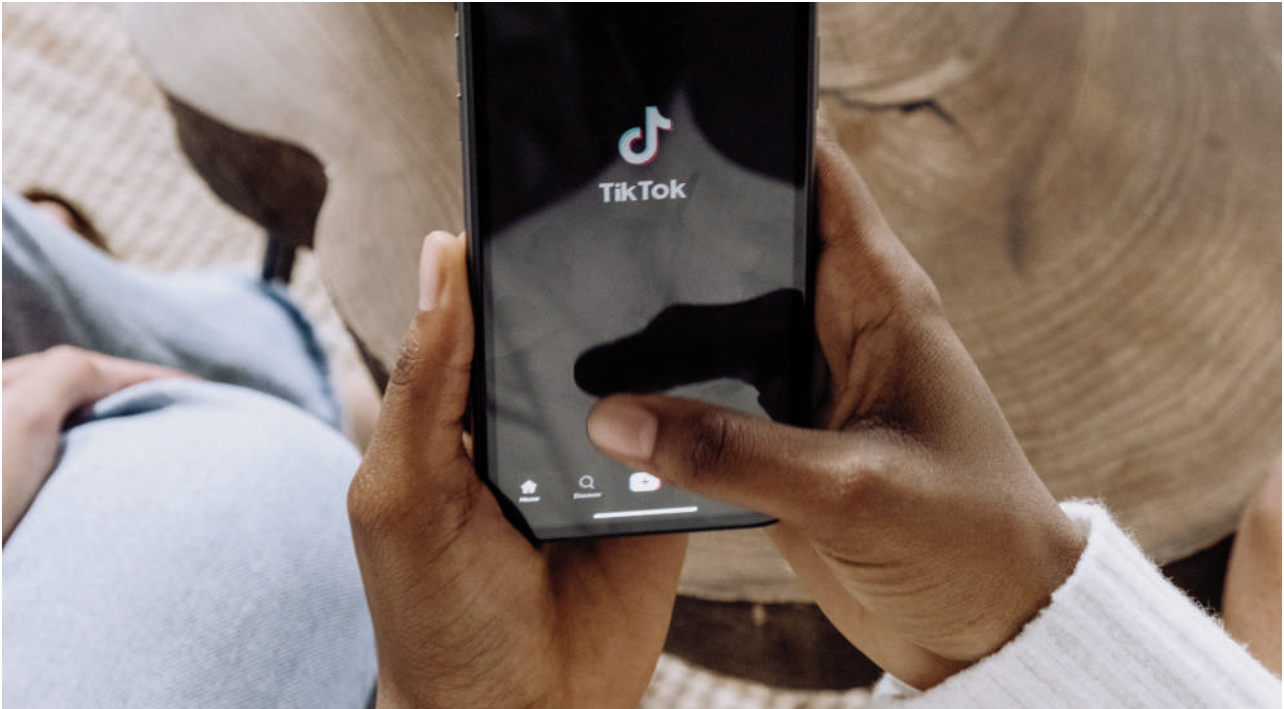
la estimación y completar el proyecto de renovación y modernización de las plataformas de experiencia con clientes en tiempo. Algo que nos permite incorporar esas nuevas capacidades de las que venimos hablando y que nos harán ser un referente en el mercado a partir de mejores experiencias y servicios aplicados a todos nuestros canales de distribución o medio de preferencia.

#### **Una vez concluido el proyecto, ¿cuál es el siguiente proyecto que tiene en mente y en qué va a consistir?**

Podríamos decir que el proyecto no concluye, sino que continua en una nueva fase natural que, como decía, ya hemos arrancado y en la que hemos asentado las bases. En el futuro inmediato, uno de los protagonistas seguirá siendo el dato y, con su ayuda, exploraremos las posibilidades de emplearlo en todos aquellos procesos clave facilitando la gestión óptima del negocio.

Mediante técnicas de inteligencia artificial y analítica avanzada del dato, podemos anticiparnos a las necesidades de nuestros clientes, ofrecerles los mejores productos y servicios, ser más eficientes en los momentos de la verdad (en la gestión de un siniestro y a estudiar cómo evitarlo, prevención del fraude, etc.) pero, también, de forma continuada ofreciendo una respuesta y servicio adaptado en todo el ciclo vital del cliente de modo que podamos actuar rápido y de forma ajustada ante cambios en las necesidades de nuestros clientes construyendo, con ello, relaciones de calidad a largo plazo.

# Uso de las redes sociales en el entorno laboral



**E**l tema de la protección de la privacidad en el ámbito laboral no es nuevo. En efecto, siempre ha sido una cuestión polémica la naturaleza de los medios tecnológicos que se entregan por la empresa a los trabajadores para realizar su trabajo, en especial, en lo referente a la posibilidad de acceso del empleador a los mails de las cuentas de correo corporativas en determinadas circunstancias, lo que aconseja contar con políticas de uso adecuadas que definan estos supuestos.

Y es que la normalización del uso de la tecnología muchas veces genera situaciones conflictivas por la vulneración de derechos personalísimos protegidos por el artículo 18 de la Constitución Española y la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que tienen su im-

pacto específico en el contexto laboral, tanto para los trabajadores como para los empleadores; en particular por el uso de redes sociales (Twitter, YouTube, TikTok, LinkedIn, Instagram, etc.) y otras tecnologías como los sistemas de mensajería (WhatsApp, Line) y las apps. Por ello, los Tribunales han ido marcando unas pautas jurisprudenciales aplicables tanto con carácter general como, específicamente, en el entorno virtual.

De esta forma, respecto a la protección del derecho al honor de la empresa (reconocido por la jurisprudencia para las personas jurídicas), la sentencia 368/2023, de 24 de enero de 2023, del Tribunal Superior de Justicia de Cataluña (Sala de lo Social) ha establecido que en una situación de huelga, prevalece la libertad de expresión de los trabajadores sobre el derecho al honor de empresario, de forma que comentarios que aisladamente podrían ser con-

sideradas denigrantes, en un contexto de conflicto laboral disminuye su carácter ofensivo, al tiempo que aumenta el grado de tolerancia exigible, máxime si la trabajadora es miembro del comité de empresa y afiliada a un sindicato, como ocurría en el caso enjuiciado, por lo que se declaró la improcedencia del despido.

En la misma línea, sobre la libertad de expresión de los trabajadores en su ámbito privado al margen de su actividad laboral, se pronunció la sentencia 307/2021, de 29 de abril de 2021, del Tribunal Superior de Justicia de Madrid (Sala de lo Social), en relación con la nulidad del despido de un trabajador de COPE, motivado por un comentario en Twitter, en respuesta a la comunicación de la denuncia presentada contra Netflix por la Asociación Española de Abogados Cristianos, por una película en la que se hacía ver a Jesucristo como homosexual. De esta forma, dado que el tuit se realizó desde la cuenta personal del trabajador, se consideró como una opinión propia que no afecta a la imagen de la empresa.

Sin embargo, sí se declaró procedente el despido la sentencia 382/2022, de 20 de abril de 2022, del Tribunal Superior de Justicia de Madrid (Sala de lo Social) en el supuesto del trabajador que puso en su estado de WhatsApp fotografías, videos y memes con la cara de la Directora de Recursos Humanos (ex mujer del dueño de la empresa) y otro Directivo (hijo de ambos), relacionándolos con la indigencia, el alcoholismo y la toxicomanía; considerándolo vulnerador de su derecho al honor, por provocar un evidente desprestigio personal y profesional, ya que el trabajador, como responsable de mantenimiento de las peluquerías de una franquicia, tenía contacto desde su móvil personal con los directores de zona, responsables de otros centros, proveedores y clientes.

Asimismo, la sentencia 2044/2022, de 18 de octubre de 2022, del Tribunal Superior de Justicia de Asturias (Sala de lo Social) confirmó la procedencia del despido de un trabajador que subió a TikTok vídeos en los que aparece vestido con su uniforme de trabajo y llamando “hijos de puta” a los clientes de su empresa, considerándolo una extralimitación de la libertad de expresión en la que no hay crítica ni opinión, sino meros insultos proferidos de forma reiterada y gratuita, lo que supone una vulneración del derecho al honor de los clientes. Y ello, implica un perjuicio para los intereses de la empresa, que se ve obligada a responder de alguna manera a tales he-

chos, por lo que está facultada para adoptar medidas al respecto.

Por lo que se refiere al derecho a la intimidad de los trabajadores, la sentencia de 14 de mayo de 2021 del Juzgado de lo Social nº. 3 Talavera de la Reina abordó el tema, entonces de candente actualidad al encontrarnos en plena pandemia, sobre si se produce una trasgresión de la privacidad del trabajador por el hecho de que en sus nóminas constase que la causa de su baja era el covid-19. Pues bien, se consideró que no se había vulnerado el derecho a la intimidad del trabajador, debido al carácter privado y personal de las nóminas, y a que su obtención se realiza mediante la descarga en una plataforma con sus propias claves de acceso; además de que las nóminas se confeccionaron según el tipo de partes de baja específico (191-COVID 19) siguiendo las instrucciones dadas por el INSS.

Por su parte, la sentencia 5288/2022, de 23 de noviembre de 2022, del Tribunal Superior de Justicia de Galicia (Sala de lo Social) se pronunció sobre los grupos de WhatsApp creados por la empresa en los que se incluyen a los trabajadores para la organización y coordinación de tareas y, en concreto, sobre si el hecho de escribir mensajes en los mismos fuera del horario laboral puede vulnerar el derecho a la desconexión digital de los trabajadores como parte de su espacio privado al margen de su actividad laboral. La Sala concluye que esta vulneración no tiene por qué producirse necesariamente por el mero hecho de recibir mensajes, siempre que su falta de lectura o contestación no conlleve aparejadas sanciones o amonestaciones.

Asimismo, la sentencia 458/2022, de 31 de enero de 2022, del Tribunal Superior de Justicia de Galicia (Sala de lo Social) ha resuelto sobre la obligación de los trabajadores de instalar en su móvil personal una app de la empresa para obtener los códigos de verificación necesarios para conectarse a los dispositivos informáticos proporcionados por la empresa para realizar su trabajo, so pena de volver al trabajo presencial; estableciendo que constituye una modificación sustancial de las condiciones de trabajo no justificada, ya que, de igual forma que entregó el equipamiento necesario para teletrabajar desde sus domicilios particulares, también podía haber proporcionado los teléfonos móviles de empresa.

Javier López  
socio de Écija Abogados



# El sector sanitario ante el aumento de ciberataques

**E**l sector sanitario es un objetivo cada vez más atractivo para los ciberdelincuentes. Y es algo que hemos visto en las últimas semanas. Según un informe de CrowdStrike, el sector salud se encuentra entre los cinco más atacados y, además, es uno en los que más han crecido los ataques: en 2022, el número de ataques sufrido por organizaciones relacionadas con la salud y la sanidad fue el doble que en 2021. Y el tipo de ataque más utilizado, según el mismo informe, fue ransomware.

Los modelos de ransomware como servicio han favorecido el incremento de los ataques, ya que los criminales ni siquiera necesitan tener conocimientos técnicos para llevar a cabo sus actividades maliciosas: simplemente pueden buscar a un proveedor de ransomware en la dark web y contratar sus servicios. En este nuevo modelo, los desarrolladores de ransomware suelen recibir un porcentaje de la extorsión y, si tenemos en cuenta que un conjunto de datos puede estimarse en unos mil euros, el negocio es suficientemente lucrativo. El alto valor de estos conjuntos de datos se debe a que en el entorno médico se utiliza mucha información confidencial que puede ser luego reutilizada para robar identidades, llevar a cabo fraudes médicos o fraudes en el pago de impuestos, ya que suelen incluir la fecha y el lugar de nacimiento de la víctima, su número de Seguridad Social, la dirección y, en ocasiones, incluso los detalles de la tarjeta de crédito. Para acceder a las infraestructuras de entornos del sector sanitario, los ciberdelincuentes suelen explotar vulnerabilidades o credenciales, pero también compran el acceso a las redes a otros criminales. Este tipo de servicios de intermediación creció un 112% en 2022, según los datos que maneja CrowdStrike, que encontró más de 2.500 anuncios de venta de credenciales. Una vez que acceden a la red corporativa, los crimi-

nales, de media, son capaces de moverse lateralmente en tan solo 1 hora y 24 minutos. Y, en el caso del sector salud, los delincuentes saben que existen recursos muy limitados por parte de los equipos de seguridad, por lo que el acceso suele ser muy eficaz y rápido y, además, como vemos, reportar beneficios muy jugosos. Por eso, es fundamental que las organizaciones sanitarias comprendan que necesitan mejorar sus estrategias de seguridad e inviertan en la protección de sus infraestructuras.

### PASOS A SEGUIR

Teniendo en cuenta tan solo cinco puntos esenciales, más de la mitad del camino estaría recorrido:

- Proteger completamente las cargas de trabajo. Los aspectos más críticos en cualquier organización son el endpoint, las cargas de trabajo, las identidades, los datos y el almacenamiento. Con una solución de detección y respuesta extendida se facilita la recogida de datos para su análisis relacional; además, permite la visibilidad completa y promueve respuestas unificadas incluso frente a las amenazas más sofisticadas y ocultas.
- Apostar por la confianza nula. Según informes de CrowdStrike, alrededor del 80 % de los criminales utiliza ahora mismo ataques basados en identidades para comprometer credenciales legítimas y moverse libremente por la red evadiendo la detección con sistemas tradicionales de seguridad. Por eso, un enfoque zero trust, o de confianza nula, puede prevenir los ataques basados en identidades en tiempo real.
- Promover la protección proactiva. Los datos existentes sobre amenazas pueden ayudar al sector sanitario a defenderse contra la mayoría de atacantes y facilitan la protección proactiva a partir del análisis de comportamientos en las intrusiones más usuales. Con un equipo externo



de seguridad, se puede mejorar también el rendimiento gracias a los servicios de respuesta ante incidentes, recuperación del endpoint y análisis proactivo de la red.

- Confiar en tecnologías innovadoras. Los ciberdelincuentes no dejan de invertir en mejorar sus técnicas de ataque, por lo que la protección de las infraestructuras sanitarias debe estar también en constante evolución. Un ataque de hoy no puede mitigarse con una tecnología de ayer: los antivirus que se basan en firmas, por ejemplo, dejaron de ser eficientes hace ya mucho tiempo. Las tecnologías basadas en Inteligencia Artificial y Machine Learning, sin embargo, son capaces de determinar si una acción es maliciosa gracias al análisis del comportamiento o a otras características fácilmente observables.

- Realizar pruebas para responder de forma efectiva en caso de emergencia. Si la organización sanitaria tiene las mejores infraestructuras de protección, mitigación y recuperación, pero no sabe ponerlas en marcha, la estrategia es, evidentemente, inútil. Por eso, realizar simulacros para ayudar a todo el personal a identificar una amenaza y conocer los protocolos de información son esenciales.

**Por Drex DeFord, responsable de soluciones para el sector sanitario en CrowdStrike**



# El Datamesh, la herramienta clave en la lucha contra el cambio climático

**E**n un mundo cada vez más impulsado por datos, las tecnologías innovadoras están revolucionando la forma de alcanzar nuestros objetivos de sostenibilidad.

Una de ellas es Datamesh, un sistema innovador que puede influir significativamente en los esfuerzos de la lucha contra el cambio climático. Al integrar fuentes de datos dispares y permitir una toma de decisiones basada en el conocimiento adquirido a través de estos, Datamesh es la clave para optimizar la asignación de recursos, reducir los residuos y promover la gestión medioambiental.

En esencia, Datamesh es una plataforma global de integración de datos que conecta diversos conjuntos de datos relacionados con el consumo de energía, las cadenas de suministro, los modelos meteorológicos y la gestión de residuos, entre otros.

Al agrupar esta información, las organizaciones y comunidades obtienen una visión holística de su huella ecológica, lo que les permite identificar ineficiencias y tomar decisiones basadas en datos para impulsar la sostenibilidad.

### EL DATAMESH

La capacidad de conexión del Datamesh con distintas fuentes de datos mejora las estrategias de asignación de recursos. Así, mediante el análisis de los patrones de consumo de energía, las organizaciones pueden identificar las áreas de mayor uso y aplicar medidas de ahorro energético. Con acceso a los datos de la cadena de suministro en tiempo real, las empresas pueden agilizar sus operaciones, reduciendo las emisiones de carbono y los residuos.

Además, Datamesh permite realizar análisis

predictivos basados en modelos meteorológicos, lo que ayuda a las organizaciones a optimizar el uso del agua y mitigar los riesgos relacionados con el clima. Al mejorar la asignación de recursos, Datamesh permite a las organizaciones minimizar su huella ecológica y, al mismo tiempo, mejorar la eficiencia operativa y la rentabilidad.

Datamesh va más allá de la integración de datos; actúa como catalizador para la colaboración y la innovación. Al crear una plataforma común para el intercambio de datos, organizaciones, gobiernos e investigadores pueden abordar conjuntamente los desafíos que plantea la sostenibilidad.

Este enfoque colaborativo fomenta el intercambio de buenas prácticas, lo que permite a las partes interesadas aprender de los éxitos y fracasos de los demás. El entorno de datos abiertos facilitado por Datamesh fomenta el desarrollo de soluciones innovadoras, haciendo avanzar aún más las prácticas sostenibles y acelerando el progreso hacia los objetivos medioambientales.

En definitiva, a medida que la sostenibilidad se hace cada vez más imperativa, tecnologías como Datamesh ofrecen un inmenso potencial para impulsar un verdadero impacto positivo.

Al integrar diversas fuentes de datos, optimizar la asignación de recursos y fomentar la colaboración, Datamesh allana el camino para una toma de decisiones más documentada y un impacto medioambiental tangible. Adoptar Datamesh es un paso fundamental hacia la creación de un futuro sostenible que aproveche el poder de la integración de datos para la gestión ecológica.

Por José Carlos Iglesias, CTO, Insights&Data Capgemini España







# IA generativa: lo que todo CISO debe saber

Las nuevas tecnologías siempre cambian el panorama de la seguridad, pero es probable que pocas tengan el poder transformador de la IA generativa. A medida que plataformas como ChatGPT siguen ganando terreno, los CISO deben comprender los riesgos de ciberseguridad sin precedentes que conllevan y qué hacer al respecto. La parte "disruptiva" de las innovaciones disruptivas suele venir de las consecuencias inesperadas que traen consigo. La imprenta facilitó la copia de textos, pero al hacerlo modificó el tejido social, político, económico y religioso de Europa. Al revolucionar la movilidad humana, el automóvil reconfiguró el diseño de las comunidades, dando lugar a los suburbios y a la cultura del automóvil del siglo XX. Más recientemente, la World Wide Web ha transformado por completo la forma en que las personas se conectan entre sí y acceden a la información, replanteando cuestiones como la privacidad, las fronteras geopolíticas y la libertad de expresión. La IA generativa parece estar a punto de ser tan transformadora como todas ellas, con grandes modelos lingüísticos como ChatGPT y Google Bard y generadores de imágenes como DALL-E que han captado un enorme interés en tan sólo unos meses. Dada la rápida adopción de estas herramientas, los CISO necesitan comprender urgentemente los riesgos de ciberseguridad asociados, y cómo estos riesgos son radicalmente diferentes de los anteriores.

## ADOPCIÓN DESENFRENADA

Decir que las empresas están entusiasmadas con las posibilidades de la IA generativa es quedarse muy corto. Según un estudio, solo seis meses después del lanzamiento público de ChatGPT, el 49% de las empresas afirmaron que ya la utilizaban, el 30% que tenían previsto utilizarla y el 93% de los primeros en adoptarla tenían intención de utilizarla más.

¿Para qué sirve? Para todo, desde redactar documentos y generar código informático hasta llevar a cabo interacciones de atención al cliente. Y eso es solo el principio de lo que está por venir. Sus defensores afirman

que la IA ayudará a resolver problemas complejos como el cambio climático y a mejorar la salud humana, por ejemplo, acelerando los flujos de trabajo en radiología y haciendo más precisos los resultados de radiografías, tomografías computerizadas (CT scan) y resonancias magnéticas (MRI), al tiempo que mejora los resultados con menos falsos positivos. Sin embargo, toda nueva tecnología conlleva riesgos, como nuevas vulnerabilidades y modalidades de ataque. En medio de todo el ruido y la confusión que rodean a la IA hoy en día, esos riesgos aún no se comprenden bien.

## ¿CON QUIÉN ESTÁS HABLANDO?

El matemático e informático británico Alan Turing concibió en la década de 1950 una prueba para comprobar si un ordenador suficientemente avanzado podía ser tomado por humano en una conversación en lenguaje natural. El sistema IA LaMDA de Google superó esa prueba en 2022, lo que pone de manifiesto uno de los principales problemas de seguridad de la IA generativa, es decir, su capacidad para imitar la comunicación humana.

Esa capacidad la convierte en una poderosa herramienta para los esquemas de phishing, que hasta ahora se basaban en mensajes falsos a menudo plagados de faltas de ortografía. En cambio, los textos y correos electrónicos de phishing creados por IA están pulidos y libres de errores, e incluso pueden emular a un remitente conocido, como el CEO de una empresa dando instrucciones a su equipo. Las tecnologías de Deep fake avanzadas llevarán esto un paso más allá con su capacidad para imitar las caras y voces de las personas y crear "escenas" completas que nunca sucedieron.

La IA generativa puede hacer esto no solo de forma individual, sino también a escala, interactuando con muchos usuarios diferentes simultáneamente para lograr

## ¿A QUIÉN PERTENECE SU INFORMACIÓN?

Muchas empresas se han subido al carro de los chatbot de IA sin tener plenamente en cuenta las implicaciones para sus datos corporativos, especialmente si



hablamos de la información sensible, los secretos de la competencia o los registros regulados por la legislación sobre privacidad. De hecho, actualmente no existen protecciones claras para la información confidencial que se introduce en las plataformas públicas de IA, ya se trate de datos personales de salud proporcionados para programar una cita médica o de información corporativa privada que se ejecuta a través de un chatbot para generar un folleto de marketing.

Las aportaciones a un chatbot de IA público pasan a formar parte de la experiencia de la plataforma y podrían utilizarse en futuros cursos de formación. Incluso si esa formación está moderada por humanos y protegida por la privacidad, las conversaciones aún tienen potencial para "vivir" más allá del intercambio inicial, lo que significa que las empresas no tienen el control total de sus datos una vez que se han compartido.

### RIESGOS DE SEGURIDAD

Muchas empresas de seguridad planean utilizar la IA para combatirla, desarrollando software para reconocer estafas de phishing generadas por IA, deep fakes y otra información falsa. Este tipo de herramientas será cada vez más importante en el futuro.

Aun así, las empresas deben aportar su propia vigilancia, sobre todo porque la IA generativa puede erosionar los silos de información tradicionales que mantienen la información protegida de forma pasiva. Mientras que la nube ha proporcionado a las empresas una especie de simulacro para hacer frente a las responsabilidades de los datos distribuidos y los sistemas abiertos, la IA generativa introduce nuevos niveles de complejidad que deben abordarse con una combinación de herramientas tecnológicas y políticas informadas. Uno de los pasos más importantes que puede dar una empresa para protegerse es evitar pensar que, como no posee ni autoriza el uso de herramientas de IA, no está en peligro ya que empleados, partners y clientes pueden estar utilizando plataformas públicas de IA.

**Por Greg Young,**  
vicepresidente de ciberseguridad de Trend Micro



CÉSAR CID DE RIVERA, VP INTERNATIONAL SALES ENGINEERING DE COMMVAULT



“Commvault ha conseguido cerrar la brecha  
entre TI y seguridad”

Hablamos con César Cid de Rivera sobre las necesidades de las empresas en protección de datos y las nuevas soluciones de seguridad que completan la de Commvault.

Por Manuel Navarro

## **¿Cómo está evolucionando la protección de los datos en las empresas?**

Hace unos días leía en un informe que el 89% de las compañías ya son multicloud. Esto quiere decir que han seleccionado distintas nubes para albergar incluso el 50% de los datos críticos, y que además han elegido hacerlo en nubes de distintos proveedores. Esto es lógico, puesto que la nube ofrece muchísimos beneficios, pero también implica más riesgos, más superficie de ataque y más necesidades de protección en materia de seguridad.

Por otra parte, los ciberataques crecen de forma exponencial. Lo que antes eran días, semanas y meses en encontrar una vulnerabilidad y atacar nuestros entornos, ahora resulta que son 84 minutos lo que los cibercriminales tardan en sobrepasar las barreras. Así que, el estrés que tiene el CISO cada vez es mayor porque el tiempo de respuesta que tienen que dar cada vez es menor. De ahí que necesitamos también tener diferentes integraciones entre todos los fabricantes para poder responder de una forma unificada a estos ataques que están creciendo de forma exponencial, especialmente cuando se trata de ransomware.

### **Parece que el ransomware es la principal amenaza, ¿es así?**

El problema que tiene el ransomware en la actualidad es que antiguamente los cibercriminales explotaban la vulnerabilidad, empezaban a hacer movimientos laterales, a encontrar credenciales, elevar privilegios, luego filtraban la información, cifraban y empezaban a extorsionar. Ahora sigue ocurriendo esto. Sin embargo, ya no se hace por notoriedad, sino por motivos económicos. Ya hay ransomware as a service. Ahora resulta que también se ataca a las empresas con publicar los datos de sus clientes, de sus visitantes, de tarjetas de crédito, información confidencial, y esto ya es triple extorsión. Con lo cual, es un negocio, está en total auge y el problema es que ya no solamente buscan esa información confidencial para exfiltrarla y cifrarla, sino que además atacan directamente también al mundo del backup.

### **En Commvault habéis lanzado nuevas capacidades de seguridad integradas en vuestra plataforma, ¿en qué consisten?**

Como los ataques van no sólo al entorno de producción sino también al de backup, hay que proteger las aplicaciones más críticas y tener unos niveles de servicio distintos a los del resto de aplicaciones y rodearlas de toda esa capa de infraestructura de seguridad para, en caso de que detectemos anomalías, poder proteger los datos lo antes posible. Lo que hemos lanzado son productos para ayudar a nuestros clientes en este ámbito.

Por supuesto que la última línea de defensa sigue siendo la re-

cuperación, para que, en el caso de que se rompan todas las barreras y los cibercriminales accedan a los datos, las empresas puedan recuperarse en el mínimo tiempo posible. Por eso lanzamos Auto Recovery, que aúna backup, replicación, niveles de servicio, etcétera, en un único sistema, con independencia del hardware, con independencia del software, y que permite a las organizaciones recuperar cargas de trabajo a escala de forma fácil y segura frente a ciberataques, con una pérdida de datos y un tiempo de inactividad mínimos. Yo tengo una plataforma única de gestión y de recuperación de la información, incluso puedo validar que los backups que estoy haciendo son los correctos y van a ser recuperables.

Incluso puedo montar esos backups en un entorno sandbox, garantizar que no tienen ningún tipo de virus con Threat Scan, que es otro de los productos que lanzamos. Las empresas pueden utilizar Threat Scan para localizar y poner en cuarentena el malware y las amenazas del contenido del backup, y ayudar a garantizar recuperaciones limpias a la vez que se reduce la probabilidad de reinfección.

Además, incorporamos a nuestra plataforma ThreatWise Advisor, que integra tecnologías de cyber deception para engañar a los atacantes. Esta herramienta también ofrece una lógica integrada en los entornos de backup de Commvault para recomendar de forma inteligente la colocación de señuelos, y reforzar aún más las cargas de trabajo críticas.

También lanzamos Risk Analysis para determinar si nuestro entorno productivo tiene ficheros huérfanos, credenciales no autorizadas y diferentes puntos dentro de nuestra superficie de ataque que necesiten tener ciertos controles. Y todo ello gestionado en una única plataforma con una única interfaz de usuario, que ofrece gestión universal para todos los productos de Commvault en un panel integrado. Ofrece indicadores de estado, niveles de riesgo, seguridad y recuperación, y mucho más, desde una única fuente.

### **También han anunciado una serie de integraciones...**

Exacto. Creemos que las integraciones son fundamentales para abordar la materia de la seguridad en las empresas. En este caso, hemos anunciado integraciones con Microsoft Sentinel y Cyberark. Es tan sencillo como aunar la producción con el backup, proteger la información, ya no solamente desde un punto de vista de garantizar las recuperaciones, sino de garantizar que la información es segura, tanto en producción como en backup, bien defendida con tecnologías de cyber deception, con Risk Analysis, con Security IQ (que antes teníamos en Metallic y ahora también está en nuestra plataforma) y, por supuesto, también con Threat Scan para poder recuperar datos que, aunque hayan sido comprometidos, a la hora de recuperarlos estén limpios.

## Los umbrales de la década digital



José Joaquín  
Flechoso,  
presidente de  
Cibercotizante.

Volvemos de las vacaciones con las pilas cargadas, pero con importantes tareas por delante que debemos resolver. La incertidumbre política del verano, fruto de las elecciones del 23J, han añadido un punto de pimienta a uno de los veranos más extraños en tiempos de democracia. La inflación, la crisis energética y los derivados de la guerra de Ucrania, ofrecen un horizonte de incertidumbre como jamás habíamos vivido en este siglo.

Ante este panorama, se renueva el interés y la ambición de la Unión Europea en ser digitalmente soberana en un mundo abierto e interconectado, comprometiéndose a ejecutar políticas públicas en un futuro digital centrado en el ser humano.

La orientación humanística de la digitalización, junto con la fortaleza regulatoria europea, se constituyen como los grandes aspectos diferenciales de nuestro continente en relación a los gigantes USA y China. Urge dar coherencia a las políticas y proyectos transnacionales dentro de las fronteras europeas, sino también a posicionar a la UE como un actor relevante en el nuevo mapa geopolítico mundial. Europa en este Año Europeo de las Competencias, establece que para 2030, al menos el 80% de todos los adultos debería tener competencias digitales básicas y debería haber veinte millones de especialistas en TIC en la UE, fomentando la presencia de mujeres adoptando este tipo de trabajo, en una clara apuesta por las carreras STEM donde hay un notable déficit femenino.

También se fija para 2030, que tres de cada cuatro empresas deberían utilizar servicios de computación en nube, ma-

crodatos, e inteligencia artificial y más del 90% de las pymes deberían alcanzar al menos un nivel básico de intensidad digital, con una clara apuesta por el número de unicornios en la UE, donde se desea alcanzar el doble de los actuales. La Comisión establece para ese horizonte mítico del 2030, que todos los servicios públicos clave deberían estar disponibles on línea, como por ejemplo en lo relativo a tener acceso a su historia clínica electrónica y donde el 80% de los ciudadanos deberían utilizar una solución de identificación electrónica.

Bruselas prevé generar un mecanismo de seguimiento de la sensibilidad social, en forma de 'Eurobarómetro digital', poniendo en marcha un mecanismo que articule los proyectos plurinacionales, interconectando el tratamiento de datos, el diseño y despliegue de la próxima generación de microprocesadores, o las redes 5G y 6G. El desafío es hacer realidad en esta Década Digital de Europa, la homogeneización de indicadores entre los países miembros y la necesidad de una diplomacia tecnológica para el posicionamiento de la Unión Europea, que implicará también acuerdos con socios más allá de nuestras fronteras.

España, junto con otros países de nuestro entorno, ha conseguido que la Comisión Europea incorpore la protección de los derechos digitales como una de las prioridades para la próxima década, siendo nuestro país uno de los motores que impulse y acelere la consolidación de un Mercado Único Digital, como vía para generar competitividad, resiliencia y bienestar social. Somos los actores de un cambio irreversible y la UE no debe quedarse atrás.



# PREMIOS BYTE TI 2023

## VUELVEN LOS PREMIOS BYTE TI Y SUS FAMOSAS ESTATUILLAS

La asistencia (*obligada*) estará limitada según el aforo del espacio, así que regístrate cuanto antes para reservar tu plaza y compartir con nosotros esta velada tan especial.

FECHA: 28 SEPTIEMBRE 2023

HORA: 19:30H

DONDE: MUSEO DEL TRAJE (MADRID)



**RESERVA TU PLAZA EN**

<https://paginas.revistabyte.es/premios-byte-2023>  
o escaneando el código QR



Patrocinadores Gold

econocom

Hewlett Packard  
Enterprise

KYOCERA

Lenovo

CLOUDERA

SOPHOS

V-Valley

vmware

Patrocinadores Silver

HORNSECURITY

hp

VIEWNEXT  
AN IBM SUBSIDIARY

Wolters Kluwer

ZUCCHETTI

# a3factura

La solución de facturación online para pymes y autónomos



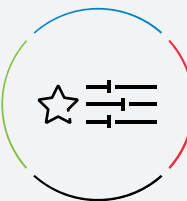
## Fácil de utilizar

**a3factura** es una solución muy fácil de utilizar que te permite hacer facturas y gestionar tu negocio de forma ágil y sencilla.



## Tu negocio bajo control

Sigue la evolución de tu negocio en tiempo real con una visión global de los principales indicadores.



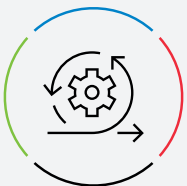
## Profesional y personalizable

Con múltiples plantillas para personalizar las facturas, presupuestos, albaranes y pedidos.



## Siempre disponible

Al ser una solución cloud, garantiza la seguridad de los datos y accesibilidad en cualquier momento y lugar.



## Gestión ágil

Crea las facturas y envíalas al momento desde **a3factura** y controla su recepción y descarga tanto en PDF como en formato electrónico.



## Trabaja con tu asesor

Con **a3factura** puedes compartir datos con tu asesor de forma automatizada. Olvídate de enviar papeles, evita errores y agiliza vuestra comunicación.