

Gestión de identidades: el nuevo perímetro de la ciberseguridad empresarial

Cómo establecer una estrategia de prevención de ciberriesgos

El nuevo manual del ransomware: extorsión con IA y auge de los ataques centrados en los datos

COMPARATIVA
Soluciones de gestión de identidades



SEGURIDAD DE SERIE. SIN INTERROGATORIOS

¿Aguantarían tus equipos de impresión un interrogatorio implacable? Las **impresoras Brother** cuentan con funciones como **seguridad de triple capa**, datos **encriptados** y documentos solo visibles para **usuarios autorizados**. Diseñadas para proteger la información y ofrecer siempre un **rendimiento óptimo. Incluso bajo presión.**

Descubre el caso completo

brother
at your side

4	Carta del Director
6	Actualidad
32	Webinars y encuentros BYTE TI
39	Comparativa 4 soluciones de gestión de identidades
47	Gestión de identidades: el nuevo perímetro de la ciberseguridad empresarial
54	Mujeres TIC Sandra Gibert
58	Un CIO en 20 líneas Alberto Baselga
61	Legalidad TIC
63	Aplicación práctica
65	Tendencias
70	Entrevista Paolo Boni
73	Cibercotizante



N. 341 | ÉPOCA IV
Edita:
Publicaciones Informáticas MKM
Septiembre 2025.

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

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

Redacción
Vanesa García (vgarcia@revistabyte.es)

Coordinador Técnico
Regina de Miguel

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

Fotógrafos
P. Varela, E. Fidalgo

Diseño de portada
María Torre

Diseño y maquetación
María Torre

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

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

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

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

Revista mensual de informática
ISSN: 1135-0407

Depósito legal: B-6875/95

© 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 autorizació expresa por escrito
del titular del Copyright. La cabecera de esta revista es
Copyright 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.

Carta del Director



Manuel Navarro Ruiz
Director de BYTE TI

Premios Byte TI 2025

El pasado 25 de septiembre celebramos el 25 Aniversario de los Premios Byte TI. La efemérides se vio recompensada por una asistencia de más de 500 personas del sector TIC que demuestran el compromiso de todo el equipo humano que forma parte Byte TI con clientes, partners y lectores.

En 25 años han sido premiados todo tipo de productos y soluciones, pero también un sinfín de personas. Las cinco categorías dedicadas a ellas (Personalidad del Año, Dirección de Marketing, Dirección de Comunicación y Mejor CIO y CISO) son las que a mi, personalmente, más me gusta destacar, pues se pone el foco en una persona concreta para valorar el trabajo que hace todo un equipo. Sin esa orquesta, el papel de quien la dirige sería insustancial.

Los Premios Byte TI son los primeros en inaugurar la temporada de galardones. A partir de entonces otros medios del sector tecnológico también otorgan sus propios reconocimientos. En nuestro caso, además de premiar lo que consideramos más relevante y a las personas que creemos más representativas del año, son una excusa para al sector TIC y pasar un rato agradable. Nuestro objetivo no es el de hacer discursos de dos horas para vanagloriarnos de lo bien que hacemos nuestro trabajo. Eso ya lo valora el creciente número de

asistentes que cada año asisten a la gala. Tampoco hacemos una entrega de premios que se alargue hasta el infinito.

Tras reconocer el trabajo que realizan personas y empresas del sector, nuestro siguiente objetivo es que quienes asistan se lo pasen bien y guarden un buen recuerdo de una fiesta. Como consideramos que lo más importante son las personas, nos centramos en ellas y en que pasen un momento lo más distendido posible. Esas dos son las prioridades de los Premios Byte TI: reconocimiento y relaciones de calidad.

Son muchas las ceremonias de entrega de premios que se van a celebrar a lo largo de este curso. Todos ellos merecen tanto la pena como los nuestros. Cada uno tiene sus directrices y sus normas para entregarlos. Todas ellas, fórmulas totalmente válidas. Ninguno de esos premios es mejor o peor que el otro. Simplemente reconocen la labor que hacen las empresas y las personas que posibilitan que esas organizaciones crezcan y desarrollen soluciones innovadoras para el beneficio de todos. Todos ellos indican la buena salud por la que atraviesa el sector TIC, algo por lo que deberíamos felicitarnos.





¿Tu organización está preparada? Cuando el ciberataque cuántico llegue, solo la criptografía postcuántica responderá

Los riesgos asociados a la computación cuántica aún no están aquí, pero llegarán antes de lo que imaginas.

En los próximos años, los ciberdelincuentes podrían conocer los algoritmos de cifrado y seguridad, y acceder a datos sensibles sin una protección robusta en tu organización. Cuando los ordenadores cuánticos maduren, podrán romper los estándares criptográficos actuales y dejar tu información al descubierto.

La criptografía postcuántica (PQC) está diseñada para resistir en este escenario

Minsait Cyber te acompaña para afrontar este desafío con tecnología PQC.

Facilitamos la **transición a arquitecturas criptográficas preparadas para responder con éxito al futuro cuántico.**

Protección de información sensible **a largo plazo**, incluso si se intercepta hoy y se descifra más adelante.

Ventaja competitiva: ciberseguridad avanzada y posicionada para liderar los retos de protección que están por venir.

Garantía de **cumplimiento**, marcado por regulaciones y organismos nacionales, europeos e internacionales.

Reducción del riesgo operativo y migraciones no planificadas.

La información protegida hoy, puede estar en riesgo mañana.

Anticipa la amenaza.
Mantén el control.
Prepara la respuesta.
¿Hablamos?

minsaitcyber.com
cyberinfo@minsait.com

Actualidad

Más del 90% de empresas no tiene preparados sus datos para la IA

Sin datos no hay Inteligencia Artificial. El que se supone que va a ser el motor de las compañías en los próximos años, es imposible que lo haga de forma correcta porque las empresas no tienen los datos para la IA suficientemente preparados. Al menos es lo que se desprende del estudio The Evolution of AI: The State of Enterprise AI and Data Architecture llevado a cabo por Cloudera.

El informe, que examina cómo se está adoptando la IA en todo tipo de empresas, qué arquitecturas de datos para la IA se están utilizando y cuáles son los retos que han surgido en 2025, se muestra que las empresas todavía están al inicio de sacar todo el potencial a esta tecnología disruptiva.

En comparación con el [informe del pasado](#) se destaca cómo han cambiado las prioridades, los retos y los objetivos en solo un año. En este sentido, un 24% de los encuestados afirma que su compañía tiene una cultura completamente data-driven, frente al 17% del 2024. Sin embargo, la accesibilidad de los datos para la IA sigue siendo un obstáculo: solo el 9% de las organizaciones afirma que todos sus datos para la IA están preparados y son accesibles, mientras que el 38% afirma que la mayoría sí lo están. Las mayores limitaciones técnicas identificadas incluyen la



integración de datos para la IA (37%), el rendimiento del almacenamiento (17%) y la potencia de computación (17%).

La IA integrada en los procesos

A nivel general, el 96% de los responsables de TI afirmaron que la IA está integrada, al menos en cierta medida, en sus procesos empresariales básicos. Esto supone un aumento con respecto a 2024, cuando la cifra fue del 88%. De hecho, el 70% de los encuestados afirmó haber logrado un éxito significativo con sus iniciativas basadas en datos para la IA, y solo el 1% aún no ha visto resultados.

Actualidad

Más del 90% de empresas no tiene preparados sus datos para la IA

El estudio también analiza qué [tipos de Inteligencia Artificial](#) se están utilizando, con la generativa en cabeza (60%), seguida del deep learning (53%) y la predictiva (50%). También se preguntó por la confianza en estos modelos, y el 67% de los responsables de TI se sienten más preparados que hace un año para gestionar nuevas formas de IA, especialmente aquellas que requieren gran volumen de datos para la IA.

“En solo un año, la IA ha pasado de ser una prioridad estratégica a convertirse en una necesidad urgente, redefiniendo las reglas de la competencia”, ha asegurado en un encuentro con la prensa especializada Juan Carlos Sánchez, vicepresidente regional de Cloudera. Sin embargo, el directivo destacó que “nuestro estudio revela que las empresas siguen enfrentándose a grandes retos en materia de seguridad, cumplimiento normativo y explotación de datos para la IA. Muchas de ellas se quedan estancadas en la fase de prueba de concepto». La misión de Cloudera es llevar la IA a los datos para la IA donde quiera que se encuentren (nube pública, privada o entornos locales), garantizando gobernanza, linaje y confianza en todo momento”.

Arquitectura de datos para la IA

Otras conclusiones del estudio incluyen que el enfoque híbrido en la arquitectura de datos para la IA se ha convertido en la norma, ofreciendo a las organizaciones la flexibilidad necesaria para gestionar cargas en entornos locales y en la nube. Entre sus principales ventajas, los encuestados mencionaron la seguridad (62%), la mejora de la gestión de datos para la IA (55%) y la optimización de la analítica (54%).

En cuanto al almacenamiento, el 63% afirmó hacerlo en la nube privada, el 52% en la nube pública y el 42% en un *data warehouse*, resaltando la necesidad de que los datos para la IA estén siempre disponibles y seguros.

La integración de la IA sigue preocupando en materia de seguridad: exactamente la mitad de los encuestados dijo que la fuga de datos para la IA durante el entrenamiento de modelos es una preocupación importante, el 48% mencionó el acceso no autorizado y el 43% el uso de herramientas de terceros no seguras.

A pesar de estas preocupaciones, las organizaciones muestran confianza: casi una cuarta parte (24%) dijo tener plena seguridad en la protección de sus datos para la IA, el 53% afirmó tener mucha confianza y el 19% expresó bastante confianza en la madurez de sus sistemas.



```
ttachEvent("onreadystatechange",H),
olean Number String Function Array
_={};function F(e){var t=_[e]={};re
[1])===!1&&e.stopOnFalse){r=!1;brea
o=u.length:r&&(s=t,c(r))}return thi
ction(){return u=[],this},disable:t
e:function(){return p.fireWith(this
nding",r={state:function(){return r
omise)?e.promise().done(n.resolve).
d(function(){n=s},t[1^e][2].disable
0,n=h.call(arguments),r=n.length,i=
r),l=Array(r);r>t;t++)n[t]&&b.isFun
><table></table><a href='/a'>a</a>
```

Actualidad

Dell impulsa la nube privada con IA, ciberresiliencia y automatización

La transformación digital ya no se detiene y, al mismo tiempo, las demandas sobre los equipos de TI se multiplican. Y es que, las compañías deben mantener vivas sus cargas de trabajo tradicionales y adoptar entornos modernos basados en contenedores, virtualización avanzada y despliegues híbridos. En este contexto, [Dell Technologies](#) ha dado un paso más con una nueva batería de soluciones que buscan reforzar tanto la ciberresiliencia como la automatización impulsada por inteligencia artificial.

Equilibrar lo tradicional y lo moderno

Uno de los grandes retos para es administrar simultáneamente cargas de trabajo heredadas y aplicaciones de nueva generación. Para responder a estas necesidades, Dell apuesta por nubes privadas desagregadas, con infraestructuras que combinan cómputo, almacenamiento y ciberresiliencia. Como parte de esa estrategia, la compañía ha integrado Dell Automation Platform con despliegues on-premises y SaaS. Esta capa permite [orquestrar entornos híbridos de manera flexible](#), mientras que la incorporación de Dell NativeEdge añade seguridad y simplicidad en operaciones distribuidas. Todo ello reforzado con Dell AIOps, que introduce inteligencia artificial en la gestión

de la infraestructura para acelerar la resolución de incidencias y mejorar la visibilidad de los sistemas.

La base de cualquier nube privada reside en el almacenamiento. Dell ha renovado su portfolio con mejoras en tres frentes principales: PowerStore, PowerFlex y PowerMax. Dell PowerStore introduce un nuevo modelo con tecnología QLC, automatización impulsada por IA e integración con Nutanix. Esto permitirá a los clientes una gestión más sencilla y escalable de sus datos, con opciones de alta capacidad y menores costes operativos. Además, la función Smart Support Auto-Heal promete reducir en un 90% los tiempos de resolución de incidencias.

Por su parte, Dell Power Max ofrece un 25% más de rendimiento y añade soporte para unidades QLC. También incorpora mejoras en seguridad, como inicio de sesión único con Microsoft Entra ID y alertas de correo electrónico cifradas. Para Thomas Cornely, vicepresidente sénior de Product Management en Nutanix, la alianza entre ambas compañías representa un punto de inflexión: "Con nuestra Nutanix Cloud Platform, estaremos ofreciendo a los clientes una nueva opción sobre cómo diseñar sus entornos virtualizados.

FERNANDO JOFRE



Frelancing: apuesta contra el edadismo laboral

Según el INE, la edad media de la población activa en 2026 será 50 años, en un escenario en el que el mercado de empleo por cuenta ajena está expulsando a los que rondan esta edad. En este contexto, la plataforma Malt acaba de publicar un informe que refleja una realidad que desmitifica muchos prejuicios sobre un colectivo senior afectado por el edadismo laboral. Las principales ventajas que aportan estos profesionales son su experiencia, compromiso, agilidad y rentabilidad, al proporcionar un alto valor sin generar costes fijos. El compromiso viene refrendado porque de ello dependerá su "marca" personal como senior. Precisamente la comunidad senior de Malt tienen un perfil principalmente tecnológico (un 33,6%), seguidos de un 27,3% dedicado a la comunicación y el marketing, y un 22,3% a la consultoría empresarial.

La elección de convertirse en freelance es sin duda una propuesta atractiva, como emprendedores, forzados al salir de su anterior empresa, o una vez jubilados. Y, es más, en el sector concreto de las TI, aportan una visión crítica e independiente muchas veces necesaria en organizaciones que necesitan de un revulsivo para avanzar en su transformación digital.

Actualidad

Digital Realty abre su laboratorio de innovación para acelerar los despliegues de IA y nube híbrida

La adopción de inteligencia artificial (IA) y la necesidad de arquitecturas híbridas están redefiniendo la manera en la que las empresas diseñan y prueban su infraestructura digital. En este contexto, Digital Realty ha anunciado la puesta en marcha de su Digital Realty Innovation Lab (DRIL), un laboratorio de innovación concebido para que compañías y partners validen proyectos de IA y cloud en un entorno real antes de escalar a producción.

El laboratorio se encuentra en el campus de [Digital Realty](#) en el norte de Virginia, uno de los polos tecnológicos más relevantes del mundo. A diferencia de entornos de simulación, el DRIL está ubicado dentro de un centro de datos activo, lo que permite a los clientes trabajar con cargas de trabajo reales y en condiciones operativas auténticas. El objetivo es sencillo: reducir la incertidumbre y los riesgos al implementar infraestructuras críticas para IA y computación de alto rendimiento (HPC).

Un cambio de paradigma

El DRIL está diseñado para que las empresas puedan replicar arquitecturas representativas, comprobar el rendimiento de nuevas aplicaciones y optimizar configuraciones sin poner en riesgo los sistemas productivos.

Además, facilita la conexión directa con proveedores de red y de servicios en la nube gracias a la plataforma ServiceFabric, que actúa como capa de interconexión global.

Entre las características más destacadas del laboratorio se incluyen racks de alta densidad capaces de soportar hasta 150kW, conectividad optimizada para [entornos híbridos](#) y herramientas de orquestación específicas para cargas de IA a través de Private AI Exchange (AIPx). También se pueden realizar pruebas de latencia entre ubicaciones, una funcionalidad clave para validar el rendimiento de arquitecturas distribuidas.

El DRIL es un punto de encuentro para un ecosistema de socios estratégicos. Empresas como AMD, Cisco, Lenovo, CommScope, Supermicro, Vcinity o Zenlayer participan activamente, aportando sus tecnologías para reforzar la propuesta. Desde AMD destacan el papel de la infraestructura para acelerar la adopción de la inteligencia artificial. "El DRIL muestra cómo los procesadores AMD EPYC y los aceleradores AMD Instinct proporcionan un rendimiento excepcional en IA y HPC en un entorno de producción de alta densidad", señaló Robert Hormuth, vicepresidente corporativo en AMD.

MANUEL LÓPEZ



Extinción vs Evolución

Vivimos tiempos de extremos. La polarización que domina el debate público ha encontrado en la IA un nuevo campo de batalla, dividiendo opiniones entre tecnófobos apocalípticos y evangelistas digitales. El mundo se ha dividido en dos bandos: los que la ven como una amenaza existencial y los que la abrazan como salvación tecnológica. El avance de la IA nos confronta con preguntas fundamentales sobre el sentido y el valor de la inteligencia humana en una era tecnológica. Para Ortega y Gasset, "la técnica es el esfuerzo por ahorrar esfuerzo", una herramienta al servicio de la realización profunda de nuestro ser y quizás esa sea la clave de la IA.

La inteligencia artificial no compite con nosotros; nos complementa. La inteligencia humana aporta intuición, creatividad contextual, razonamiento ético y comprensión emocional. La IA contribuye con velocidad de procesamiento, análisis de patrones complejos, memoria perfecta y capacidad de síntesis masiva. Separadas, ambas tienen limitaciones evidentes; unidas, crean un marco cognitivo sin precedentes. No estamos ante una sustitución, sino ante una extensión de nuestras capacidades intelectuales.

Dejemos de elegir bandos. En lugar de preguntar si la IA nos sustituirá, preguntémonos cómo podemos amplificar nuestro valor único a través de ella.



Todos los ganadores de los Premios Byte TI 2025

Con el marco espectacular que proporciona el madrileño Museo del Traje, se celebró la XXV edición de los Premios Byte TI 2025. Con la presencia de casi 500 personas ligadas al sector tecnológico, se premiaron productos, soluciones, proyectos y personas que recibieron las famosas «estatuillas». El acto contó con el patrocinio Gold de [HP](#), [HPE](#), [HCLSoftware](#), [Kyocera](#), [AWS](#), [Evolutio](#), [V-Valley](#), [Cloudera](#), [Econocom](#), [Data4](#), [Lexmark](#) y [Lifera](#). Asimismo, [NetApp](#), [itera](#) y [Wolters Kluwer](#) fueron patrocinadores Silver. Este es el resumen fotográfico de una noche tecnológica e inolvidable.



Actualidad



Premios Byte TI 2025



PREMIO A LA PERSONALIDAD DEL AÑO. Suzana Curic, country leader de AWS. Entregaron el premio, Nacho Sáez, director general de MKM Publicaciones y Manuel Navarro, directo de Byte TI



PREMIO AL MEJOR CIO. Juan Luis Cruz Bermúdez, director de transformación digital del Hospital 12 de Octubre de Madrid



PREMIO AL MEJOR CISO. Daniel Damas, CISO de Nationale-Nederlanden



PREMIO A LA MEJOR DIRECCIÓN DE MARKETING. Miguel Ángel de Ramón, director de marketing de Evolutio. Entregó el galardón Laura Sierra, account manager de Byte TI



PREMIO A LA MEJOR DIRECCIÓN DE COMUNICACIÓN. Paola Ortega, directora de comunicación de IBM.



HPE Y MINISTERIO DE SANIDAD. Premio a la mejor innovación tecnológica para garantizar un servicio permanente y seguro

Actualidad



Premios Byte TI 2025



HP Y BANCO SABADELL. Premio a la innovación y experiencia de usuario en el Digital Workplace. Recogieron el galardón David Casas, Director de Workplace de Banco Sabadell y Catalina Roa, Directora de marketing para España y Portugal de HP



HCLSOFTWARE Y MUTUA MADRILEÑA. Premio a la Excelencia en Innovación IT. Recogieron el premio Iván Izquierdo, Director de transformación IT de Mutua Madrileña y Santos Díez, Customer Experience Director de HCL Software.



KYOCERA Y CORREOS EXPRESS. Premio a la Automatización Inteligente con IA



AWS E IBERIA. Premio a la innovación y la transformación digital. Recogieron el premio Gabriel Perdiguero, Chief Financial Officer de Iberia, y Paz Vigil, Senior Enterprise Sales Manager de AWS para España



EVOLUTIO Y GISS. Premio al mejor proyecto de migración a nube pública



V-VALLEY Y GMV. Premio al mejor desarrollo de negocio en ciberseguridad. Recogieron el premio Nathalie Dahan García, BDM & Partner Strategy Manager de GMV y Alberto López, Country Manager de V-Valley Ciberseguridad.

Actualidad



Premios Byte TI 2025



CLOUDERA Y MASORANGE. Premio a la excelencia en calidad de servicio mediante la Gestión del Dato



DATA4 Y MEGAPORT. Premio al Mejor proveedor de Network as a Service. Recogieron el premio Lorenzo Ruggiero, Head of Southern Europe de Megaport y Fran Ramírez, Country Managing Director de Data4.



LIFERAY Y PRINCIPADO DE ASTURIAS. Premio a la excelencia en innovación en servicios públicos digitales. Entregó el premio Enrique Amado. Manager Sector Público de Liferay y lo recogió Javier Fernández Rodríguez. Dirección General de Estrategia Digital e Inteligencia Artificial del Principado de Asturias.



MEJOR EMPRESA TIC. Salesforce. Recogió el premio María Ángeles Santos, Vicepresidenta de Salesforce



MEJOR EMPRESA DE CIBERSEGURIDAD. Palo Alto Networks. Recogió el premio Luis Fuertes, director de marketing de Palo Alto Networks



MEJOR SOLUCIÓN DE IMPRESIÓN A3. Gama de dispositivos A3 de Lexmark. Entregó el premio, Fernando Jofre, colaborador de Byte TI y lo recogió Juan Leal, director general de Lexmark.

Actualidad



Premios Byte TI 2025



MEJOR SOLUCIÓN DE RECURSOS HUMANOS. WOLTERS KLUWER A3INNUVA NÓMINA. Recogió el premio Ana Belén Moreno, Payroll & HCM Product Manager en Wolters Kluwer y lo entregó Manuel López, colaborador de Byte TI.



MEJOR DESARROLLO DE CENTROS DE DATOS. SARENET. Recogió el premio Jon Arberas, director general de Sarenet y lo entregó Alejandra Méndez, responsable de CRM de Byte TI.



MEJOR SOLUCIÓN DE CIBERSEGURIDAD. PING IDENTITY. Recogió el premio Guillermo Arias, Strategic Account Executive Iberia de Ping Identity.



MEJOR PLATAFORMA DE AUTOMATIZACIÓN. APPIAN. Recogió el premio Julio Campoy, Regional Vice President de Broad Markets Iberia & Latam.



MEJOR HERRAMIENTA DE IA. MICROSOFT COPILOT. Recogió el premio Antonio Cruz, director de AI Business Solutions para Microsoft España.



MEJOR PLATAFORMA DE SERVICIOS EMPRESARIALES. SERVICENOW. Recogió el premio Luis Miguel Domínguez, Area VP de ServiceNow de manos de María Vicente, coordinadora de eventos y comunidad de Byte TI.

Actualidad



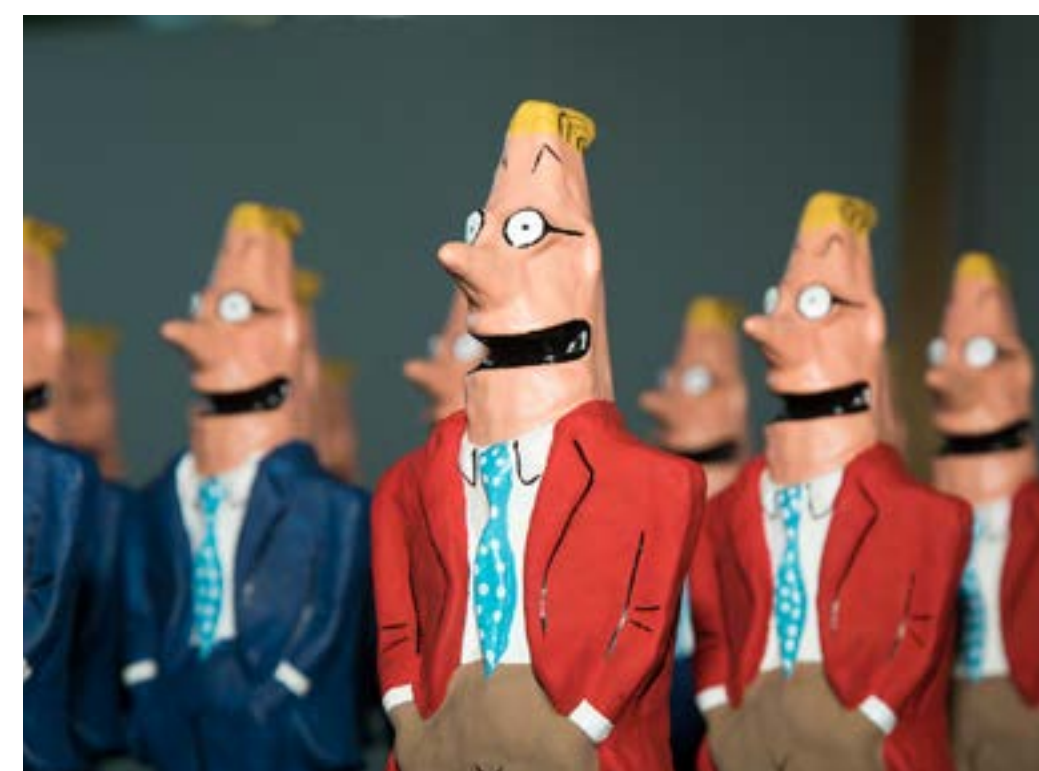
Premios Byte TI 2025



FINALISTAS Y GANADOR DEL PREMIO AL MEJOR CISO. Acompañan a Daniel Damas, Laura Baus, CISO de Vodafone España; Jesús Abascal, CISO de ENI; Gabriel Moliner, CISO de Carrefour y Lucero Ramos, CISO de Idealista.



FINALISTAS Y GANADOR DEL PREMIO AL MEJOR CIO. Acompañan a Juan Luis Cruz-Bermúdez, Virginia Vera, CIO de FritRavich; Beatriz de la Cruz, directora de IT de Verdecora y Javier Mallo, CIO de Carrefour



Actualidad – Te interesa

Revolución en los cielos: Iberia y AWS marcan un hito en la transformación digital de la aviación comercial

La migración completa a la nube y el aprovechamiento de las capacidades de AWS ha permitido a Iberia no solo mejorar su eficiencia operativa, sino también posicionarse como líder en la innovación del transporte aéreo.

La aerolínea española Iberia ha dado un paso histórico en su trayectoria centenaria al completar una de las transformaciones digitales más ambiciosas del sector aeronáutico europeo. La compañía, que opera una extensa red de vuelos que conecta Europa, América Latina, Norteamérica, Asia y África, ha elegido a Amazon Web Services (AWS) como su socio tecnológico preferente para acelerar su modernización digital.

La magnitud del cambio

En una decisión estratégica sin precedentes, Iberia ha desmantelado por completo sus centros de datos tradicionales para migrar toda su infraestructura a la nube de AWS. Los resultados de esta transformación son espectaculares: la aerolínea ha conseguido multiplicar por mil la velocidad de actualización de sus sistemas y reducir los tiempos de ciclo en un 40%.



Actualidad – Te interesa

Este proceso de modernización ha implicado la migración de toda la infraestructura tecnológica de la compañía a AWS, incluyendo la implementación de servicios cloud avanzados como Amazon ECS, AWS Fargate, Amazon EventBridge, Amazon DynamoDB y Amazon Aurora Serverless. Esta suite de tecnologías ha permitido a Iberia revolucionar su forma de operar y servir a sus clientes.

“El sector aeronáutico está experimentando una transformación sin precedentes, donde la adaptabilidad y la vanguardia tecnológica son cruciales”, afirma **Suzana Curic, directora general de AWS para España y Portugal**. “La colaboración con Iberia ejemplifica cómo la nube puede potenciar la resiliencia operativa y catalizar la innovación en la experiencia del viajero. El despliegue estratégico de tecnologías basadas en IA en áreas clave como la atención al cliente, el mantenimiento y las operaciones demuestra el potencial transformador de la nube en la aviación, abriendo nuevos horizontes para un sector más ágil y centrado en el cliente”.

Por su parte, **Gabriel Perdiguero, Director Financiero y Tecnológico de Iberia**, destaca el impacto transformador de esta iniciativa: “Nuestra alianza estratégica con AWS marca un antes y un después en la trayectoria de Iberia. La migración de nuestros sistemas a la nube y la adopción de tecnologías de vanguardia en IA



La transformación digital de Iberia va mucho más allá de una mera actualización tecnológica

y análisis de datos no solo han revolucionado nuestra eficiencia interna, sino que nos han dotado de las herramientas necesarias para reinventar la experiencia de volar. Este salto tecnológico nos permite anticiparnos a las necesidades del viajero del futuro, consolidando nuestra posición como líderes en innovación aeronáutica y reforzando nuestro compromiso de conectar personas y culturas de manera sostenible y eficiente”.

Optimización operativa e innovación en la experiencia del cliente

La transformación digital de Iberia va más allá de la mera actualización tecnológica. La implementación de soluciones basadas en inteligencia artificial (IA) está permitiendo a la aerolínea mejorar significativamente la satisfacción de sus pasajeros. Los sistemas automatizados y la analítica

Revolución en los cielos

avanzada permiten ofrecer experiencias más personalizadas y eficientes en cada punto de contacto con el cliente.

Asimismo, la migración a la nube ha permitido a Iberia optimizar sus operaciones en múltiples niveles. Una mayor velocidad en la actualización de sistemas y la reducción de los tiempos de ciclo han mejorado la eficiencia en áreas críticas como la gestión de vuelos, el mantenimiento de aeronaves y la coordinación de tripulaciones. Por otro lado, la implementación de aplicaciones críticas en la nube ha aumentado significativamente la fiabilidad y resiliencia de los sistemas de Iberia. Esto se traduce en una mayor estabilidad operativa y una capacidad mejorada para manejar picos de demanda y situaciones imprevistas.

Impacto en la competitividad

Esta transformación digital está posicionando a Iberia como líder en innovación dentro del sector aeronáutico. La agilidad y eficiencia conseguidas permiten a la aerolínea adaptarse más rápidamente a las cambiantes condiciones del mercado y ofrecer servicios más competitivos.

La adopción de tecnologías cloud e inteligencia artificial no solo mejora las operaciones actuales, sino que también prepara a Iberia para el futuro del transporte

Actualidad – Te interesa

aéreo. La compañía está ahora mejor equipada para desarrollar nuevos servicios innovadores y responder ágilmente a las necesidades cambiantes de sus clientes.

Sostenibilidad y eficiencia

Uno de los temas más debatidos en la actualidad es el impacto que tiene la migración de cualquier empresa u organización a la nube en términos de sostenibilidad. Para Iberia, la eliminación de sus centros de datos físicos y la optimización de recursos tecnológicos contribuirán a reducir la huella de carbono de la compañía, alineándose con los objetivos de sostenibilidad del sector aeronáutico.

Y es que según un reciente informe de Accenture, la infraestructura global de AWS es hasta 4,1 veces más eficiente energéticamente que las instalaciones tradicionales on-premises. Esta eficiencia se traduce en cifras concretas: las empresas que migran sus cargas de trabajo a AWS pueden reducir su huella de carbono hasta en un 98%. En el caso de Iberia, esta eficiencia se multiplica gracias a la optimización de sus sistemas y al aprovechamiento de tecnologías específicas de AWS diseñadas para maximizar el rendimiento energético, contribuyendo así de manera significativa a los objetivos de sostenibilidad de la aerolínea y del sector en su conjunto.

Perspectivas de futuro

La transformación digital de Iberia sienta las bases para una nueva era en la aviación comercial. La combinación de infraestructura cloud con capacidades de inteligencia artificial está permitiendo a la aerolínea reimaginar el transporte aéreo desde sus cimientos, creando nuevas posibilidades para la innovación y la mejora continua.

Este proyecto plurianual de transformación refleja el compromiso de Iberia con su propósito de generar prosperidad conectando personas en todo el mundo. La modernización tecnológica no solo mejora la eficiencia operativa, sino que también permite a la compañía ofrecer experiencias excepcionales a sus clientes.

Despegando hacia el futuro digital

La alianza de Iberia y AWS demuestra cómo la adopción estratégica de tecnologías cloud e inteligencia artificial puede transformar fundamentalmente una empresa tradicional. La decisión de migrar completamente a la nube y aprovechar las capacidades de AWS ha permitido a Iberia no solo mejorar su eficiencia operativa, sino también posicionarse como líder en la innovación del transporte aéreo.

Esta transformación digital marca un antes y un después en la historia de Iberia y establece un

Revolución en los cielos



Este proyecto refleja el compromiso de Iberia con su propósito de generar prosperidad conectando personas en todo el mundo

nuevo estándar para la industria aeronáutica. A medida que el sector continúa evolucionando, la base tecnológica construida por Iberia le permitirá seguir innovando y ofreciendo experiencias excepcionales a sus clientes, manteniendo su posición como una de las aerolíneas más avanzadas tecnológicamente en Europa.

El éxito de esta iniciativa demuestra que la transformación digital no es solo una actualización tecnológica, sino una reimaginación completa de cómo una empresa puede operar y servir a sus clientes en la era digital. Iberia ha sentado un precedente que sin duda inspirará a otras compañías del sector a emprender sus propios viajes de transformación digital.



Actualidad – Te interesa

La identidad: el nuevo perímetro de seguridad

Por JOSÉ MARÍA OCHOA,
Cybersecurity Area Director
de OneseQ (el área de
ciberseguridad de Alhambra IT)



La escena es inolvidable: Misión Imposible (1996), Ethan Hunt (Tom Cruise) descendiendo desde el techo, suspendido por un cable, evitando con precisión quirúrgica sensores de movimiento, temperatura y sonido. Todo un despliegue de controles perimetrales que buscaban impedir el acceso a un sistema crítico. Pero, al final, la clave no eran los rayos láser ni las cámaras de vigilancia. El verdadero punto débil estaba en la **identidad**: si alguien lograba hacerse pasar por quien no era, todo lo demás se derrumbaba.

Esto no es cine, es la realidad diaria de nuestras organizaciones. Durante años hemos concebido la ciberseguridad como muros, firewalls y perímetros físicos o virtuales. Sin embargo, en un mundo donde el trabajo remoto, la nube y la movilidad son ya la norma, el perímetro clásico ha desaparecido. Hoy, el nuevo perímetro es la **identidad digital**.



Identidad: la llave maestra

Cada usuario, cada aplicación, cada sistema conectado a nuestra red se presenta con una "llave". Si esa llave es débil, compartida o reutilizada el atacante no necesita técnicas de ataque y evasión al estilo Hollywood: simplemente entra por la puerta principal. Las estadísticas lo avalan: más del 70% de las brechas de seguridad comienzan con credenciales comprometidas. Un solo descuido

—una contraseña débil, un clic en un correo de phishing— puede abrir el camino a un ransomware devastador o a un robo masivo de información confidencial.

Mucho más que autenticación del usuario

Aquí es donde solemos cometer un error de concepto. Pensamos en gestión de identidades como sinónimo de "usuario + contraseña + multifactor". Pero la realidad es más amplia:

Actualidad – Te interesa

hablamos de Identity and Access Management (IAM), que incluye políticas de aprovisionamiento y des-aprovisionamiento, gestión de privilegios, segregación de funciones y revisiones periódicas de accesos. En una compañía, no es un problema exclusivo del empleado que usa la misma clave en su correo personal y en la VPN

“La gestión moderna se apoya en autenticación multifactor, biometría, análisis de comportamiento y políticas adaptativas

corporativa: es una responsabilidad de gobierno de la seguridad IT, un marco corporativo que establece cómo se conceden, controlan y revocan los accesos en toda la organización.

Identidad también entre máquinas

Y no olvidemos que la identidad no pertenece solo a las personas. Hoy, gran parte del tráfico corporativo es máquina a máquina, aplicación a aplicación. Servicios en la nube que validan tokens, APIs que intercambian información, microservicios que se autentican entre sí. Si estos procesos carecen de un gobierno de identidades robusto, se convierten en puertas traseras perfectas para un atacante. No basta con proteger al usuario humano; también debemos garantizar que cada sistema es quien dice ser y que solo hace lo que debe.

La identidad: el nuevo perímetro de seguridad

De la contraseña al control inteligente

La gestión moderna se apoya en autenticación multifactor, biometría, análisis de comportamiento y políticas adaptativas que ajustan el nivel de seguridad según el riesgo. El enfoque Zero Trust lo resume bien: no confiar en nadie por defecto, aunque esté “dentro”. Cada acceso debe ser validado, ya sea de un usuario o de un sistema. Y cada acción debe quedar registrada para poder ser auditada.

Conclusión: menos espectáculo, más control

La escena de Misión Imposible nos entretiene porque convierte en espectáculo lo que en realidad debería ser rutinario: controlar accesos y proteger la identidad. En el cine hay música trepidante y giros imposibles; en la empresa, lo que hay son responsabilidades legales, sanciones regulatorias y, sobre todo, la reputación de un negocio en juego. La gestión de identidades ya no es un “extra”, es la primera línea de defensa. Porque en ciberseguridad, el verdadero perímetro no son los firewalls ni IDSs o IPSs ...: es saber con certeza quién eres tú, quién es tu sistema y qué puede hacer cada uno.



Actualidad – Te interesa

HCLSoftware: Desde IBM hasta el blueprint XDO — seis años de evolución y liderazgo en la era Digital+

En el dinámico mundo del software empresarial, pocas compañías han demostrado un crecimiento y una transformación tan notables como HCLSoftware en los últimos seis años. Desde su histórica adquisición de productos de IBM hasta la introducción de su innovador blueprint XDO (Xperience, Data, Operations), la compañía ha consolidado su posición como socio estratégico para miles de organizaciones que buscan prosperar en la economía Digital+.

2018–2019:

La adquisición que cambió el rumbo

El punto de inflexión llegó en 2019, cuando HCL firmó el mayor acuerdo de adquisición de software por parte de una empresa india, valorado en **1.8 mil millones de dólares**, para incorporar múltiples productos de IBM a su portafolio. Esta operación no solo amplió de forma significativa sus capacidades, sino que también marcó el nacimiento de la unidad de negocio de Products & Platforms, que posteriormente evolucionaría a HCLSoftware.

La integración de estos productos —líderes en colaboración, desarrollo, seguridad y comercio electrónico— permitió a HCLSoftware ofrecer



HCLSoftware

una propuesta de valor completa y robusta, impulsando su expansión a nivel global y fortaleciendo su presencia en sectores estratégicos.

2020–2021:

Innovación orgánica y expansión global

En paralelo a la integración, la compañía aceleró su **desarrollo orgánico**, creando nuevas soluciones para simplificar operaciones de TI y de negocio. Su visión: combinar la

innovación tecnológica con una profunda comprensión de las necesidades reales de las empresas.

Durante estos años, HCLSoftware amplió su huella internacional, alcanzando más de **18.000 clientes** en **135 países**, incluyendo más de **220 empresas Fortune 500**. Además, incrementó su inversión anual en I+D a más de 130 millones de dólares, respaldada por 19 laboratorios de innovación en todo el mundo.

2022–2024:

Consolidación de la estrategia Digital+

Con el avance de la **economía Digital+**, caracterizada por la hiperconexión de personas, organizaciones y equipos, HCLSoftware adaptó su enfoque para ayudar a las empresas a ofrecer experiencias digitales integradas, seguras y eficientes. En esta etapa, reforzó sus capacidades en áreas clave:

► **AI & Intelligent Operations:** soluciones como HCL DRYiCE y UNO para automatizar operaciones, optimizar procesos y potenciar la toma de decisiones.

Actualidad – Te interesa

- **Data & Analytics:** plataformas para transformar datos en información accionable, impulsando la agilidad empresarial.
- **Total Experience:** uniendo experiencia de cliente (CX), empleado (EX), usuario (UX) y multiexperiencia (MX) en un solo enfoque coherente.

También fortaleció productos insignia como BigFix para gestión unificada de endpoints, AppScan para seguridad de aplicaciones, Workload Automation para orquestación empresarial, Unica para marketing de precisión, y Commerce Cloud para comercio electrónico escalable.

2025: Hacia un modelo unificado con XDO

En 2025, HCLSoftware presentó su blueprint XDO — Xperience, Data, Operations, una propuesta que redefine el modelo operativo de las organizaciones modernas.

XDO parte de una premisa clara: el éxito en la era digital requiere integrar la experiencia del cliente y del empleado (Xperience), aprovechar al máximo los datos (Data) y optimizar las operaciones (Operations).

- **Xperience:** transformar interacciones fragmentadas en recorridos continuos y

personalizados, que generen valor y fidelidad en cada punto de contacto.

- **Data:** tratar los datos como un activo estratégico, accesible y confiable, que alimente decisiones rápidas y precisas.
- **Operations:** pasar de operaciones rígidas a flujos dinámicos, habilitados por automatización, observabilidad y adaptabilidad.

Este enfoque no solo conecta áreas críticas del negocio, sino que también facilita la adopción efectiva de tecnologías emergentes como la inteligencia artificial generativa (GenAI), la automatización avanzada y la nube híbrida.

HCLSoftware hoy: un socio estratégico para la transformación

Actualmente, HCLSoftware es mucho más que un proveedor de software: es un **orquestador de resultados** en la economía Digital+. Su portafolio abarca soluciones para **negocios e industria, inteligencia artificial y operaciones inteligentes, analítica de datos, ciberseguridad, colaboración soberana y software especializado**, todas diseñadas para ofrecer flexibilidad de despliegue y escalabilidad sin comprometer seguridad ni rendimiento.

Con un ADN basado en la **confianza, la agilidad, la responsabilidad y la innovación**, la compañía

HCLSoftware: Desde IBM hasta el blueprint XDO



Actualmente, HCLSoftware es mucho más que un proveedor de software: es un orquestador de resultados en la economía Digital+

sigue impulsando el éxito de sus clientes a través de un enfoque pragmático y visionario.

En solo seis años, HCLSoftware ha pasado de ser un nuevo jugador en el mercado de software empresarial a convertirse en un líder global que impulsa la transformación digital de miles de organizaciones. Desde la adquisición estratégica de productos de IBM hasta la creación del blueprint XDO, su evolución refleja una capacidad única para anticiparse a las tendencias, adaptarse a los cambios y entregar valor tangible.

En la economía Digital+, donde la experiencia, los datos y las operaciones marcan la diferencia, HCLSoftware se posiciona como el socio que ayuda a las empresas no solo a mantenerse relevantes, sino a liderar el cambio.



Actualidad – Te interesa

Transformación Digital de Laboratorios Universitarios con Amazon AppStream 2.0 y WorkSpaces

Sobre VIU

La Universidad Internacional de Valencia (VIU) es una universidad online con sede en España que pertenece a la división de Formación y Universidades del Grupo Planeta. Esta división está presente en 8 países y cuenta con 22 instituciones educativas. VIU está especializada en formación superior a distancia a través de un modelo educativo flexible y personalizado.

El contexto

VIU identificó la necesidad de crear un entorno de aprendizaje moderno, flexible y seguro que permitiera a estudiantes y profesores acceder a herramientas académicas desde cualquier lugar, en cualquier momento. El objetivo era proporcionar una plataforma digital intuitiva para compartir información, colaborar en proyectos y facilitar la enseñanza remota con experiencias de usuario de alto nivel.

El desafío

Uno de los principales retos consistía en ofrecer laboratorios virtuales equipados con software especializado, adaptados a los



requerimientos de cada programa académico, sin incurrir en altos costes de infraestructura física ni comprometer la escalabilidad ni la seguridad. Además, se requería gestionar de forma centralizada y automatizada la actualización de software, el licenciamiento y el control de acceso, asegurando una

experiencia fluida para más de 10.000 estudiantes por ciclo escolar.

La solución

Desde Itera Process se diseñó y se implementó una solución en la nube basada en Amazon AppStream 2.0 y Amazon WorkSpaces,

Actualidad – Te interesa

permitiendo la entrega segura y escalable de escritorios virtuales y aplicaciones especializadas bajo demanda.

Gracias a la integración con flujos de autenticación personalizados, los estudiantes acceden a sus entornos con un solo clic, desde cualquier dispositivo y sin necesidad de instalaciones locales.

Con AppStream 2.0, los estudiantes pueden ejecutar aplicaciones intensivas en recursos directamente desde el navegador, con alto

rendimiento, baja latencia y sin comprometer la experiencia de usuario.

Además, el modelo de pago por sesión optimiza los costes, garantizando una excelente relación coste-beneficio tanto para la universidad como para los alumnos. La solución se complementa con un servicio de soporte gestionado 24/7, que asegura una operación continua y sin interrupciones.

"Destacamos el acompañamiento cercano y profesional de Itera, con quienes colaboramos desde el inicio para desplegar eficientemente

los entornos e integrar los distintos softwares. Además, contamos con el apoyo constante del equipo de soporte 24x7, con quienes mantenemos una comunicación fluida y efectiva".

Rubén Cañavera Domingo, Responsable Laboratorios Virtuales y Software en VIU

Beneficios

La implementación de Amazon AppStream 2.0 y WorkSpaces ha sido clave en la estrategia tecnológica de la universidad, permitiéndose posicionar como una institución reconocida internacionalmente por su enfoque en educación digital de alto rendimiento. Con tiempos de aprovisionamiento reducidos a minutos y una experiencia de usuario optimizada, más de 10.000 estudiantes por ciclo acceden a herramientas de aprendizaje sin barreras físicas ni técnicas.

La solución planteada desde Itera permitió a la Universidad no solo reducir costes operativos y administrativos, sino también mejorar significativamente la flexibilidad, disponibilidad y escalabilidad de su infraestructura tecnológica educativa, alineándose con las demandas actuales del aprendizaje remoto e híbrido.

Conoce más en: iteraproces.com



itera
it & business process

CASO DE ÉXITO: UNIVERSIDAD INTERNACIONAL DE VALENCIA
Transformación Digital de Laboratorios Universitarios con Amazon AppStream 2.0 y WorkSpaces

Destacamos el acompañamiento cercano y profesional de Itera, con quienes colaboramos desde el inicio para desplegar eficientemente los entornos e integrar los distintos softwares. Además, contamos con el apoyo constante del equipo de soporte 24x7, con quienes mantenemos una comunicación fluida y efectiva.

 Rubén Cañavera Domingo
Responsable Laboratorios Virtuales y Software en VIU

viu Universidad Internacional de Valencia
De: Planeta Formación y Universidades

aws
PARTNER
Premier Tier Services



Actualidad – Te interesa

Elevando la Ciberresiliencia: Cómo SentinelOne y PurpleAI Están Transformando las Operaciones de Seguridad

El panorama de la ciberseguridad evoluciona a una velocidad que no deja espacio para la complacencia. Las amenazas impulsadas por inteligencia artificial, junto con infraestructuras cada vez más complejas, hacen que las defensas tradicionales ya no sean suficientes. Hoy, las organizaciones deben estar preparadas no solo para prevenir ataques, sino también para detectarlos, responder y recuperarse en tiempo real.

La plataforma Singularity de SentinelOne, combinada con la inteligencia de PurpleAI, marca un nuevo estándar de resiliencia. De la mano de partners de confianza como Nextret, las empresas están fortaleciendo sus operaciones de seguridad y ganando eficiencia frente a riesgos crecientes.

Protección Unificada Sin Ruido

La plataforma Singularity consolida la protección de endpoints, cargas en la nube e identidades en una única solución basada en IA. A diferencia de herramientas aisladas que generan alertas dispersas, ofrece una visión unificada de la superficie de ataque. Su motor de IA conductual identifica y neutraliza amenazas —incluyendo ataques de día cero y ransomware— a la velocidad de la máquina, muchas veces antes de que se ejecuten.

Este enfoque reduce la exposición, acorta los ciclos de remediación y garantiza continuidad operativa incluso ante intentos de ataque. Partners como Nextret destacan cómo esta consolidación libera a los equipos de la fatiga de alertas, permitiéndoles centrarse en lo esencial: proteger los activos críticos.

PurpleAI: Un Analista Que Nunca Duerme

Los Centros de Operaciones de Seguridad suelen enfrentarse a una avalancha de alertas e investigaciones complejas. Aquí entra en juego PurpleAI, el analista de IA de SentinelOne. No se limita a asistir: amplía las capacidades humanas al clasificar automáticamente alertas y correlacionar datos entre endpoints, nube, identidades y registros de SIEM. Gracias a su capacidad de responder a consultas en lenguaje natural —por ejemplo, “¿Cuál fue la causa raíz de este intento de ransomware?”—, PurpleAI reduce drásticamente los tiempos de detección (MTTD) y de respuesta (MTTR). El resultado: equipos más rápidos, efectivos y confiados.

PurpleAI también automatiza flujos completos de investigación y respuesta, genera informes claros y sugiere pasos de remediación. Esto libera a los analistas de tareas repetitivas y les permite dedicar

más tiempo a actividades de mayor valor, como la búsqueda proactiva de amenazas o la planificación estratégica.

En un contexto de escasez de talento y equipos sobrecargados, esta capacidad se convierte en un multiplicador esencial. Como señala Nextret, soluciones como PurpleAI permiten que equipos de cualquier tamaño alcancen un nivel de seguridad empresarial sin que los costes crezcan proporcionalmente.

Construyendo un Futuro Resiliente

A medida que los atacantes utilizan IA para perfeccionar y escalar sus operaciones, las empresas necesitan defensas igual de adaptativas. La combinación de Singularity y PurpleAI ofrece la autonomía, la inteligencia y la velocidad necesarias para mantenerse un paso adelante. Con el apoyo de partners como Nextret, las organizaciones pueden implementar estas soluciones de manera eficaz, asegurando resiliencia, agilidad y claridad en sus operaciones. Ya no se trata solo de defenderse de las amenazas, sino de construir la capacidad de prosperar con seguridad en la era de la IA.



Actualidad – Te interesa

El espejismo de las suites all-in-one: Por qué las alertas inteligentes marcan la diferencia en gestión de gastos de viaje corporativos

La promesa de tenerlo todo en una única plataforma sigue seduciendo a muchos CIOs. Pero cuando se trata de controlar los gastos de viaje profesionales, la especialización con inteligencia embebida está demostrando ser más efectiva que la amplitud funcional.

“One vendor, one throat to choke”: Durante dos décadas, este ha sido el mantra que ha guiado las decisiones tecnológicas empresariales. Sin

embargo, con el 67% de los CIOs asumiendo responsabilidad financiera (según Gartner), surge una pregunta incómoda: ¿puede una suite que promete hacer todo destacar en algo tan crítico como el control de gastos en tiempo real?

La promesa incumplida del “todo en uno”

Cuando las grandes suites ERP y HR decidieron añadir módulos de gestión de gastos a su

propuesta de valor todo parecía indicar que estábamos antes la solución definitiva. Integración total, un único proveedor, simplicidad contractual, un menor TCO (Total Cost of Ownership)... Prometedor, ¿verdad?

Sin embargo, la realidad que están descubriendo los responsables de TI es bastante diferente. Además de los costes ocultos de personalización, mantenimiento o soporte o de la dependencia total del roadmap de un único proveedor, el gran riesgo está en la **ineficacia para detectar irregularidades**.

Un reciente informe de [ACFE](#) revela que el fraude en el reembolso de gastos tarda 18 meses en ser detectado, lo que ocasiona una pérdida media de 50.000 dólares anuales. En cambio, las empresas que cuentan con una solución especializada logran detectar las irregularidades antes de 6 meses.

¿Por qué esta diferencia? La causa es estructural: los módulos de gastos de las suites *all-in-one* operan con procesamiento batch nocturno, pero carecen de las **alertas en tiempo real** que, es lo que realmente marca la diferencia.

Es como tener un antivirus que te avisa de la infección un mes después. Las herramientas “todo en uno” te dan informes sobre lo que ya pasó, no te ayudan a prevenir lo que está pasando.



Actualidad – Te interesa

Alertas inteligentes multicapa: El factor diferencial de la especialización

En cambio, las soluciones especializadas como [Okticket](#) cuentan con una arquitectura event-driven que operan en tiempo real, transformando la gestión reactiva en proactiva. En este sentido, la aplicación de digitalización de gastos de viajes profesionales ha desarrollado un sistema de [alertas inteligentes](#) que operan en tres capas complementarias:

- **Alertas preventivas:** Bloquean gastos irregulares antes de que se produzcan. Por ejemplo, si un empleado intenta reservar un hotel de cinco estrellas cuando la política interna indica que no puede superar las tres, el sistema lo impide automáticamente. El resultado es una reducción del 94% de los gastos que incumplen la política.
- **Alertas operativas:** Notificaciones instantáneas que se lanzan durante el proceso de gasto. Pongamos el caso de un proyecto que alcanza el 85% de su presupuesto. En ese momento, los managers reciben una alerta inmediata, no un informe a final de mes. El impacto es una reducción del 70% en tiempo de gestión administrativa.
- **Alertas analíticas:** Consiste en la detección de patrones mediante *machine learning*. El sistema identifica automáticamente cuando un proveedor cobra sistemáticamente un 20% más que las alternativas, o cuando hay patrones de gasto anómalos que podrían indicar fraude.

La fuerza del 'best-of-breed': integración que realmente importa

Incluso el argumento de que las suites *all-in-one* se integran mejor se ha convertido en una de sus mayores debilidades. Estas herramientas sólo se integran bien dentro de su propio ecosistema, lo que obliga a las empresas a una dependencia tecnológica completa.

Las herramientas especializadas modernas, por el contrario, nacen con **APIs abiertas** diseñadas para conectarse con cualquier sistema. Volvemos al caso de [Okticket](#), que se [integra de forma simple](#) y bidireccional con los principales sistemas de ERP y de Recursos Humanos.

Esta integración lleva una media de dos o tres semanas, mientras que modificar el comportamiento del módulo de gastos en una suite requiere proyectos de customización de seis meses con consultorías especializadas.

El test definitivo para tu empresa

¿Debería replantearse tu estrategia de gestión de gastos corporativos? Si tardas más de 24 horas en responder a las siguientes preguntas, la respuesta está clara:

- ¿Cuánto gastó exactamente el departamento comercial esta semana?
- ¿Qué empleados están cerca de exceder su límite mensual ahora mismo?

El espejismo de las suites all-in-one

- ¿Existen patrones de gasto anómalos en este momento?
- ¿Qué proveedores nos están cobrando sistemáticamente de más?

Conclusión: el futuro es proactivo, no reactivo

Por tanto, el debate ya no está en si elegir una suite *all-in-one* o una *best-of-breed*. Ahora hay que decidir entre gestión reactiva o proactiva.

Posiblemente las herramientas todo en uno sigan teniendo un lugar destacado en los procesos estables y predecibles. Pero en la gestión de gastos corporativos **las soluciones especializadas con inteligencia embebida pueden marcar la diferencia** entre controlar o ser controlado por los gastos.

En definitiva. Para el CIO moderno, la pregunta ya no es: "¿Puedo tenerlo todo en uno?", sino: "¿Puedo permitirme no tener lo mejor en lo que realmente importa?".

Sobre Okticket: Solución SaaS española especializada en la gestión inteligente de gastos de viaje profesionales, con más de 2.000 empresas usando su sistema de alertas en tiempo real. Certificada por la Agencia Tributaria y con ISO 27001, ofrece ROI demostrable desde el primer mes de uso.



Actualidad – Te interesa

10 medidas de seguridad que deberías tener implementadas en tu entorno Microsoft en 2025

En 2025, la seguridad en los entornos Microsoft 365 no puede dejarse al azar. Con un volumen creciente de amenazas, ataques cada vez más sofisticados y un entorno empresarial cada vez más distribuido, es imprescindible adoptar un enfoque estructurado, preventivo y automatizado. A continuación, se detallan diez medidas que toda organización debería tener implementadas para garantizar una postura de seguridad robusta.

Por FRANCISCO R. GARCÍA.

1. MFA obligatorio

La autenticación multifactor (MFA) es la defensa más efectiva contra accesos no autorizados. Debe aplicarse sin excepciones, incluso en cuentas de servicio y administradores. Herramientas como Microsoft Authenticator o claves FIDO2 refuerzan la seguridad sin afectar la experiencia del usuario.



2. Protección de identidades con Entra ID Protection

Esta solución evalúa el riesgo de inicio de sesión en tiempo real y responde automáticamente ante



Actualidad – Te interesa

10 medidas de seguridad que deberías tener implementadas en tu entorno Microsoft

comportamientos sospechosos. Integrada con políticas de acceso condicional, permite una protección adaptativa.

3. Clasificación automática de la información

Microsoft Purview permite etiquetar y proteger documentos y correos según su contenido. Esto facilita el cumplimiento normativo (RGPD, LOPDGDD) y mejora la conciencia de seguridad.

4. Prevención de fuga de datos (DLP)

Las políticas DLP deben aplicarse en todos los canales: correo, nube, Teams, etc. Es vital identificar datos sensibles (NIF, cuentas bancarias, historiales médicos) y evitar su salida sin control.

5. Seguridad de dispositivos con Intune y Defender for Endpoint

La gestión de dispositivos debe estar integrada con la protección contra amenazas. Intune permite configurar dispositivos seguros, aplicar borrado remoto y controlar el acceso a recursos corporativos.

6. Detección avanzada con Microsoft Defender XDR

Defender XDR correlaciona eventos entre identidades, dispositivos y aplicaciones,

detectando ataques complejos. El uso de KQL permite automatizar respuestas y mejorar la eficiencia operativa.

7. Microsoft Sentinel como SIEM moderno

Sentinel agrega eventos de seguridad de todo el entorno, incluyendo soluciones de terceros. Su capacidad de automatización permite una respuesta rápida y escalable.

8. Acceso condicional basado en riesgo

El acceso debe adaptarse al contexto: ubicación, tipo de dispositivo, sensibilidad de la aplicación. Esto protege activos críticos sin afectar la productividad.

9. Gestión de privilegios con PIM

Privileged Identity Management otorga permisos elevados solo cuando se necesitan, bajo aprobación y por tiempo limitado. Esto reduce el riesgo y mejora la trazabilidad.

10. Simulacros y formación contra phishing

La mayoría de los ataques comienzan con un clic. Microsoft 365 permite realizar simulacros y campañas de concienciación personalizadas, convirtiendo a los empleados en defensores activos.



Las políticas DLP deben aplicarse en todos los canales. Es vital identificar datos sensibles y evitar que se produzca una salida sin control de los mismos

CONCLUSIÓN

Estas medidas representan una estrategia integral para fortalecer la seguridad, cumplir normativas y proteger activos críticos. Aunque requieren inversión, cualquier organización puede empezar con un equipo experto que le acompañe en el proceso.

La seguridad en Microsoft 365 no es un destino, sino un camino continuo que exige compromiso y evolución constante.



Actualidad – Te interesa

Vertiv impulsa el futuro de la energía crítica: resiliencia y eficiencia para la nueva era de los centros de datos

Vertiv aborda los desafíos actuales de los centros de datos con una propuesta tecnológica que combina innovación, fiabilidad y visión de futuro. Su estrategia se centra en soluciones de Sistemas de Alimentación Ininterrumpida (SAIS) que garantizan alto rendimiento, eficiencia y sostenibilidad.

Vertiv Trinergy: Energía Inteligente y Modularidad Extrema

Vertiv™ Trinergy™ es el SAI más avanzado de la compañía, con más de 16 GW instalados globalmente. Su diseño modular permite escalar de 1.5 MW a 20 MW, adaptándose a despliegues en sala o soluciones prefabricadas. Alcanza una eficiencia de hasta el 99% gracias al modo Dynamic Online, que combina la disponibilidad de la doble conversión con el ahorro energético. Trinergy ofrece disponibilidad para estándares Tier IV, gestiona picos de demanda y variaciones de carga comunes en entornos de IA y computación de alto rendimiento. Además, se integra con energías alternativas como baterías de ion-litio o pilas de combustible, ampliando las opciones de sostenibilidad. Mario Vasconcelos, Sales director Enterprise Accounts en Vertiv, destaca que: "Trinergy está diseñado para ofrecer máxima disponibilidad en entornos de alta densidad y cargas

dinámicas, permitiendo a los operadores responder a las demandas energéticas y avanzar hacia la sostenibilidad sin comprometer el rendimiento".

Liebert® EFC: Eficiencia en Refrigeración y Reducción del Consumo de Agua

La gestión del consumo de agua y la eficiencia térmica son cruciales. Liebert® EFC es la respuesta de Vertiv a esta inquietud: un sistema de refrigeración de última generación que optimiza el uso de recursos hídricos y energéticos, adaptándose a climas y cargas variables. Este sistema es fundamental para reducir el impacto ambiental de los centros de datos.

Vertiv LIFE Services: Monitorización y Gestión Inteligente

La tercera pieza de la estrategia es Vertiv LIFE Services, una plataforma de monitorización y gestión que combina análisis en tiempo real, mantenimiento predictivo y soporte remoto. Integra datos de SAIS, unidades de refrigeración y distribución eléctrica, ofreciendo una visión unificada del estado del data center. Su enfoque de mantenimiento basado en la condición real de los equipos permite planificar intervenciones solo cuando son necesarias, evitando

revisiones innecesarias y reduciendo el riesgo de averías. Esto se traduce en mayor disponibilidad, reducción de paradas imprevistas, optimización de recursos, menores costes operativos y una extensión de la vida útil de los activos críticos. Vertiv LIFE Services se apoya en la red global de Vertiv, con más de 3.500 ingenieros de campo y 240 centros de servicio, garantizando soporte local con alcance global.

Respondiendo a las Tendencias de 2025

El desarrollo de Trinergy, Liebert® EFC y Vertiv LIFE Services se alinea con las tendencias actuales de los centros de datos: el crecimiento exponencial de la demanda energética por IA, HPC y servicios en la nube; la presión regulatoria y social para reducir el consumo de agua, emisiones y huella de carbono; y la necesidad de garantizar la continuidad operativa absoluta. Vertiv ha tenido en cuenta estos desafíos, apostando por la modularidad, la eficiencia y la integración con energías limpias. Vasconcelos concluye que "el futuro de los centros de datos se construye con innovación y responsabilidad, y que las soluciones de Vertiv están diseñadas para que tecnología y sostenibilidad avancen de la mano".





De la oficina a las zonas más remotas: Conectividad con Starlink y Sewan



Cobertura global y fiable
incluso en zonas remotas



Internet rápido y seguro,
con tecnología satelital



Fácil integración
con SD-WAN, fibra y Cloud Firewall Fortinet



Respaldo garantizado
con la confianza y experiencia de Sewan

Webinar exclusivo: Starlink con Sewan

Martes, 21 de octubre – 11:00h (online)

Conoce la oferta de Sewan como **revendedor autorizado** de Starlink y sus claves de negocio

- Casos reales**
y ventajas competitivas
- Integración**
con SD-WAN y seguridad
- Claves prácticas**
para impulsar tu conectividad

Regístrate aquí



Comidas BYTE TI

Los retos de la inteligencia artificial en la empresa



Hablar de inteligencia artificial, hoy en día, es hablar de una realidad que ya se encuentra implícita en la rutina de cualquier departamento de TI. Lo que parecía un experimento, se ha convertido en una herramienta que agiliza tareas, ayuda a los equipos y obliga a replantearse nuevos formatos de trabajo. Los responsables tecnológicos ya lo tienen en cuenta: la IA ya es hábito más.

Para analizar este fenómeno, desde ByteTI hemos organizado un encuentro con Antonio Gil, Director Corporativo de Operaciones y Sistemas de GVC Gaesco; Francisco Borja Escalona, Chief Data Officer de Carrefour España; Henar Pinilla, CTO de CESCE; Héctor Moreno, Corporate Head of Networks and Telecoms Department de Acciona; Francisco Pachón, Head of Enterprise Architecture de National-Nederlanden; Jesús Garrido, Director de Tecnologías de la Información del Instituto Nacional de Técnica Aeroespacial, INTA; Eduardo Rodríguez, Director TI / CTO de Urbaser; Juan Pedro Gozalo, Head of Hyperautomation de Allfunds; Jaime Requejo, Lead Architect-Strategist Solutions de HCLSoftware; Guillermo Arias, Strategic Account Manager de Ping Identity y Julián Sanz, Cloud Solution de Arsys.

Beneficios de la IA en los departamentos

En palabras de Francisco Borja Escalona, Chief Data Officer de Carrefour España, el apoyo desde la alta dirección ha sido determinante: "Nuestra CEO es una ferviente admiradora de la inteligencia artificial, y eso ha hecho que todas las áreas de negocio de Carrefour tengan proyectos y un roadmap claro de IA". Según

Comidas BYTE TI



Hay muchos casos de uso que pueden parecer viables en concepto, pero que más adelante no llegan a consolidarse

explicó, la compañía ha automatizado procesos cotidianos como la atención telefónica de clientes y la toma de decisiones comerciales con algoritmos: "El día del Club Carrefour se apoya en decisiones tomadas con IA, pero siempre con un humano detrás para validar".

Por su parte, Henar Pinilla CTO de CESCE destacó la utilidad de la IA en la fase de pruebas: "Estamos aplicando IA en testing unitario y en casos de prueba, lo que nos ha permitido mejorar la calidad del desarrollo". No obstante, advirtió que en el terreno de negocio los avances son aún limitados: "No podemos decir que estamos utilizando IA de manera decisoria porque la normativa no lo permite, aunque creemos que esto cambiará".

Al igual que sus compañeros, Héctor Moreno, Corporate Head of Networks and Telecoms



Antonio Gil,
Director Corporativo de Operaciones y Sistemas de GVC Gaesco

Department de Acciona subrayó la aportación de la IA a la eficiencia: "Hemos conseguido unificar toda la información generada en el mundo, lo que nos permite responder con rapidez a las necesidades de negocio y reducir tiempos de forma drástica". En su caso, cada línea de negocio (agua, energía, construcción) desarrolla proyectos propios, pero con la mirada puesta en una estrategia común que permita escalar de forma ordenada.

A pesar de ello, no todas las iniciativas alcanzan la meta: "Un proyecto que debía estar en producción el año pasado aún sigue parado porque el usuario exige respuestas exactas que hoy son difíciles de garantizar. Es un ejemplo de cómo un caso de uso puede ser viable en concepto, pero no llegar a consolidarse", reconoció Héctor Moreno.



Eduardo Rodríguez,
Director TI y CTO de Urbaser



Francisco Borja Escalona,
Chief Data Officer de Carrefour España

Siguiendo este punto, Francisco Pachón, Head of Enterprise Architecture de National-Nederlanden, puntualiza que la raíz de los fracasos está en el dato: "Queríamos desarrollar un chatbot para la red comercial que se alimentara de documentación histórica. El problema fue que esos documentos, acumulados durante años, se contradecían entre sí, lo que impedía dar una respuesta fiable. Tuvimos que volver atrás y centrarnos primero en limpiar y catalogar los datos".

Principales retos de la IA en TI

Como bien explicó Antonio Gil, Director Corporativo de Operaciones y Sistemas de GVC Gaesco, el gran desafío está en equilibrar expectativas y eficiencia: "Nuestro reto principal es la eficiencia. El 90% de los casos de uso están

Los retos de la inteligencia artificial en la empresa

Comidas BYTE TI



Francisco Pachón,
Head of Enterprise
Architecture de
National–Nederlanden



Guillermo Arias,
Strategic Account
Manager de Ping
Identity



Héctor Moreno,
Corporate Head of
Networks and Telecoms
Department de Acciona



Henar Pinilla,
CTO de CESCE



Jaime Requejo,
Lead Architect–Strategist
Solutions de HCLSoftware

ligados a la automatización de procesos. Pero también debemos gestionar las expectativas de los usuarios, que esperan de la IA respuestas inmediatas a todo”.

De manera complementaria, Francisco Pachón de National–Nederlanden puso el acento en la calidad de la información: “Cuando manejas datos pensados para humanos, un algoritmo puede no entenderlos igual. Si la base no está bien estructurada, la IA dará respuestas erróneas”.

En la misma línea, Jesús Garrido, Director de Tecnologías de la Información del Instituto Nacional de Técnica Aeroespacial, INTA recordó que el tiempo se ha convertido en un factor decisivo: “En apenas tres meses aparecen modelos nuevos que dejan obsoletos los

anteriores. O haces proyectos muy pequeños que duren tres meses o no llegas a tiempo”.

La velocidad de cambio tecnológico, ¿oportunidad o amenaza?

De acuerdo con Garrido, la rapidez del mercado puede jugar en contra: “Estuvimos un año trabajando con IBM Watson y los resultados fueron mediocres. En cuanto salió ChatGPT, en pocas semanas superamos lo que habíamos conseguido en meses. Pero todo lo anterior hubo que tirarlo”.

Muchas veces, el verdadero cambio es cultural, así lo destacó Eduardo Rodríguez, Director TI / CTO de Urbaser: “Hace apenas unos años era impensable aplicar IA en un sector tan tradicional como el de la limpieza urbana. Hoy tenemos

proyectos en plantas de tratamiento que identifican residuos o chatbots de soporte, y ya hemos detectado 70 u 80 iniciativas con retorno claro”. Sin embargo, advirtió de un problema grave: “No hay suficientes expertos en IA, ni dentro ni fuera de la empresa”.

Y es que, la clave, como apuntó Jaime Requejo, Lead Architect–Strategist Solutions de HCLSoftware, no está solo en elegir modelos, sino en coordinarlos: “Estamos entrando en una era en la que no solo se trata de probar modelos, sino de cómo los orquestamos. Los modelos pequeños, especializados en tareas concretas, van a ser clave, y el reto será coordinarlos”.

La regulación y el marco legal

En opinión de Henar Pinilla, las normativas

Los retos de la inteligencia artificial en la empresa

Comidas BYTE TI



Uno de los mayores retos de la IA es el cambio cultural, pero no hay nadie que dude de que estas tecnologías generan valor

actuales actúan como freno: "En seguros, la toma de decisiones no puede automatizarse todavía con IA, por lo que estamos limitados a pilotos y pruebas en TI".

Coincidiendo en este diagnóstico, Julián Sanz, Cloud Solution de Arsysis recordó la importancia de moverse en un marco seguro: "Somos una compañía europea y hemos decidido trabajar únicamente en este ámbito para cumplir con todas las regulaciones. Cualquier producto que lanzamos está pensado para ajustarse a las normativas actuales y futuras, como la AI Act".

La IA como palanca de transformación del negocio

Según expuso Guillermo Arias, Strategic Account Manager de Ping Identity, la inteligencia artificial debe contemplarse como una oportunidad de liderazgo: "El principal reto es económico. La



Jesús Garrido, Director de Tecnologías de la Información del Instituto Nacional de Técnica Aeroespacial, INTA

velocidad a la que avanza la IA genera un coste de oportunidad: si no apuestas hoy, mañana puede ser tarde. No hacer nada también supone un riesgo".

Del mismo modo, Eduardo Rodríguez señaló que la presión viene ahora también de los clientes: "El mayor reto ha sido el cambio cultural. Ahora ya nadie duda de que estas tecnologías generan valor".

El factor humano: talento y cambio cultural

En palabras de Francisco Borja Escalona, Chief Data Officer de Carrefour España, la IA nunca sustituye al criterio humano: "Todas las decisiones críticas siguen siendo humanas. La IA nos ayuda en aprovisionamiento, surtidos o promociones,

Los retos de la inteligencia artificial en la empresa



Juan Pedro Gonzalo
ALLFUNDS

pero el criterio final es de las personas".

El cuello de botella sigue estando en los perfiles especializados: "No hay talento suficiente. Incluso las consultoras más especializadas se ven desbordadas porque la tecnología cambia más rápido de lo que se puede aprender", recalcó Eduardo Rodríguez de Urbaser,

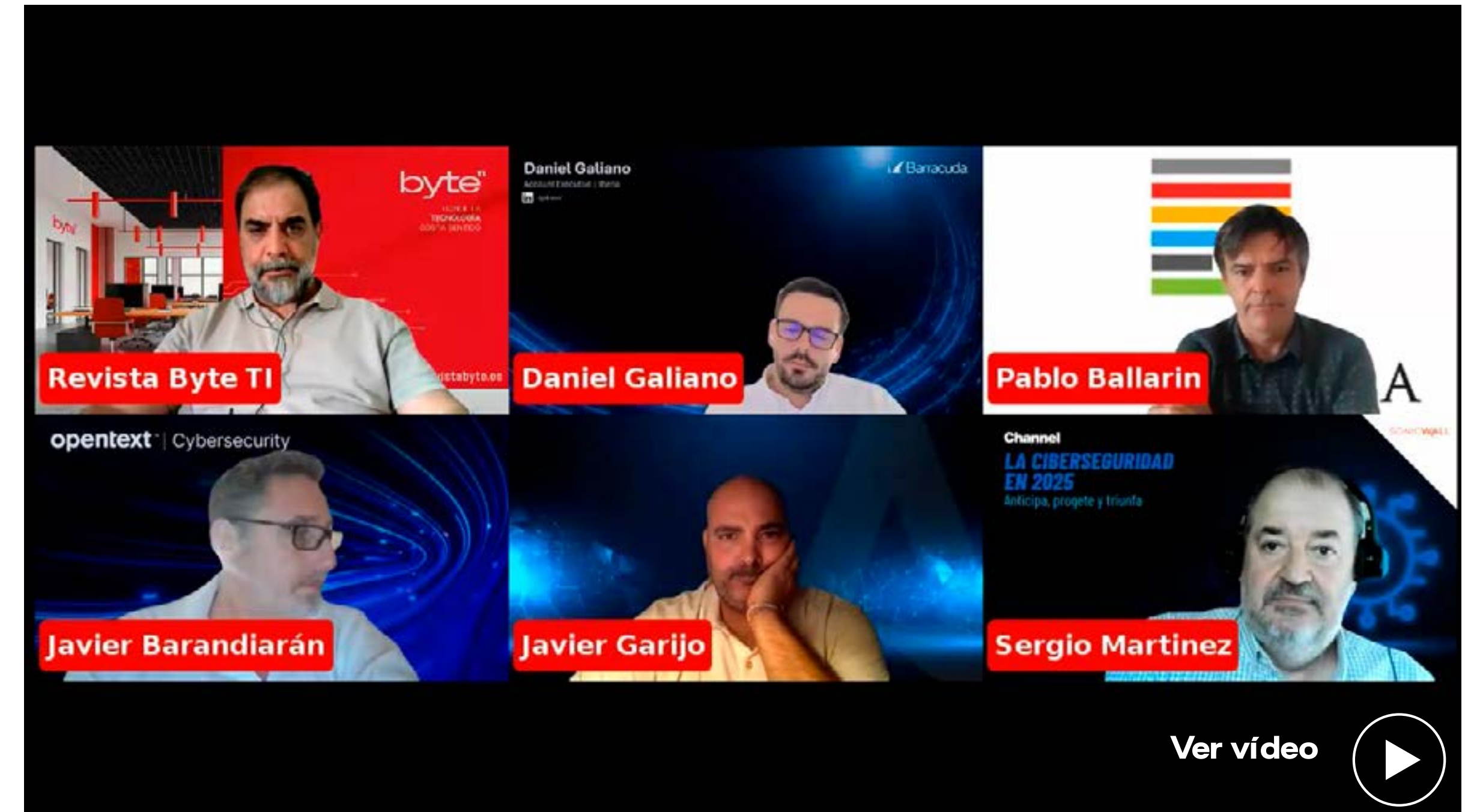
Finalmente, Antonio Gil de GVC Gaesco insistió en la importancia de la formación: "Formar a la gente en IA no es como formar en una nueva versión de software. Requiere un cambio de mentalidad y de procesos que solo es posible si la dirección empuja desde arriba".



Webinars BYTE TI

Cómo establecer una estrategia de prevención de ciberriesgos

Las empresas se enfrentan a una infinidad de ciberriesgos. Frente a este escenario, establecer una estrategia de prevención ya no es opcional, así que las organizaciones tienen que evolucionar los enfoques defensivos tradicionales. Para tratar sobre ello, Byte TI organizó un encuentro que contó con la participación de Sergio Martínez, Iberia Senior Regional Manager de Sonicwall; Pablo Ballarín de la Junta Directiva ISACA Valencia & Co-fundador de Balusian; Javier Barandiarán, CyberSecurity Partner Manager de Opentext; Javier Garijo, Head of Cybersecurity Consulting de VARGROUP y Daniel Galiano, Account Executive de Barracuda.



El encuentro comenzó estudiando qué metodologías y soluciones es necesario emplear para la detección proactiva de amenazas. Pablo Ballarín de la Junta Directiva ISACA Valencia & Co-fundador de Balusian, defendió la aplicación rigurosa de frameworks como el NIST por su "capacidad para integrar la ciberseguridad dentro de la gestión de negocio", insistiendo en que "la clave no está tanto en las herramientas aisladas, sino en cómo se engranan personas, procesos y tecnología con visión de conjunto".

Por su parte, Sergio Martínez, Senior Regional Manager Iberia de Sonicwall, fue aún más rotundo: "Todos tendremos un incidente antes o después; no hay que asustarse, pero sí

asumirlo". Para Martínez, la defensa en capas continúa siendo esencial ya que en su opinión, "desde hace años repetimos lo mismo porque no hay otra forma eficaz de protegerse. La conectividad crece, pero la ciberseguridad va a remolque". El directivo subrayó la importancia de la monitorización continua, ya que "el tiempo medio desde que aparece una brecha hasta su explotación es de 48 horas, y la mayor parte de los ataques se producen en la madrugada del viernes al sábado". Además, recalcó el desafío del parcheo: "Se tardan de media 120 días en parchear sistemas críticos, lo que expone a las empresas durante periodos prolongados".

El consenso fue claro respecto al valor de la normalización. Tal y como expuso Javier

Webinars BYTE TI

Cómo establecer una estrategia de prevención de ciberriesgos



Daniel Galiano,
Account Executive de
Barracuda



Javier Barandiarán,
CyberSecurity Partner
Manager de Opentext



Javier Garijo,
Head of Cybersecurity
Consulting de VARGROUP



Pablo Ballarín de la Junta
Directiva ISACA Valencia &
Co-fundador de Balusian



Sergio Martínez,
Iberia Senior Regional
Manager de Sonicwall

Barandiarán, CyberSecurity Partner Manager de Opentext, "es un error "reinventar la rueda" cuando los marcos regulatorios como NIS2 o DORA ya contemplan las metodologías más eficaces según cada contexto de negocio. El secreto está en definir procesos claros y contar con personas adecuadas, no solo productos".

Javier Garijo, Head of Cybersecurity Consulting en VARGROUP, remarcó que "cada compañía tiene su propio foco y debe adaptar la normativa a la especificidad de sus activos, priorizando la protección donde realmente importa". Por su parte, Daniel Galiano, Account Executive de Barracuda, cree que "la detección proactiva exige combinar inteligencia artificial, análisis de comportamiento y monitorización continua,

además de fomentar políticas de segmentación de red y control de accesos".

Estrategia de prevención de ciberriesgos

Uno de los bloques centrales abordó si las empresas españolas cuentan hoy con una estrategia sólida de prevención de ciberriesgos. Para Galiano, "muchas organizaciones confunden prevención con reacción. No basta con una auditoría anual; es imprescindible la formación continua del personal y disponer de backups efectivos y bien probados". Por su parte, el portavoz de VARGROUP observó una "brecha significativa entre empresas maduras y aquellas que, forzadas por la regulación, apenas empiezan a articular una estrategia integral". Mientras, que desde Opentext, Barandiarán advirtió que "la presión regulatoria está

activando el cambio, pero no se puede pedir al mismo equipo que ejecute tareas de protección de ciberriesgos y de detección-respuesta sin especialización".

En cuanto a los errores más graves al abordar la ciberseguridad, Ballarín fue tajante en señalar el exceso de fe en la tecnología sin respaldo de procesos y cultura. "El problema no es poner equipamiento nuevo, sino qué ocurre cuando no hay gente formada ni responsabilidades claras. Sin cultura de ciberseguridad, la mejor tecnología es ineficaz", sentenció el portavoz de Isaca.

Sergio Martínez de Sonicwall reforzó esta idea al asegurar que "pensar que nunca nos va a pasar nada es una trampa muy común. Por este motivo, la monitorización es fundamental; un entorno no

Webinars BYTE TI

Cómo establecer una estrategia de prevención de ciberriesgos

monitorizado es un caramelo para los atacantes. Además, se menosprecia el riesgo del phishing a través del correo, vector de entrada predominante en muchos incidentes recientes". En este aspecto, Javier Barandiarán añadió que "invertir solo en monitorización reactiva y no en medidas básicas, como la autenticación multifactor, es un error. Hay que priorizar según la criticidad del activo, no repartir recursos sin criterio".

El impacto de la IA en la prevención de ciberriesgos

Durante el encuentro se exploró el impacto que tiene la inteligencia artificial en la prevención de ciberriesgos. Daniel Galiano de Barracuda indicó que "la IA está revolucionando la prevención permitiendo detección en tiempo real y automatización de respuestas"; mientras que Garijo resaltó su valor para acortar los tiempos de análisis y toma de decisiones. En su opinión, "muchos fabricantes ya integran la IA de forma nativa, mejorando la efectividad de SIEM y XDR, aunque siempre deben intervenir personas para validar las alertas ya que la Inteligencia Artificial todavía no es infalible". En este sentido, Barandiarán aportó un matiz diferencial: "Hemos dado un salto incorporando IA generativa no solo para facilitar la remediación de vulnerabilidades, sino para reducir drásticamente los tiempos de resolución. Eso es clave en escenarios donde el coste humano es elevado".

Sin embargo, el panel coincidió en que los atacantes también se aprovechan de las ventajas que proporciona la IA. Así el portavoz de Opentext explicó que los ciberdelincuentes, "han automatizado la búsqueda y explotación de vulnerabilidades, encadenan exploits y desarrollan nuevas técnicas de evasión cada vez más sofisticadas. Además, juegan con ventaja, porque pueden probar y desplegar mejoras sin obstáculos regulatorios".

Pablo Ballarín recalcó la aparición de la IA como "nuevo vector de ataque dentro de la propia organización, obligando a una revisión adicional en aspectos éticos y de confianza", lo que ha impulsado nuevas capacitaciones específicas en ISACA.

El portavoz de Barracuda hizo hincapié también en que, a pesar de lo que muchos se piensan hay que confiar en la Inteligencia Artificial porque "la IA no viene a sustituirnos sino a potenciarnos. La detección automática de ransomware es cuestión de milisegundos, pero el juicio humano sigue siendo esencial para decidir cuándo y cómo actuar, especialmente en situaciones críticas".

Recomendaciones en la prevención de ciberriesgos

El debate concluyó con recomendaciones prácticas. Desde Isaca, Ballarín propuso a

las pymes "empezar por identificar procesos críticos y activos esenciales, contextualizando la seguridad en función del valor real para el negocio; la tecnología debe encajar en ese engranaje, no al revés".

Por su parte, Sergio Martínez resaltó el papel de los servicios gestionados de seguridad. Tal y como explicó, "ningún sistema es invulnerable. Lo esencial es poder responder y detectar rápido. En este aspecto, los servicios gestionados que tenemos en Sonicwall monitorizan toda la infraestructura, empleando IA y un SOC europeo que reacciona aunque el cliente esté inoperativo, mitigando las amenazas antes de que escalen".

Barandiarán ejemplificó el enfoque integrado de OpenText, con soluciones que "cuidan la gestión de identidades, control de acceso adaptativo y gestión documental segura, todo bajo el prisma de la protección y el valor del dato", mientras desde VARGROUP, Garijo subrayó el valor del diagnóstico previo: "Antes de invertir hay que analizar vulnerabilidades, cultura interna y el impacto de negocio; sólo así la inversión en ciberseguridad tiene sentido para la dirección".

El último bloque se centró en el futuro de la IA como aliada o amenaza.



Comparativa

4 soluciones de gestión de identidades

En la era de la digitalización, la gestión de identidades y accesos (IAM, por sus siglas en inglés) se ha consolidado como un pilar estratégico de la seguridad y la eficiencia empresarial. Según un estudio de la empresa de investigación de mercados Fortune Business Insights, el mercado global de IAM aumentará hasta los 61.740 millones de dólares en 2032, con una tasa de crecimiento anual del 15,3%; una importante expansión que refleja no solo la paulatina complejidad de los entornos digitales, sino la necesidad de soluciones que gestionen de manera segura las identidades digitales y los accesos a los sistemas críticos.

En paralelo, una investigación de Mandiant, compañía de ciberseguridad propiedad de Google, reveló que, el año pasado, el uso de credenciales sustraídas representó el 35% de los vectores de acceso inicial más frecuentes en los ciberataques, superando al phishing, que se situó en un 14%. Este dato subraya, por tanto, la creciente importancia de proteger las credenciales digitales dentro de la estrategia de ciberseguridad de las organizaciones.

Definición y claves

La finalidad de una solución de gestión de identidades y accesos es que la persona, dispositivo



Comparativa

o máquina correcta accedan a los recursos adecuados en el momento oportuno. Para lograrlo, IAM combina un conjunto de políticas, procesos y tecnologías para la creación, mantenimiento, modificación y eliminación de cuentas de usuario; la asignación de roles y permisos; la autenticación y verificación de identidades; y la monitorización y auditoría de accesos.

Estas soluciones IAM cumplen con diversas funciones estratégicas. En primer lugar, refuerzan la seguridad al reducir el riesgo de accesos no autorizados y brechas de datos, incorporando mecanismos como la autenticación multifactor, el inicio de sesión único, el acceso condicional y la gestión de accesos privilegiados. Además, facilitan el cumplimiento normativo, permitiendo auditorías detalladas y reportes precisos para regulaciones, lo que evita sanciones y ayuda a proteger la reputación corporativa.

Las soluciones IAM cumplen con diversas funciones. Sobre todo, refuerzan la seguridad al reducir el riesgo de accesos no autorizados y brechas de datos

Estas soluciones también optimizan la eficiencia operativa al automatizar procesos de alta, baja y modificación de usuarios, minimizando errores humanos y liberando recursos del departamento de TI. Al mismo tiempo, mejoran la experiencia del trabajador al facilitar accesos rápidos y seguros sin la necesidad de recordar múltiples contraseñas o credenciales complejas.

Capas complementarias

El ecosistema IAM no es homogéneo y se compone de varias capas complementarias. Por ejemplo, la gestión de identidades se centra en todo el ciclo de vida de las cuentas digitales, asegurando que los permisos y roles se ajusten al perfil y la función del usuario. La gestión de accesos define, por su parte, políticas de

4 soluciones de gestión de identidades

autorización basadas en roles, riesgos o atributos, aplicando tecnologías avanzadas como SSO y MFA. Mientras, el gobierno de la identidad establece la estrategia global del sistema IAM, supervisa el cumplimiento regulatorio, y realiza auditorías periódicas para garantizar la coherencia y seguridad de los accesos. Por último, la autenticación y autorización avanzadas incorporan biometría, modelos zero trust, autenticación adaptativa y gestión de privilegios, protegiendo a la organización frente a amenazas internas y externas. Los beneficios de IAM se materializan en sectores como educación, finanzas o salud, entre otros.



Comparativa

Cisco Duo Identity & Access Management (IAM)

Se trata de una solución integral de seguridad que transforma la manera en que las organizaciones protegen las identidades frente a las amenazas modernas potenciadas por la IA. Basada en una tecnología de autenticación multifactor, ofrece una protección contra el phishing y otros ataques de ingeniería social con un doble fin: mejorar la experiencia del trabajador y simplificar la administración de las TI.

En este contexto, Cisco responde a las vulnerabilidades críticas con un enfoque de zero trust que incorpora la seguridad por defecto, ayudando a las empresas a prevenir accesos no autorizados sin sacrificar la productividad. Hay que subrayar varias funcionalidades como un nuevo Directorio de Usuarios que facilita el almacenamiento centralizado de credenciales y roles, y que simplifica la gestión de accesos. Asimismo, la autenticación multifactor y el inicio de sesión único combinan seguridad y facilidad de uso, con un acceso simple a cientos de aplicaciones desde un único portal.

Por otro lado, para reforzar la protección frente al robo de credenciales y sesiones, los ingenieros de la norteamericana han integrado las siguientes innovaciones: Complete Passwordless, Proximity Verification y Session Theft Protection. La primera

suprime la necesidad de contraseñas, verificando la identidad del usuario con su huella, su rostro o un dispositivo de seguridad especial. Así, se reduce el riesgo de robo de credenciales y se simplifica el acceso, ya que no es necesario recordar ni gestionar contraseñas.

En el caso de Proximity Verification lo que se asegura es que los dispositivos móviles y de autenticación estén físicamente próximos; con esto se evita que los atacantes que están lejos accedan a las cuentas porque dicho acceso solo se garantiza si el usuario se encuentra físicamente cerca del dispositivo. Por último, Session Theft Protection elimina la dependencia de cookies del navegador, protegiendo frente al secuestro de sesiones. El sistema, en ese caso, emplea un token seguro que hace más difícil que los atacantes roben o tomen control de una sesión activa.

La apuesta por una integración flexible es otra característica a destacar: gracias a un nuevo motor de enrutamiento, Duo IAM se conecta fácilmente con sistemas de identidad de terceros, actuando como proveedor secundario o intermediario. Además, el asistente de IA de Cisco ayuda a las organizaciones empresariales en la implementación y la administración diarias.

4 soluciones de gestión de identidades



Duo IAM se integra, a su vez, con la solución Cisco Identity Intelligence, conectando datos de identidad y acceso en toda la Cisco Security Cloud.

Entre los beneficios, las compañías disfrutan de ventajas como la reducción de costes de gestión mediante un directorio centralizado e integración con sistemas de terceros. También la capacidad de adaptarse a negocios de todos los tamaños y sectores, y a lo que vendrá en el futuro que es la seguridad de identidades diseñada para la era de la inteligencia artificial.



Cisco



A consultar


www.cisco.com/c/es_es

www.cisco.com/c/es_es/about/contact-cisco.html

Comparativa

4 soluciones de gestión de identidades

CyberArk: Plataforma de Seguridad de la Identidad

La Plataforma de Seguridad de la Identidad de CyberArk permite una implementación escalable, protegiendo a las identidades a lo largo del ciclo de acceso en infraestructuras híbridas, SaaS y multinube. Diseñada como primera línea de defensa frente a ciberdelincuentes, accesos no autorizados, ciberataques y amenazas internas, aplica un enfoque zero trust que refuerza la seguridad desde el núcleo de la infraestructura.

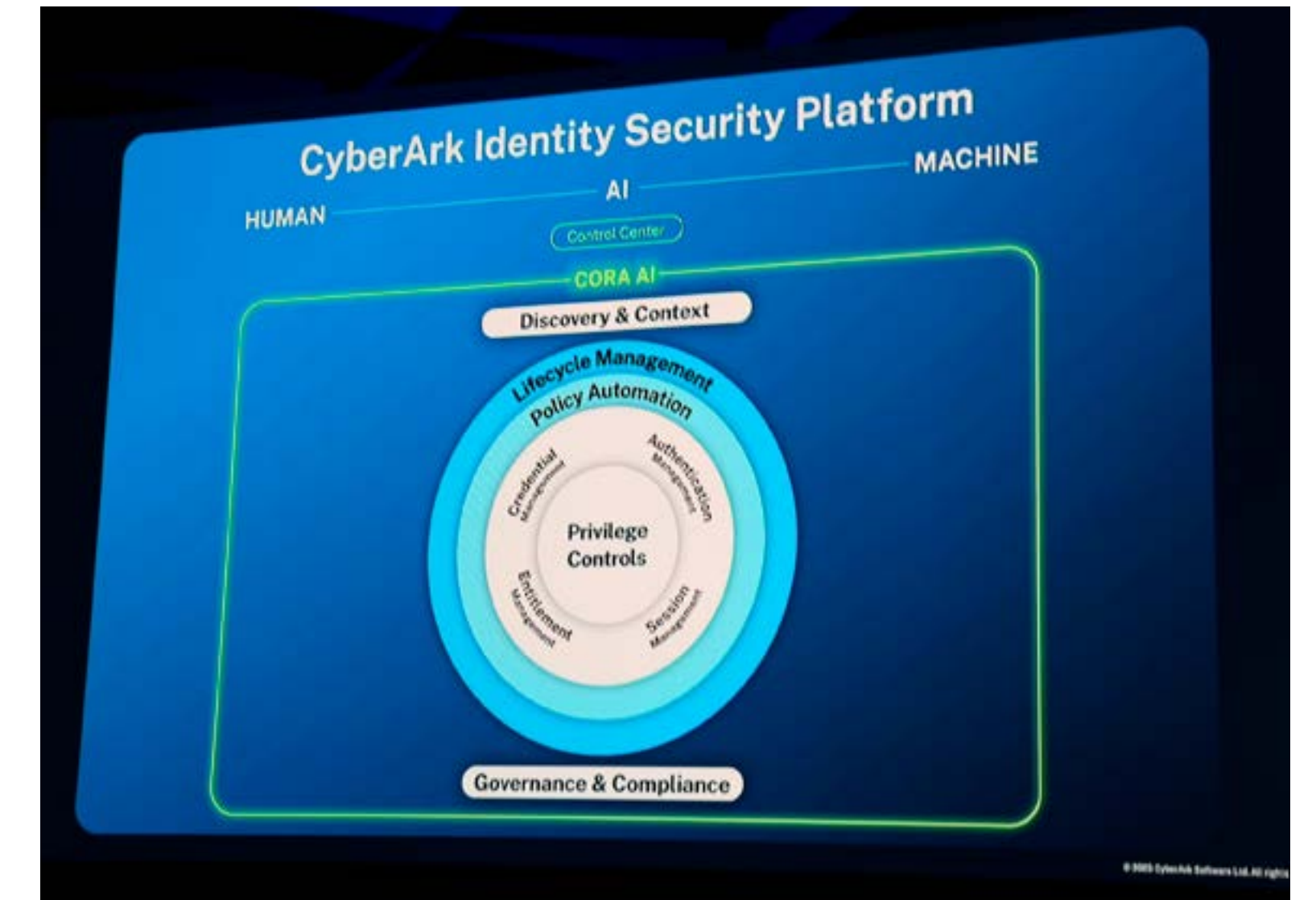
En este sentido, proporciona un acceso seguro y sin fricciones mediante tecnologías como SSO, MFA adaptativa, gestión del ciclo de vida de identidades, federación de directorios y análisis de comportamiento. Esto garantiza que los usuarios acceden a los recursos que necesitan sin comprometer la seguridad, desde cualquier dispositivo y ubicación. A su vez, ayuda a redefinir el concepto de privilegios, extendiéndolo más allá de los administradores tradicionales: lo hace aplicando controles granulares a cualquier identidad que requiera acceso elevado, ya sea permanente o just-in-time.; ello incluye empleados, proveedores externos, endpoints e identidades de máquina.

Asimismo, la automatización es clave en esta plataforma. Desde la incorporación de nuevos usuarios hasta la revocación de accesos, todo

el ciclo de vida de la identidad se gestiona de forma eficiente. La orquestación de accesos, la federación de servicios de directorio y la integración con herramientas de cumplimiento facilitan que las organizaciones operen con precisión, minimizando errores humanos y garantizando auditorías efectivas.

La propuesta de CyberArk se articula en torno a cinco módulos principales que permiten proteger de manera integral los entornos de TI empresariales. El primero es Endpoint Privilege Security, que elimina los derechos de administrador local en los endpoints para reducir la superficie de ataque y aplica el principio de mínimo privilegio adaptado a cada rol dentro de una compañía. Le sigue Privileged Access Management que protege credenciales y secretos con privilegios en toda la infraestructura de TI

El tercer módulo recibe el nombre de Secrets Management. Su cometido es asegurar el acceso a los recursos sensibles en entornos empresariales de TI, tanto internos como externos, y minimizar riesgos operativos mediante la centralización y automatización del manejo de secretos como claves API, tokens y contraseñas. Cloud Security (el cuarto) se



encarga de supervisar y de proteger los accesos en entornos en la nube, eliminando permisos excesivos y visualizando accesos de identidades humanas y de máquina. Además, refuerza la seguridad en consolas, CLI y servicios cloud, alineándose con principios de mínimo privilegio y zero trust. Finalmente se encuentra Identity Management que automatiza la gestión de identidades digitales en todos los entornos de TI empresariales; analiza de forma centralizada el acceso para dimensionar correctamente los permisos; y facilita la aplicación del principio de mínimo privilegio mediante una gestión eficiente del ciclo de vida de la identidad.

Comparativa

Microsoft Entra ID

El Gigante de Redmond, bajo el nombre de Entra, ha desarrollado una completa familia de productos de identidad y acceso a la red. En concreto, abarca la administración de identidades y accesos para personal, clientes e identidades no humanas; la gobernanza y protección de identidades; el uso de credenciales comprobables; y las soluciones básicas de acceso a la red para entornos SASE (Secure Access Service Edge).

En esta familia se encuentra Microsoft Entra ID: anteriormente Azure Active Directory, es un servicio de administración de identidades y acceso en la nube que proporciona la identidad, autenticación, directiva y protección necesarias para blindar trabajadores, dispositivos, aplicaciones y recursos. Entre sus capacidades integrales, destaca la integración de aplicaciones e inicio de sesión único, de modo que las organizaciones 'conecten' a su personal con las aplicaciones que necesitan desde cualquier ubicación y con cualquier dispositivo.

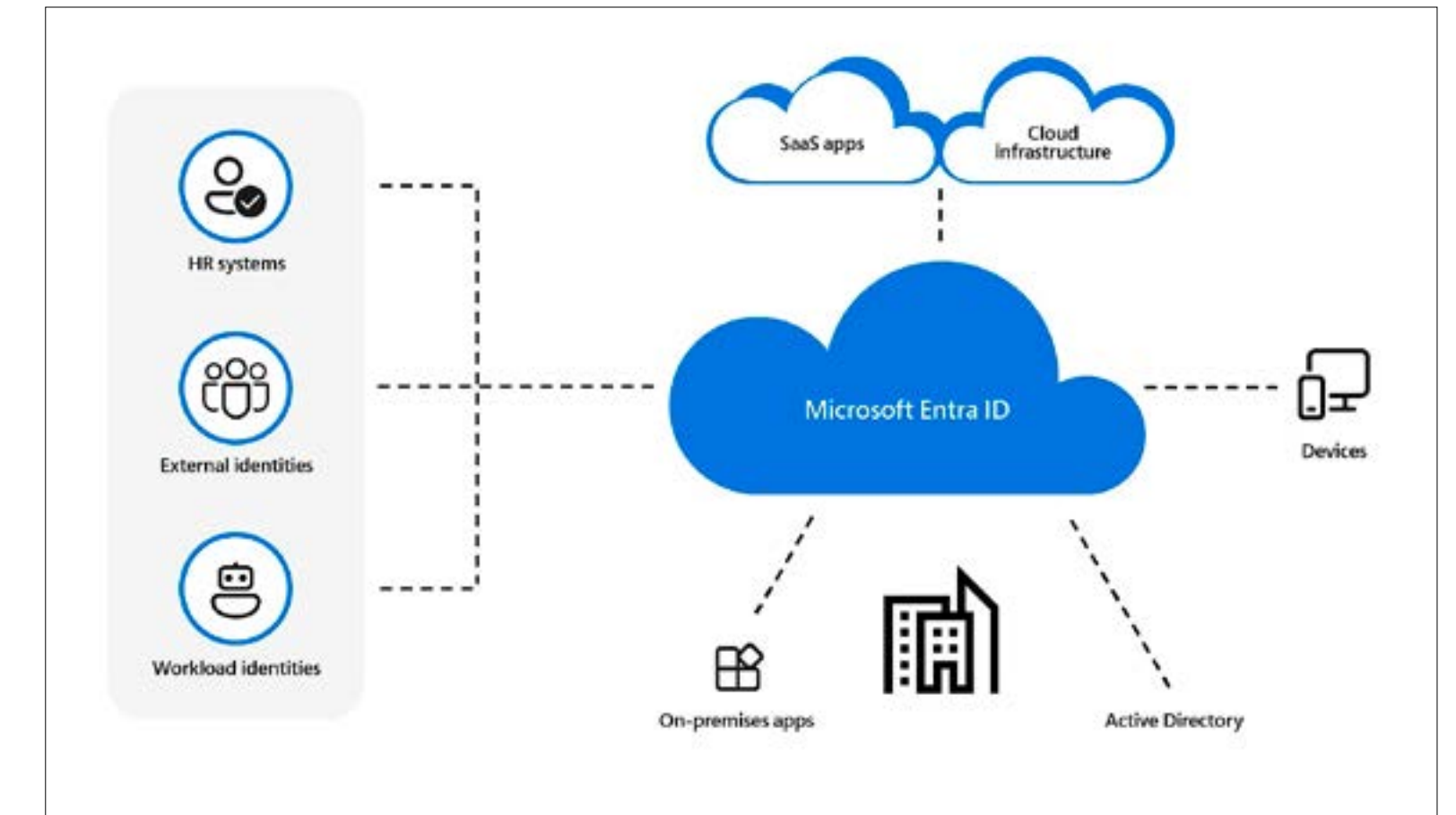
Sus características incluyen, asimismo, la autenticación multifactor y sin contraseña, junto al acceso condicional, que aplica los controles de acceso adecuados para reforzar la seguridad. Microsoft Entra ID protege, asimismo, las identidades y bloquea los ataques relacionados con accesos no autorizados en tiempo real,

garantizando que solo los usuarios legítimos acceden a los recursos de la organización. Además, refuerza la seguridad de las cuentas con privilegios mediante políticas estrictas y controles de acceso avanzados. Los empleados, incluso, gestionan su propia identidad gracias a portales de autoservicio como Mis aplicaciones, Mi acceso, Mi cuenta y Mis grupos, lo que reduce la carga de soporte técnico. Todo esto se administra por medio de un único centro unificado desde el que se controla las identidades y accesos en entornos multinube.

Microsoft ha incorporado a su estrategia Microsoft Security Copilot, una plataforma que reúne la eficacia de la IA y la experiencia humana para ayudar a los administradores y equipos de seguridad a responder a los ataques. Microsoft Entra es uno de los complementos que permiten a esta generar información precisa y relevante. A través de este complemento, Security Copilot investiga y resuelve riesgos de identidad, evalúa identidades y acceso con inteligencia controlada por IA, y completa tareas complejas. Recientemente, se ha anunciado que los agentes de Security Copilot estarán disponibles en toda su plataforma de seguridad end to end.

Entre los agentes disponibles están agente de triaje de Phishing en Microsoft Defender, que analiza

4 soluciones de gestión de identidades



alertas de phishing, identifica amenazas reales frente a falsas alarmas y proporciona explicaciones sobre sus decisiones; los agentes de triaje de Alertas de Microsoft Purview, que clasifican las alertas de prevención de pérdida de datos y riesgos internos y priorizan incidentes; el agente de optimización del Acceso Condicional de Microsoft Entra, que supervisa nuevos usuarios o aplicaciones no cubiertas por las políticas existentes; el agente de corrección de vulnerabilidades de Microsoft Intune, que supervisa y prioriza vulnerabilidades y tareas de remediación para solucionar problemas de configuración de aplicaciones y políticas; y el agente de Threat Intelligence de Security Copilot, que recopila información relevante sobre amenazas, basándose en los atributos únicos de cada organización y su exposición a riesgos.

Comparativa

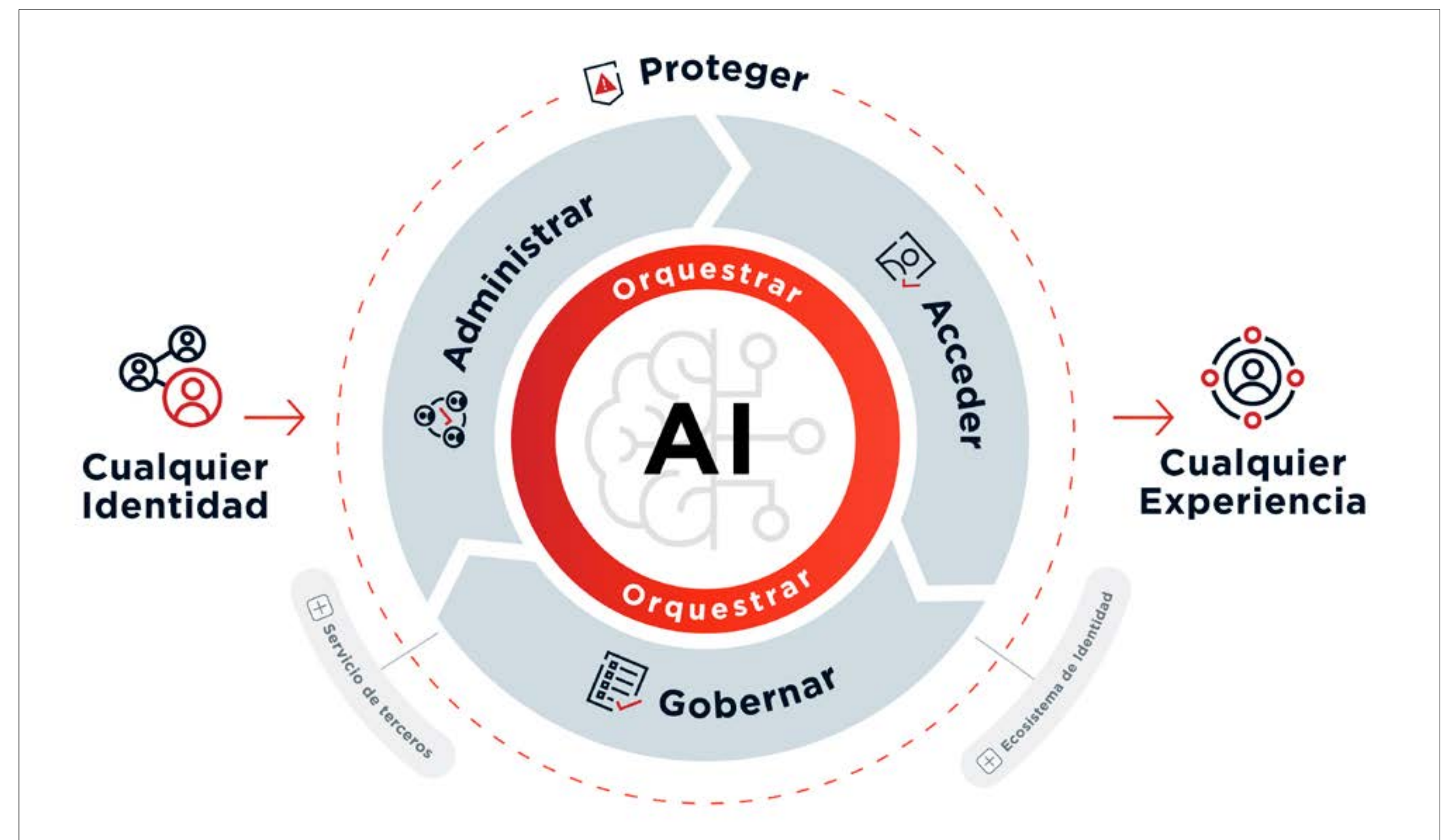
4 soluciones de gestión de identidades

Ping Identity

Con oficinas repartidas por todo el mundo, Ping Identity es una multinacional norteamericana que, desde sus primeros pasos en 2002, ha gestionado, según datos facilitados por la propia firma, más de 3.000 millones de identidades. Consciente que lo importante es asegurar experiencias de usuario que resulten fluidas y seguras, y que los clientes 'exigen' interacciones online coherentes, sin tediosos procesos de registro ni de contraseñas, participa en esta comparativa de la mano de su plataforma: lo hace para brindar una experiencia ágil y confiable para cualquier tipo de identidad, en cualquier caso de uso o entorno de implementación.

Las organizaciones empresariales interesadas tienen a su disposición una solución completa de gestión de identidades y accesos digitales basada en la inteligencia artificial que las ayuda no solo a gestionar todo el ciclo de vida. También a proporcionar un acceso seguro y a controlar cualquier clase de identidad. De este modo, y gracias a la ayuda de determinadas herramientas, tecnologías y prácticas, las empresas logran un equilibrio entre ofrecer un servicio fácil y agradable de usar y, al mismo tiempo, garantizar que tanto los usuarios como la propia organización están protegidos frente a riesgos o amenazas.

Con la plataforma Ping Identity, estas compañías pueden, en otro orden de cosas, migrar de integraciones complejas de productos puntuales a una arquitectura optimizada. De la misma manera, puede implementarse para cientos o millones de identidades en cualquier entorno de TI con un triple objetivo: reforzar la seguridad, profundizar en las relaciones con los clientes, e incrementar la productividad de los empleados y los socios.



Características clave

Uno de sus pilares fundamentales de la plataforma que estamos 'desgranando' es la orquestación de experiencias de usuario, que permite a las organizaciones diseñar interacciones seguras y sin interrupciones. En este caso, además, su enfoque no-code/low-code ayuda a que los equipos de trabajo creen flujos personalizados de autenticación y acceso sin necesidad de escribir grandes cantidades de código: en la práctica del día a día esto va a reducir la complejidad del desarrollo y acelerar la implementación de soluciones de identidad. Esta orquestación facilitada por la propia plataforma es la que se muestra por otro lado, como un marco de integración flexible y adaptable para diseñar flujos de trabajo automatizados enfocados a diferentes casos de uso de identidad, incluida la autenticación, la verificación de identidad y la detección de fraudes.

Comparativa

Otro aspecto clave de Ping Identity es la gestión del ciclo de vida que hace posible otorgar el acceso adecuado en el momento preciso. Dentro de este contexto, y dado que los datos de identidades evolucionan con el paso del tiempo (desde un cliente con una nueva dirección de correo electrónico hasta un empleado que cambia de puesto laboral), esta gestión del ciclo de vida garantiza que los atributos de identidad actualizados sean incorporados u obtenidos de los sistemas necesarios a fin de asegurar una experiencia de acceso seguro, simple y continuo.

Mientras tanto, la gestión de relaciones se muestra como un componente esencial para que una empresa se encuentre preparada para afrontar y adaptarse a las necesidades cambiantes del negocio por medio de modelos de datos de identidad flexibles. Y es que el poder de la identidad reside precisamente en estas relaciones: al igual que se crean varias pestañas en planillas y se emplean tablas dinámicas para organizar información de manera eficiente, la gestión de relaciones permite vincular diferentes tipos de datos de identidad entre sí. Esto facilita la creación de tablas dinámicas ad-hoc que generan combinaciones únicas de información, sin necesidad de concentrarlo todo en una sola pestaña. De este modo, la plataforma no solo organiza los datos de manera lógica y escalable, sino que ofrece asimismo la

flexibilidad necesaria para analizar y emplear la información adaptándose a las necesidades de cada negocio.

Cabe señalar, por otro lado, que los usuarios cuentan con una gestión de credenciales digitales para crear, emitir y administrar credenciales verificables y reutilizables desde un portal SaaS centralizado. En la práctica, los proveedores de servicios y las partes de confianza verifican al instante la autenticidad, la exactitud de la emisión y la integridad de los datos en el momento que se presentan.

La plataforma Ping Identity le concede a las organizaciones la capacidad de gestionar de forma segura los datos de identidad y los perfiles de los usuarios a gran escala, asegurando que la información crítica esté protegida y organizada de manera eficiente, incluso cuando se trata de miles o millones de usuarios. Complementando esta gestión, el inicio de sesión único (SSO) es el que ayudará a los usuarios a acceder a múltiples aplicaciones y recursos con un solo identificador, simplificando la experiencia de uso y reduciendo la necesidad de recordar múltiples contraseñas. Para reforzar la seguridad, Ping Identity incorpora de la misma manera autenticación multifactor y sin contraseña, garantizando que estos usuarios son realmente quienes dicen ser a través de métodos de verificación adicionales como la biometría o las notificaciones en dispositivos confiables.

4 soluciones de gestión de identidades

Sus características incluyen también la protección contra las amenazas (el objetivo es detectar el fraude y responder con una visibilidad de los vectores de ataque, la telemetría de sesión y el comportamiento de los usuarios), y la verificación de identidad que es la que confirma la identidad real de un usuario durante el registro y posteriormente.

Con solicitudes de acceso sencillas y autoservicio para recortar los costes del servicio de asistencia técnica, la plataforma promete una revisión eficaz y rápida del acceso de los usuarios, así como la segregación de funciones para implementar políticas de acceso con privilegios mínimos. En lo que autorizaciones se refiere, las empresas tienen la capacidad de gestionar de manera centralizada el acceso a aplicaciones, API y datos. Estas autorizaciones implican, entre otros, el control de acceso del contexto para datos; servicios y transacciones; experiencias personalizadas con una mejor gestión de la privacidad y el consentimiento de los datos; controles centralizados y visibilidad de las políticas de autorización en toda la compañía; y orquestación rápida sin código o con apenas código de los flujos y recorridos de autorización.



Ping Identity


sales@pingidentity.com

www.pingidentity.com/es


A consultar

Comparativa

Conclusiones

Cisco, CyberArk, Microsoft y Ping Identity son las firmas que han participado en la comparativa de este mes, soluciones de gestión de identidades. En este caso, y teniendo en cuenta el panorama actual de la gestión de identidades y accesos, donde la seguridad y la experiencia de usuario deben coexistir sin fricciones, las soluciones disponibles en el mercado sugieren diferentes enfoques y ventajas competitivas. Las cuatro propuestas que se han descrito son alternativas interesantes para cualquier negocio, pero hay dos de ellas que, en nuestra

opinión, sobresalen ligeramente sobre el resto: la plataforma Ping Identity y Cisco Duo Identity & Access Management (IAM).

Ping Identity destaca por su capacidad de orquestación con flujos no-code/low-code que facilitan la creación de experiencias seguras y fluidas, además de su gestión flexible de datos de identidad; la administración del ciclo de vida de los usuarios; y la emisión centralizada de credenciales digitales verificables. Por su parte, Cisco aporta la robustez de su ecosistema de seguridad, integrando identidad con sus reconocidas capacidades de protección de red,

4 soluciones de gestión de identidades

detección de amenazas y escalabilidad global, lo que refuerza la confianza y garantiza una defensa integral frente a riesgos crecientes.

Ahora bien, no debe pasarse por alto que las otras dos plataformas analizadas también representan propuestas de gran valor para el mundo empresarial. CyberArk es referente en la gestión de accesos privilegiados, asegurando el control de cuentas críticas y minimizando el riesgo de uso indebido en entornos complejos. Microsoft con Entra ha desarrollado una completa e importante familia de productos de soluciones de identidad y acceso a la red donde destaca Entra ID.

ASPECTOS DESTACADOS				
Nombre de la solución	Cisco Duo Identity & Access	CyberArk: Plataforma de Seguridad de la Identidad	Microsot Entra ID	Ping Identity
Valoración	★★★★★	★★★★★	★★★★★	★★★★★
Características clave	* Nuevo Directorio de Usuarios: facilita el almacenamiento centralizado de credenciales y roles, y simplifica la gestión de accesos. * MFA y SSO avanzados: combinan seguridad y facilidad de uso, con acceso simple a cientos de aplicaciones desde un único portal. * Innovaciones como Complete Passwordless, Proximity Verification y Session Theft Protection refuerzan la protección frente al robo de credenciales y sesiones. * Gracias a un nuevo motor de enrutamiento, se conecta con sistemas de identidad de terceros, actuando como proveedor secundario o intermediario. * IA aplicada a la gestión.	* Aplica tecnologías como la gestión del ciclo de vida de identidades, la federación de directorios y el análisis de comportamiento. * Identity Management: automatiza la gestión de identidades digitales en todos los entornos de TI empresariales. * Cloud Security: supervisa y protege accesos en entornos en la nube, eliminando permisos excesivos y visualizando accesos de identidades humanas y de máquina. * Endpoint Privilege Security: elimina los derechos de administrador local en los endpoints para reducir la superficie de ataque. * Privileged Access Management: protege credenciales y secretos con privilegios en toda la infraestructura de TI.	* Microsoft Entra es el nombre de una familia de productos de soluciones de identidad y acceso a la red. Uno de los productos de esta familia es Entra ID. * La familia de productos Microsoft Entra abarca cuatro fases del acceso seguro de un extremo a otro para cualquier identidad de confianza. Estas fases incluyen el establecimiento de controles de acceso de confianza cero y la protección del acceso para empleados, clientes, asociados y cualquier entorno en la nube. * Entra ID: integración de aplicaciones e inicio de sesión único, autenticación multifactor y sin contraseña, centro de administración unificada, autoservicio del usuario final... * Protege el acceso de los empleados a aplicaciones y recursos en cualquier nube o entorno local.	* Se trata de una solución integral de gestión de identidades y accesos digitales basada en IA que permite a las empresas estionar todo el ciclo de vida, proporcionar un acceso seguro y controlar cualquier identidad. * Se puede implementar para cientos o millones de identidades en cualquier entorno de TI. * Segregación de funciones. Opción de implementar políticas de cceso con privilegios mínimos. * Gestionar de forma centralizada el acceso a aplicaciones, API y datos. * Creación, emisión y gestión de credenciales digitales verificables y reutilizables desde un único lugar.

Gestión de identidades: el nuevo perímetro de la ciberseguridad empresarial

Por VANESA GARCÍA

La gestión de identidades es uno de los grandes ejes de la ciberseguridad. La realidad es la siguiente: la multiplicación de servicios en la nube, el auge del teletrabajo y la proliferación de identidades digitales están transformado por completo el perímetro de las organizaciones. Lo que se traduce en que, los sistemas tradicionales de control de accesos resultan insuficientes, y las compañías se ven obligadas a evolucionar hacia modelos más avanzados y centralizados.



Portada

Según Gartner, para 2026 más del 70% de las organizaciones habrán centralizado la gestión de accesos en soluciones IAM (Identity and Access Management), lo que refleja que el mercado está en plena transición hacia la madurez. Sin embargo, todavía tienen que enfrentarse al reto de la fragmentación de sistemas y a la complejidad de las infraestructuras digitales.

En opinión de Ángel Núñez Simón, responsable de Identidad Digital de Accenture en España y Portugal, la estrategia actual "podría calificarse como en transición hacia la madurez", aunque aún existen carencias en la automatización del ciclo de vida de las identidades y en el control de credenciales no humanas.

Carla Roncato, vicepresidenta de Identidad de WatchGuard Technologies, coincide al afirmar que las compañías que se apoyan en zero trust avanzan más rápido: "Las que han adoptado este enfoque reducen la superficie de ataque y habilitan experiencias seguras en cualquier lugar y momento, frente a aquellas que mantienen marcos de seguridad perimetral".

Por su parte, Álvaro Fernández, director de ventas en Iberia de Sophos, advierte de que todavía hay demasiados enfoques fragmentados. A su juicio, la mejora pasa por "consolidar la visibilidad y aplicar políticas consistentes en todo el ciclo de vida IAM, especialmente en entornos híbridos y multicloud".

Gestión de identidades

En esta misma línea, Alfonso Ríos, Global Head of Digital Identity Solutions Business Development en Minsait, recuerda que muchas estrategias siguen a medio camino: "En general, las organizaciones cuentan con estrategias de gestión de identidades en desarrollo o implementadas parcialmente, lo que indica un nivel de madurez medio o bajo". El portavoz subraya que la automatización de altas y bajas de usuarios, la adopción generalizada de MFA y la simplificación de accesos mediante SSO siguen siendo grandes asignaturas pendientes

Y es que, aunque las empresas reconocen la importancia estratégica de la gestión de identidades, su estrategia actual es todavía reactiva y en una fase de transición compleja",



“ Para el año que viene más del 70% de las organizaciones habrán centralizado la gestión de accesos en soluciones de identidad y gestión de accesos

Portada

añade Ángel Serrano, Senior Manager en Palo Alto Networks. Pues, la fragmentación derivada de entornos multicloud dificulta la aplicación de políticas coherentes y rompe con el principio de mínimo privilegio, advierte.

La gestión de identidades como prioridad estratégica en ciberseguridad

La identidad digital se ha convertido en el nuevo perímetro de la seguridad empresarial. Un informe de Cybersecurity Ventures revela que los ataques basados en credenciales representan la principal vía de entrada en el 60% de las brechas de datos, lo que explica que cada vez más compañías consideren la gestión de identidades como un pilar estratégico.

Tal y como subraya Núñez, "para preservar la seguridad de una empresa es fundamental contar con un riguroso control de accesos", recordando además que normativas como NIS2, DORA o el propio RGPD han sido un motor clave en la adopción de soluciones IAM.

Por otro lado, Roncato recalca que "los ataques basados en credenciales representan el riesgo más grande, continuo y significativo para las empresas en los últimos 15 años". A su juicio, resulta imprescindible que las organizaciones revisen de forma constante su postura de riesgo e incorporen monitorización continua.

“En la actualidad, los ataques basados en credenciales representan la principal vía de entrada en el 60% de las brechas de datos de las empresas

Desde la visión de Fernández, "la gestión de identidades ya es uno de los pilares de la ciberseguridad". Advierte de que la rápida migración a la nube y la proliferación de APIs han multiplicado los permisos innecesarios o mal configurados, lo que obliga a las compañías a apoyarse en un marco sólido y coherente de gestión de accesos.

A esta valoración se suma Ríos, incidiendo en que "la mayoría de las brechas de seguridad actuales están relacionadas con identidades comprometidas". La transformación digital, la generalización del trabajo remoto, la presión normativa y la necesidad de garantizar experiencias seguras han situado la gestión de identidades como "una base imprescindible en cualquier estrategia moderna de ciberseguridad".

Gestión de identidades

Serrano pone el acento en que la dispersión de datos y aplicaciones, junto con el auge del trabajo híbrido, ha hecho que IAM se consolide como una prioridad ineludible. "La identidad digital se ha convertido en el nuevo perímetro sobre el que se construyen tanto la seguridad moderna como la habilitación del negocio digital", concluye.

Robo de credenciales y suplantación de identidad: la primera causa de filtraciones

La suplantación de identidad continúa siendo la causa más frecuente de filtraciones de datos. Ante este panorama, las empresas han reforzado los mecanismos de autenticación y detección de amenazas.

"Las compañías han adoptado medidas orientadas a reducir la dependencia de contraseñas tradicionales y aplicar controles adicionales de verificación", explican desde Accenture. Entre ellas, mecanismos de MFA resistentes al phishing, tecnologías passwordless y planes de concienciación dirigidos a empleados.

Sin embargo, como advierten desde WatchGuard, la respuesta no siempre es proactiva: "En general, las empresas desconocen los factores de riesgo hasta que un enlace de phishing es clicado o se detecta un ataque de fuerza bruta".

Portada



Gestión de identidades

Sophos apunta que MFA, SSO y detección de anomalías de inicio de sesión ya se están combinando con análisis de comportamiento en tiempo real, aplicando además el principio de privilegios mínimos.

Centralización y gobierno de identidades: del modelo fragmentado al descentralizado

La consultora Forrester señala que el 45% de los incidentes de acceso indebido se deben a duplicaciones e inconsistencias entre sistemas de identidad. Estos datos evidencian la necesidad de un gobierno unificado.

Sobre este punto, Núñez resalta la importancia de estándares como SAML, OAuth2 o OpenID Connect, que facilitan la federación de identidades. "La automatización del ciclo de vida y los modelos basados en roles han dotado de robustez al gobierno de identidades".

De forma complementaria, Roncato explica que los sistemas modernos tienden a ser descentralizados para minimizar el riesgo de un único punto de fallo. "La resolución de entidades es el proceso de eliminar duplicados y verificar qué identidad es la auténtica", explica.

Para Javier San Juan, Blockchain Technology Sales Head de Var Group España, el futuro

pasa por un esquema descentralizado (SSI), donde cada persona disponga de una identidad única y verificable. Cita como ejemplo proyectos en Ceuta o Andorra que ya permiten a los ciudadanos controlar sus credenciales y revocarlas cuando lo deseen.

En palabras de Fernández, los conectores nativos hacia aplicaciones SaaS y los directorios unificados han permitido "una mayor estandarización y reducción de silos", avanzando hacia un gobierno más coherente.

Automatización del ciclo de vida de las identidades: del aprovisionamiento al Just-In-Time

Un informe de Deloitte estima que el 60% de las brechas de seguridad ligadas a identidades están relacionadas con errores en la gestión manual de permisos y cuentas. La automatización del ciclo de vida de las identidades (ILM) se consolida así, como un requisito indispensable.

Para Ángel Núñez de Accenture, la clave es integrar estas plataformas con RR. HH. y directorios corporativos para aprovisionar y desaproveccionar cuentas de manera automática, reduciendo riesgos de error humano. "El acceso Just-In-Time ha supuesto un avance significativo, ya que permite accesos temporales,

Gestión de identidades

limitados y bajo demanda, solo cuando son necesarios y por el tiempo estrictamente requerido”, afirma.

En palabras del portavoz de WatchGuard, el acceso Just-In-Time y el modelo Just Enough Access son ya los dos principios clave en la gobernanza moderna, eliminando privilegios permanentes. Fernández de Sophos coincide y recalca que estos modelos “aportan un valor crítico al permitir accesos temporales, auditables y limitados en alcance”.

También Ángel Serrano de Palo Alto Networks, recuerda que la automatización ha pasado de ser aspiración a capacidad esencial: “El aprovisionamiento y desprovisionamiento mediante estándares como SCIM y APIs garantiza que los accesos se actualicen de forma sincronizada en todas las aplicaciones, evitando cuentas huérfanas”.

Alfonso Ríos, Global Head of Digital Identity Solutions Business Development en Minsait, alerta de que muchas estrategias aún carecen de automatización plena en provisión y revocación, lo que “genera errores humanos y ralentiza procesos”.

Identidades no humanas: un reto que ya supera a las humanas

Según Gartner, para 2026 las identidades máquina (APIs, bots, certificados, servicios

en la nube) superarán en más del doble a las humanas. Esta proliferación plantea un reto urgente en seguridad y gobierno. “Uno de los grandes riesgos es que persistan credenciales estáticas embebidas en código, tokens sin caducidad o contraseñas por defecto”, advierten desde Accenture, que recuerda la necesidad de rotación y control centralizado.

Por otro lado, en WatchGuard, Roncato

señala que muchas empresas aún confían en herramientas pensadas para usuarios humanos, que no sirven para identidades dinámicas y efímeras. Siguiendo este esquema, en opinión de la compañía Sophos, la estrategia adecuada pasa por aplicar los mismos principios Zero Trust a identidades máquina, con vaults de secretos y rotación automática de claves.

Coinciden en Minsait Cyber que, “la clave

“Para 2026, las identidades máquina superarán en más del doble a las identidades de los humanos



Portada

de todo está en inventariar las identidades no humanas, aplicar gobernanza unificada, automatizar la gestión y aplicar principios de Zero Trust”.

Desde Palo Alto Networks añaden que la gestión de accesos privilegiados (PAM) será el gran diferencial: “IAM establece las bases, pero PAM garantiza el control real de accesos sensibles, especialmente en agentes de IA y entornos multicloud”.

Seguridad y experiencia de usuario: un equilibrio posible

Datos de McKinsey muestran que el 70% de

los usuarios abandona un servicio digital si el proceso de autenticación es demasiado complejo. El desafío está en equilibrar seguridad robusta con accesos ágiles.

Para Núñez, el futuro se basa en “una seguridad contextual, automatizada y transparente, donde el usuario apenas note que está siendo protegido”. En esta misma línea, Roncato defiende el uso de passkeys: “son resistentes al phishing y preservan la privacidad, simplificando el inicio de sesión en múltiples plataformas”.

San Juan pone ejemplos prácticos de cómo en Ceuta y Andorra se eliminan contraseñas, validando identidad con un simple QR. Ríos

añade que MFA adaptativo, SSO y autenticación biométrica son claves para ofrecer accesos intuitivos y fluidos sin renunciar a la seguridad. Mientras que Serrano subraya que el equilibrio se logra convirtiendo la seguridad en “un facilitador dinámico e inteligente, no en una barrera estática”.

Inteligencia artificial y analítica: la nueva guardia de la identidad

El auge de la IA está transformando la gestión de identidades. Según IDC, el 80% de las empresas planea usar IA para monitorizar accesos y detectar anomalías antes de 2026.

“

Según la consultora McKinsey hasta un 70% de los usuarios abandona un servicio digital si el proceso tiene demasiada complejidad



Portada

Gestión de identidades



El representante de Accenture resalta que la IA analiza patrones en tiempo real y puede bloquear cuentas o generar alertas ante actividades sospechosas. Por su parte el portavoz de WatchGuard observa que técnicas de machine learning ya ayudan en ITDR y en la evaluación de riesgos.

El director de ventas en Iberia de Sophos asegura que "la IA permite detectar accesos atípicos y ajustar políticas en tiempo real, reforzando la protección sin incrementar la carga administrativa".

Además, la IA convierte modelos estáticos en dinámicos: "pasa de un modelo reactivo a uno proactivo y adaptativo, detectando amenazas antes de que ocurran", incide Ríos. Lo mismo opina Serrano al resaltar que la IA es ya "aliado un indispensable", capaz de aprender el comportamiento habitual de cada identidad y descubrir desviaciones que indicarían riesgo interno.

Cumplimiento normativo y privacidad: regulaciones que marcan el camino

El RGPD, la directiva NIS2 y la inminente eIDAS2 han elevado la exigencia en materia de identidades. Las organizaciones ya no solo deben asegurar accesos, sino también garantizar derechos y demostrar cumplimiento



Las empresas deben adaptarse a normativas que obligan a pedir consentimiento explícito y garantizar derechos como el de acceso o eliminación

en auditorías. "Las organizaciones deben adaptarse a normativas que obligan a pedir consentimiento explícito y garantizar derechos como el de acceso o eliminación", apuntan desde Accenture. Roncato, de WatchGuard recuerda que el enfoque debe ser "privacy & security by design, con evidencias en tiempo real que permitan demostrar cumplimiento continuo".

Finalmente, el portavoz de VarGroup enfatiza que blockchain asegura "inmutabilidad y trazabilidad, facilitando la auditoría y reforzando la confianza", mientras que Ríos de Minsait) detalla que las medidas clave incluyen consentimiento informado, minimización de datos, logs de acceso y evaluaciones de impacto de privacidad.



Mujeres TIC

Sandra Gibert

CEO Intelcia Spanish Region



Fecha de nacimiento: 18 de enero de 1970

Hijos: 3 hijos

Aficiones: viajar, leer, decoración

Formación: Licenciada en Administración y Dirección de Empresas por ICADE (Universidad Pontificia Comillas). Ha completado su formación con programas ejecutivos en escuelas de primer nivel, como el Programa de Dirección General (PDG) del IESE Business School. Además, cuenta con una certificación en Buen Gobierno de Sociedades por el Instituto de Consejeros-Administradores (IC-A), centrada en sostenibilidad, estrategia y funciones del consejo.

¿Cómo llegó al mundo TIC?

A través de la práctica diaria en la gestión de operaciones con clientes. Nuestro negocio es mucho más tecnológico de lo que parece a simple vista: se sustenta en tres pilares clave —personas, tecnología y procesos—, por lo que inevitablemente terminas adentrándote en el mundo de la tecnología aplicada a la atención al cliente. Desde lo más básico, como las centralitas telefónicas y los sistemas CTI, que permiten gestionar y priorizar de forma inteligente las interacciones; hasta los CRM, que ayudan a conocer mejor al cliente y adaptarse a sus necesidades. Actualmente trabajamos con soluciones avanzadas de automatización, digitalización, RPA, análisis del habla, biometría de voz y múltiples aplicaciones de IA que usamos de forma real y cotidiana, tanto empleados como clientes. Es un entorno absolutamente tecnológico que tiene como objetivo facilitar el trabajo de las personas para ofrecer un mejor servicio.

¿Qué es lo que más valora de su trabajo?

Valoro especialmente la posibilidad de generar un impacto real en las personas y de contribuir a la transformación del sector BPO y de las compañías que confían en nosotros. El área de atención al cliente está orientada a mejorar la relación entre las empresas y sus usuarios, lo que tiene un efecto positivo sobre miles de consumidores cada día.

Liderar una compañía como Intelcia me da la oportunidad de impulsar el talento y la profesionalización en los contact center, fomentar la innovación en el punto en que convergen tecnología y experiencia humana, y crear entornos dinámicos y motivadores donde cada persona pueda desarrollarse plenamente.

Me motiva especialmente comprobar cómo nuestras decisiones estratégicas se traducen en oportunidades reales de crecimiento profesional para nuestros equipos y en soluciones eficaces para nuestros clientes.

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

Mujeres TIC

Es un problema multifactorial que empieza desde edades muy tempranas. Aunque los sesgos de género están desapareciendo progresivamente, aún persisten estereotipos culturales muy arraigados que pueden influir en que muchas mujeres no se planteen carreras STEM como una opción.

Es fundamental trabajar esta cuestión desde la educación, tanto en colegios como en universidades, visibilizando referentes femeninos en ámbitos científicos y tecnológicos para que la igualdad se integre como algo natural. En los últimos años se ha avanzado mucho en esta narrativa, logrando romper poco a poco con patrones tradicionales.

Las empresas también jugamos un papel clave, promoviendo programas de mentoring, formación y desarrollo profesional que ayuden a crear una cultura que valore el trabajo y el talento sin etiquetas.

¿Cree que existe el "techo de cristal" en las empresas TIC? ¿Cuál debería ser la solución?
Está más que demostrado que las capacidades profesionales y de liderazgo no dependen del género. Tampoco deberían verse condicionadas por la forma de ser o de gestionar situaciones complejas. La solución pasa por un compromiso firme y sostenido con la igualdad de oportunidades. Un compromiso que impregne todos los niveles



Se necesita un compromiso activo desde la alta dirección para garantizar la igualdad de oportunidades aplicando políticas de selección equitativas

de la organización, fomentando una cultura empresarial que entienda esa igualdad como una fortaleza y un activo estratégico.

¿Una política de cuotas puede resolver el problema?

En su momento, las cuotas sirvieron para visibilizar una realidad que muchas mujeres afrontaban: la dificultad para desarrollar su carrera profesional en igualdad de condiciones y sin sesgos.

Hoy el reto es distinto. Se necesita un compromiso activo desde la alta dirección para garantizar la igualdad de oportunidades, aplicando políticas de selección equitativas, planes de desarrollo profesional y evaluando a las personas por su desempeño y potencial, no por otras cuestiones.

En el comité directivo de Intelcia, más del 70 % son mujeres —seis de nueve personas—. No por

Sandra Gibert, CEO Intelcia Spanish Region

el hecho de serlo, sino porque han demostrado ser las mejores en su área y cuentan con mi total confianza.

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

En lo profesional, dentro de la compañía, no encontré ninguna. Siempre se ha valorado la capacidad y el aporte de valor de cada persona por encima de cualquier otra circunstancia.

Lo que sí he vivido son barreras personales, que una misma se impone: decidir si quieres o no asumir ciertas responsabilidades, lo que dejas atrás a nivel familiar, cómo te organizas en casa, cómo superas las críticas o juicios del entorno que cuestionan tus decisiones. En muchas ocasiones se interpreta que priorizas la ambición o el trabajo por encima de la familia.

En mi caso, esas decisiones se fueron tomando de forma natural, sin prejuicios. Trabajo, me esfuerzo porque es mi forma de entender la vida, y eso me ha permitido avanzar. También he tenido la suerte de contar siempre con el apoyo incondicional de mi familia, de mi marido y mis hijos.

¿Qué es lo que más valora de su empresa con respecto al desarrollo profesional de la mujer?

Sin duda, el liderazgo enfocado en el bienestar colectivo y la igualdad de oportunidades. Y cuando hablo de igualdad, me refiero a

Mujeres TIC

cualquier aspecto: género, edad, nacionalidad o procedencia.

En Intelcia apostamos por el talento sin etiquetas. Valoramos la motivación, el compromiso y el potencial, y trabajamos para empoderar a nuestros profesionales. Me siento especialmente orgullosa de nuestro proyecto POWER IN, lanzado en 2024 desde el área de Talento, que busca reconocer, desarrollar y potenciar el talento interno.

Este proyecto incluye iniciativas como Intelcia University, y programas como High Potential, que identifica a personas con gran proyección en la compañía para ofrecerles un plan de desarrollo profesional específico con el objetivo de convertirlas en futuros líderes de Intelcia.

¿Cómo compatibiliza su vida laboral con la personal? ¿Tiene su empresa planes para facilitarlos?

Es un reto constante para cualquiera que tenga responsabilidades directivas. En mi caso, he aprendido a establecer prioridades, delegar eficazmente y rodearme de un equipo en el que confío plenamente.

En Intelcia somos conscientes de que el bienestar personal repercute directamente en el entorno laboral. Por eso pusimos en marcha Made for You, un programa centrado en

promover el bienestar de nuestros profesionales a través de la flexibilidad y la conciliación.

Dentro de este programa están herramientas como SWAP, que permite a cada persona gestionar sus turnos de forma autónoma, y medidas como Flexilia, que promueve una mayor eficiencia y flexibilidad en la gestión del tiempo. Gracias a ella, se han recuperado ya el 20 % de todas las horas perdidas por ausencias o retrasos.

¿Qué cree que hay que mejorar para que se pueda compatibilizar mejor la vida privada y profesional? ¿Es un problema de las empresas, de las relaciones personales o de uno mismo?

Intervienen muchos factores: personales, sociales y laborales. Pero las empresas tenemos una gran responsabilidad en este ámbito. Debemos encontrar un equilibrio entre los objetivos del negocio y el bienestar de nuestros profesionales.

En Intelcia, el área de personas es especialmente relevante porque el sector de atención al cliente exige una gran capacidad de adaptación, con un alto nivel de exigencia en resultados y calidad de servicio. Programas como "Made for You" han demostrado tener un impacto positivo y medible en la satisfacción y bienestar de nuestros equipos.

Sandra Gibert, CEO Intelcia Spanish Region

La conciliación no debe entenderse como un privilegio, sino como un derecho que las empresas tenemos la responsabilidad de garantizar desde la empatía y el compromiso.

Un 35 % de los alumnos no finaliza Bachillerato ni FP. ¿Está en la educación el problema de la falta de perfiles especializados?

Vivimos en un contexto económico y social muy complejo, con altos niveles de incertidumbre que han podido minar la motivación y expectativas de muchos jóvenes.

Además, hay sectores como el tecnológico que evolucionan tan rápido que pueden llegar a provocar un desfase entre la educación formal y lo que realmente necesita el mercado laboral.

La colaboración entre empresas e instituciones educativas es fundamental para construir itinerarios formativos que respondan a la demanda real de talento y mostrar a los jóvenes que existen múltiples caminos hacia el éxito profesional.

En Intelcia trabajamos por acercar nuestro sector a las nuevas generaciones con iniciativas como Intelcia Summer Camp, talleres prácticos para futuros profesionales STEM. También participamos activamente en eventos universitarios, como los organizados por ESIC, donde explicamos cómo se aplica la tecnología —incluida la IA— en el día a día de nuestras operaciones.

Mujeres TIC

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

Por supuesto. Cursar una carrera universitaria, sea cual sea, es fundamental para adquirir madurez, compromiso, espíritu de sacrificio y esfuerzo. Todo ello forma parte de la huella personal de cada uno.

Además, nunca hay que dejar de aprender. Estar al día en nuevos modelos de gestión, tecnologías, legislación... es imprescindible. La vida profesional es un camino de aprendizaje constante y uno debe estar dispuesto a formarse por iniciativa propia.

Hay que rodearse de buenos partners y aprender de ellos, incluso en una simple reunión. Hay que tener siempre los ojos y oídos abiertos y muchas ganas de seguir creciendo.

Solucione el problema de la educación en España...

La solución exige una visión a largo plazo y una apuesta decidida por la innovación pedagógica. Es necesario modernizar contenidos, priorizar metodologías prácticas y fomentar los intereses y habilidades individuales.

También es clave fortalecer la relación entre el sistema educativo y el tejido empresarial para que la formación profesional esté alineada con las competencias que demanda el mercado.

Si tuviera que aconsejar a un joven qué estudiar para tener un futuro laboral estable, ¿qué le diría?

Le diría que escoja una formación que combine lo que le gusta con lo que el mercado demanda. Áreas como las STEM, la IA, la ciberseguridad o el análisis de datos ofrecen grandes oportunidades.

Pero también es crucial desarrollar habilidades transversales: comunicación, trabajo en equipo, inteligencia emocional, resiliencia, aprendizaje continuo... El mundo laboral cambia constantemente. Lo que hoy es ventaja competitiva, mañana puede quedar obsoleto. Por eso, más que elegir una carrera concreta, lo importante es adoptar una actitud flexible, curiosa y proactiva.

¿Hacia dónde cree que va el sector TIC?

¿Cuáles son las tendencias que realmente van a transformar la sociedad?

Big Data, ciberseguridad y la Inteligencia Artificial van a seguir marcando el futuro del sector TIC.

La IA está abriendo un abanico de posibilidades inmenso. En el ámbito de la atención al cliente, por ejemplo, en solo dos años hemos visto cómo ha transformado completamente el sector con asistentes conversacionales basados en IA generativa,

herramientas de análisis del lenguaje o sistemas de gestión inteligente del conocimiento.

Pero para que esta transformación sea positiva, sostenible y responsable, hay que mantener a las personas en el centro. La tecnología debe estar siempre al servicio de las personas, y no al revés.

IA, automatización, robótica... ¿De verdad cree que el futuro pasa por las personas?

Sin duda. La tecnología por sí sola no aporta valor; son las personas quienes le dan sentido, dirección y utilidad.

En Intelcia apostamos por una tecnología con aplicación operativa real. Utilizamos IA y automatización para liberar a nuestros agentes de tareas repetitivas, lo que les permite enfocarse en aquellas de mayor valor añadido. Herramientas como asistentes virtuales o speech analytics son ya una parte fundamental de nuestro día a día.

Pero, especialmente en la atención al cliente, la empatía, la creatividad o la interpretación del contexto seguirán siendo tareas humanas. Precisamente ahora que los chatbots se han generalizado, el papel de los agentes humanos cobra más valor que nunca.



Un CIO en 20 líneas

“El principal reto es recalibrar continuamente los recursos para generar valor para la compañía”

Alberto Baselga, CIO de Northius

Northius es uno de los grupos líderes en formación en España con más de 1.000 empleados. Integra diversas instituciones formativas con el mismo objetivo: la captación y la preparación de los profesionales del futuro. Cuenta actualmente con 65.000 usuarios activos y más de 35.000 nuevas matriculaciones al año. Cuenta con más de 40 centros formativos distribuidos en la Península Ibérica además de una importante presencia en otros países de Europa y Latinoamérica. Entre sus marcas se encuentran algunas como CEAC, Unisport, Deusto Formación o Campus Training. Hablamos con Alberto Baselga sobre cuál es la problemática que se encuentra un CIO en un grupo empresarial tan complejo.



Un CIO en 20 líneas

Alberto Baselga, CIO de Northius

¿Cuántas personas tienes a tu cargo? ¿En qué consiste tu trabajo diario?

Lidero un equipo de unas 70 personas. Me contrataron para impulsar la transformación digital de una compañía con 14 años de historia que, aunque crecía tanto orgánica como inorgánicamente, mantenía demasiados procesos manuales. Eso hacía imposible seguir escalando al mismo ritmo.

Hoy facturamos más de 100 millones de euros al año. No es lo mismo pasar de uno a diez millones que de cien a mil: el reto es muy distinto y la tecnología se convierte en un pilar esencial.

Cuando llegué no había nadie dedicado al producto tecnológico. Solo personal de sistemas ocupándose de la wifi, los equipos o los puestos de trabajo. Todo lo demás se hacía con proveedores externos, a través de proyectos llave en mano. La solución era clara: Northius debía convertirse en una empresa tecnológica, con capacidades propias, propiedad intelectual y, sobre todo, ofreciendo al estudiante una experiencia personalizada.

Eso supone tomar decisiones constantes de build versus buy en todas las fases del funnel del estudiante: cómo lo captamos, cómo lo fidelizamos, cómo funciona nuestra red comercial, cómo servimos el producto, qué forma tecnológica tiene, qué coberturas le damos... Y al final, cómo conectarlo con el mercado laboral.

Para construir esa estrategia contraté perfiles especializados: ingenieros, desarrolladores, expertos en producto digital, product managers, equipos de inteligencia artificial y de analítica y gestión de datos. Y a todo ello se suma la parte de IT, imprescindible en una organización con múltiples delegaciones y oficinas.

Mi día a día consiste en tomar decisiones sobre qué oportunidades de negocio debemos abordar desde la tecnología: funcionalidades que nos aporten ventaja competitiva, aperturas de mercados, nuevos nichos o el análisis de nuestros estudiantes.

¿Cuáles son los problemas internos con los que te encuentras?

Tenemos unos 1.500 empleados trabajando por todo el mundo. El headquarter está en A Coruña, pero, además, contamos con call centers en ciudades como Barcelona, Oviedo, Madrid, Barcelona o Valencia, además de otros internacionales.

La principal dificultad está en que hay que tener una visión 360° del estudiante, nuestro cliente, que está distribuido por todo el mundo. Esto implica estar pendiente del networking, la telefonía y el acceso a la red.

Lo que comentas es complejo, pero tiene una ventaja: casi todo lo que has desarrollado lo has hecho partiendo de cero...

Sí, en gran medida. La compañía ya llevaba operando 14 años. El CRM, por ejemplo, estaba más pensado para los empleados que en el cliente. Eso nos obligó a cambiar la forma de trabajar.

Todo lo que hemos ido desarrollado ha sido para tener oportunidades de negocio que den más valor, pero para hacerlo hemos tenido que prescindir de muchas cosas legacy.

¿Cuáles son los dos principales problemas que tienes actualmente?

Ahora mismo los problemas ya no son tecnológicos, son de negocio. Mi principal reto diario es el de recalibrar continuamente los recursos

Un CIO en 20 líneas

para optimizarlos y alinearlos con el fin de generar valor para la compañía.

¿Cuáles son los principales riesgos que pueden afectar ahora mismo a una empresa como la vuestra?

El phishing, sin duda. No deja de crecer y sabemos que algunos alumnos pueden caer. El reto es doble: por un lado, el riesgo interno que tenemos todas las compañías, con falsos correos que intentan provocar transferencias o ingresos indebidos. Y por otro, un riesgo específico: que nuestros estudiantes sean engañados con mensajes que utilizan nuestro nombre. Ese es uno de los puntos más sensibles y lo vigilamos continuamente.

Tienes barra libre para gastar, ¿qué es lo que implantarías?

Si no tuviese ninguna restricción presupuestaria, pasaría de las casi 70 personas que somos en el departamento a unas 150. El reto tiene varias dimensiones: el funnel del estudiante, la diversidad de marcas y nichos, y la presencia internacional.

Cada marca es un mundo. No es lo mismo diseñar un producto para oposiciones que para jardinería. Lo mismo ocurre con los países, un jardinero en España no tiene las mismas necesidades que uno en Brasil. Son dos productos educativos diferentes, dos contextos. Para asumir esa complejidad se necesitan equipos multidisciplinares que trabajen en problemas muy específicos. Esa sería mi primera línea de gasto, en personal tecnológico.

La segunda, sin duda, sería en Inteligencia Artificial. Actualmente tengo un gasto bastante alto en APIs de proveedores de IA de LLM como OpenAI, Claude, Google, etc. No puedo sacarle todo el partido

que me gustaría porque no tengo todo el personal para maximizar el potencial de todas estas herramientas.

¿Qué otras tendencias son las que ves ahora mismo?

La más importante es la Inteligencia Artificial, sin ninguna duda. La segunda está ligada al uso de la tecnología en escenarios de aprendizaje.

Cada vez hay más escuelas punteras que utilizan la tecnología para crear nuevos entornos formativos. Antes aprender significaba ir a clase o a una academia. El COVID demostró que la formación online y asíncrona puede tener algunos defectos, pero también grandes virtudes. Ahora vemos modelos híbridos que combinan lo mejor de ambos mundos.

Este modelo permite que el estudiante no solo use un ordenador, sino que acceda a un espacio digital que le ofrece nuevas capacidades y lo prepara para hacer frente a nuevos retos.



Mi día a día consiste en tomar decisiones sobre qué oportunidades de negocio debemos abordar desde la tecnología: funcionalidades que nos aporten ventaja competitiva, aperturas de mercados, nuevos nichos o el análisis de nuestros estudiantes.



Legalidad TIC

El imparable efecto dominó de la digitalización en notarías y registros

Por JUANJO HDEZ. BONACHE,
Asociado Principal de [ECIJA](#)

Hace ya varios años que la digitalización llegó como un verdadero tsunami a nuestras vidas, dejando de ser una promesa de futuro para convertirse en una realidad de nuestro día a día.

Dentro del entorno empresarial, son muchos los sectores que mostraron una inmediata atracción por esta nueva corriente (servicios financieros, seguros, retail, tecnología, telecomunicaciones, logística, transporte e industria, entre otros), pero, como en todos los grandes avances, ha habido ciertas actividades históricamente más tradicionales que se han mostrado más reticentes a subirse a esta imparable ola (por ejemplo, construcción, sector primario o notarías y registros públicos).

Durante décadas, los procedimientos en notarías y registros fueron sinónimo de largas filas, documentos físicos y lentos procesos de verificación. Hoy, gracias a la digitalización, las empresas y particulares pueden acceder

a servicios en línea, [firmar documentos electrónicamente](#) y hacer seguimiento de sus trámites en tiempo real.

Así es la digitalización en notarías y registros

La digitalización de notarías y registros no es solo una cuestión de modernización, sino de adaptación del Derecho a la nueva realidad social

y tecnológica. El reto es claro: lograr un equilibrio entre innovación tecnológica y preservación de garantías jurídicas fundamentales.

Ya en el año 2024 entró en vigor la Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y



Legalidad TIC

registrales; pudiendo afirmar que los avances implementados han sido un verdadero éxito.

Según datos oficiales, desde su entrada en vigor, se han registrado casi 20 millones de notificaciones electrónicas y más de 4,7 millones de documentos presentados telemáticamente, así como la consolidación del sistema gracias al uso de sellos de tiempo digitales —más de 388 millones en el primer año— y la implementación de herramientas como la comparecencia por videoconferencia, carpetas registrales y el servicio "Cómo va lo mío".

Diversos países han creado plataformas digitales que permiten realizar gestiones notariales sin necesidad de presencia física como, por ejemplo, la firma electrónica certificada, registro electrónico de escrituras, [plataformas de atención virtual](#) e incluso algunos países están incorporando sistemas de videollamadas y validación biométrica para identificar al usuario, garantizando seguridad en los procesos a distancia.

Resulta incuestionable que la digitalización ha permitido una atención más ágil y personalizada, especialmente útil para personas con movilidad reducida o residentes en zonas rurales. Además, ha impulsado una mayor transparencia y trazabilidad en los trámites, reduciendo las posibilidades de corrupción o manipulación de documentos, así como la lucha contra el blanqueo de capitales y fraudes fiscales que eran

muy habituales en, por ejemplo, transacciones inmobiliarias.

Para los notarios y registradores, estas herramientas han optimizado el tiempo de trabajo, minimizado la acumulación de papel físico y permitido un mejor control de los expedientes en curso.

Sin embargo, la transformación digital está en continua evolución y es relativamente sencillo dar un paso en falso que pueda poner en jaque estos novedosos sistemas, por lo que no está exenta de desafíos para preservar el equilibrio entre la utilidad y la validez de su intervención.

Con carácter principal, estos sistemas deben garantizar la fe pública notarial, ya que el notario debe verificar la voluntad y capacidad de las partes. La actuación a distancia o por medios electrónicos puede dificultar esta función, planteando dudas sobre cómo preservar la intervención personal del notario.

También el tratamiento de datos sensibles en entornos digitales requiere protocolos estrictos de seguridad, cifrado y almacenamiento conforme a la legislación de protección de datos o incluso la adaptación legislativa ya que hasta el momento muchos marcos jurídicos aún no contemplan integralmente la escritura electrónica o la inscripción digital.

El imparable efecto dominó de la digitalización en notarías y registros



La digitalización está en continua evolución y es relativamente sencillo dar un paso en falso que pueda poner en jaque estos novedosos sistemas

En cualquier caso, latendencia apunta hacia notarías híbridas con una combinación entre servicios presenciales y virtuales, interoperabilidad entre registros de distintos países, inteligencia artificial para apoyar las tareas repetitivas, revisión de documentos y alertas de riesgo legal, uso de tecnologías emergentes como blockchain para asegurar la inmutabilidad de los registros o tokenización de activos y contratos inteligentes con intervención notarial.

En conclusión, estando ante una transformación histórica que no solo mejora la eficiencia del sistema, sino que refuerza los derechos ciudadanos en un mundo cada vez más digital, es muy importante no perder de vista los pilares que nos han traído hasta aquí para que la combinación sea cada vez más exitosa.



Aplicación Práctica

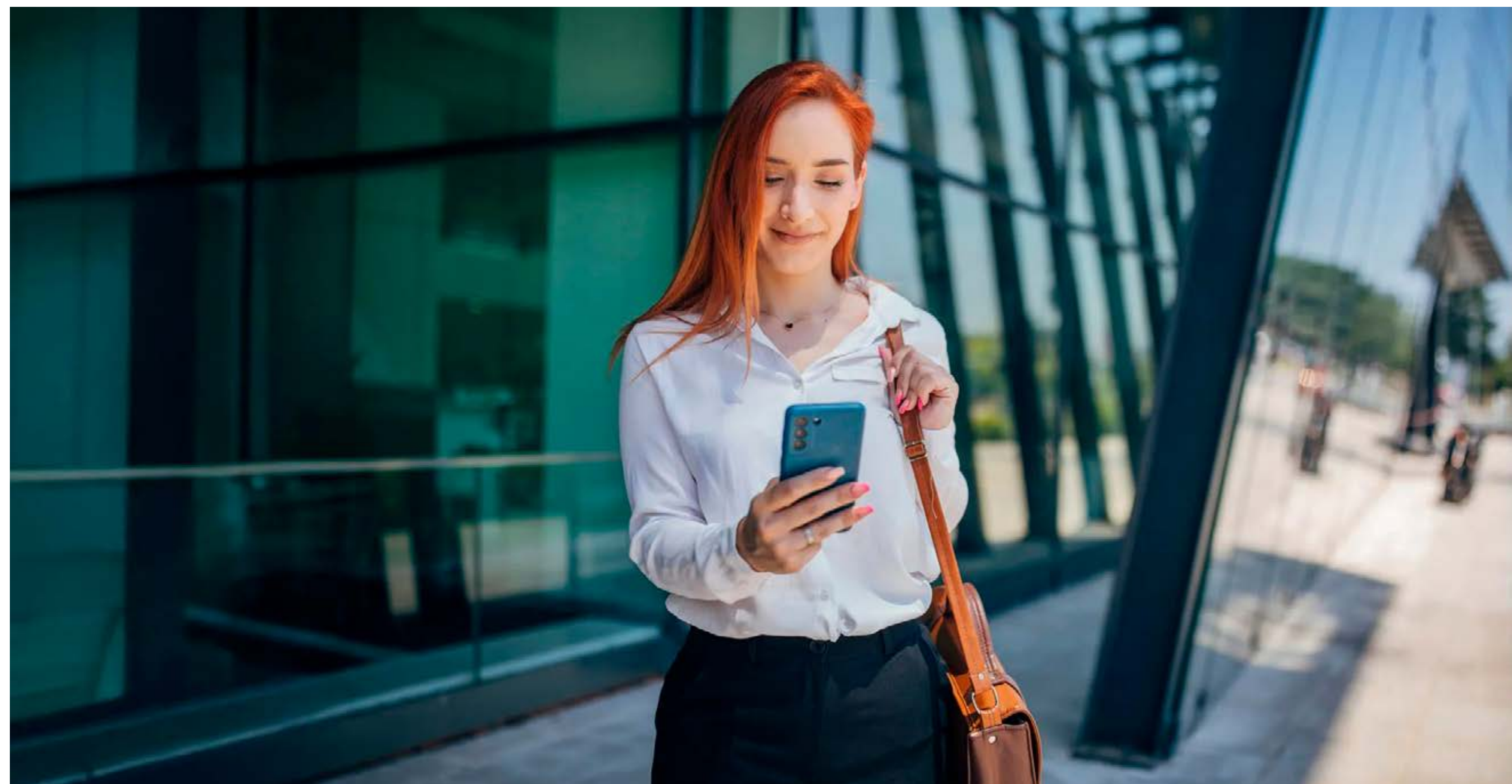
MasOrange mejora el servicio a sus clientes y moderniza su red gracias a la analítica avanzada de datos

[MasOrange](#), el mayor operador de telecomunicaciones de España por número de clientes con 39 millones de líneas de banda ancha y móviles, ha mejorado sus capacidades de análisis y ha acelerado la implantación de la inteligencia artificial (IA) mediante la plataforma de [Cloudera](#), la única compañía que impulsa la IA a través de los datos en cualquier entorno. Como consecuencia, ha logrado una mejora significativa en la experiencia y el servicio a sus clientes.

Un inmenso volumen de información

Las operaciones de MasOrange generan una gran cantidad de información, tanto relacionada con su infraestructura de telecomunicaciones como con los servicios que ofrece a sus clientes. En concreto, su red registra entre 600.000 y 800.000 eventos por segundo, las 24 horas del día. Estos eventos incluyen datos sobre llamadas, saturación de la red, estado de las antenas y otras cuestiones relevante, como métricas de satisfacción del usuario, que ayudan a identificar el riesgo de pérdida de clientes.

Para aprovechar el valor de todos esos datos y promover casos de uso que mejoraran su



infraestructura, el operador necesitaba contar con una solución que fuera escalable. En este sentido, apostó por la plataforma de Cloudera, la cual abarca todas las necesidades del ciclo de vida de los datos e integra funcionalidades de gobernanza, auditoría y linaje, análisis e IA.

Estas capacidades han sido fundamentales para garantizar la calidad de los datos y permitir una supervisión continua que facilitara la detección de posibles fallos en los procesos. En especial, el enorme volumen de información generada por las llamadas de los usuarios requiere un

Aplicación Práctica

filtrado eficaz para identificar la información relevante mediante modelos adecuados, una tarea especialmente compleja cuando se realiza en tiempo real.

Otra cuestión crucial deriva del hecho de que la información en este sector es a menudo sensible y está sujeta a normativas de cumplimiento no solo a nivel local, sino también a nivel europeo. Por lo tanto, ha sido imprescindible garantizar desde Cloudera la gobernanza y la seguridad de los datos durante todo el proceso.

Innovación y eficiencia a través del potencial del dato

Gracias a la solución Cloudera Data Flow y a otras capacidades integradas de gestión de datos, la compañía ha podido gestionarlos de manera eficiente, segura y desde un único punto de control. Esto ha permitido más de 50 casos de uso en producción, dentro de los que destacan los centrados en la experiencia del cliente y en la planificación de las redes.

La gestión del riesgo de pérdida de clientes fue uno de los primeros casos de uso que implementó MasOrange. Mediante el análisis del comportamiento de los usuarios, se generan mapas de calor que identifican a los clientes con una alta probabilidad de abandono, lo que permite tomar medidas preventivas.

MasOrange ha evolucionado su plataforma, inicialmente instalada en un centro de datos local, hacia una arquitectura híbrida en Cloudera

La mejora del servicio al cliente desde el call center ha sido otro caso de uso relevante. A través del procesamiento en tiempo real y a un mejor análisis de datos, los agentes ahora tienen acceso a información precisa y actualizada. Esto les permite recomendar la gama de ofertas más adecuada para cada usuario, adaptando sus recomendaciones a sus necesidades específicas y ofreciendo propuestas personalizadas.

La optimización de la distribución de las antenas también ha sido un caso de uso fundamental, con repercusiones en los costes y la experiencia del cliente. Con más datos y mejores análisis, MasOrange ahora puede identificar cuáles deben reforzarse y cuáles están infrautilizadas, lo que permite una mejor

MasOrange mejora el servicio a sus clientes

asignación de recursos y una infraestructura de red más eficiente, lo que, una vez más, se traduce en un mejor servicio.

Evolución hacia una arquitectura híbrida

Como parte de su proceso continuo de innovación, MasOrange ha evolucionado su plataforma, inicialmente instalada en un centro de datos local, hacia una arquitectura híbrida en Cloudera. Esto ha permitido elegir dónde se ejecutan los nuevos casos de uso (en la nube o en el centro de datos) sin necesidad de reescribirlos o migrarlos. Esta arquitectura híbrida presenta además numerosas ventajas en términos de gestión de costes, flexibilidad e integración de sistemas.

"Gracias a Cloudera, MasOrange es capaz de evolucionar continuamente, a través de una arquitectura híbrida que funciona en centros de datos y nubes públicas. Planeamos añadir análisis más avanzados y casos de uso impulsados por la inteligencia artificial, ahora que contamos con una base sólida en materia de gobernanza y linaje de datos", concluye Giuseppe Monno, Manager del área Business Intelligence & Big Data en MasOrange.



Tendencias

El nuevo manual del ransomware: extorsión con IA y auge de los ataques centrados en los datos

Por DEEPEN DESAI
vicepresidente ejecutivo y director de seguridad en Zscaler

El ransomware está atravesando una transformación radical impulsando la extorsión con IA. Entre abril de 2024 y abril de 2025, la infraestructura en la nube de Zscaler bloqueó más de 10.8 millones de intentos de ransomware, lo que representa un asombroso aumento interanual del 145,9%, y marca el volumen más alto desde que comenzamos a registrar estos datos. Pero este cambio no

se trata solo de cantidad, sino también de sofisticación.

Lo que antes eran ataques generalizados basados en el cifrado de sistemas, ahora son campañas altamente dirigidas que se enfocan en robar información sensible y utilizarla para extorsionar, generando presión psicológica y reputacional. Además, los cibercriminales están utilizando inteligencia artificial generativa para [automatizar la recopilación de información](#), crear malware y lanzar campañas de phishing con una eficiencia sin precedentes.

De cifrado a extorsión: la extorsión con IA

El modelo tradicional del ransomware, cifrar sistemas y exigir rescate, está siendo reemplazado por una táctica más eficaz: la filtración de datos. Los atacantes ya no bloquean el acceso, sino que extraen datos sensibles y amenazan con hacerlos públicos. Este enfoque aprovecha el miedo a sanciones regulatorias, pérdida de propiedad intelectual y daño reputacional, obligando a muchas organizaciones a pagar incluso si sus sistemas siguen funcionando.

La IA generativa potencia la extorsión con IA, permitiendo ataques más rápidos, personalizados y sofisticados. Los cibercriminales ahora se enfocan en usuarios con acceso privilegiado y utilizan técnicas de suplantación para moverse lateralmente dentro de las redes, evitando detecciones tradicionales.

Sectores en la mira: manufactura, salud y tecnología

En 2024, los sectores más afectados fueron salud, tecnología, manufactura, agricultura y energía. El sector salud lidera la lista, con 725 brechas y 275 millones de registros expuestos,



Tendencias



La solución pasa por adoptar arquitecturas zero trust nativas en la nube, impulsadas por Inteligencia Artificial

debido al alto valor de la información médica y su exposición regulatoria.

En energía, los intentos crecieron un 935 %, impulsados por la automatización y la debilidad en sistemas de control industrial. La agricultura aumentó un 677 %, ya que la digitalización superó la capacidad de respuesta en ciberseguridad. Tecnología y manufactura también fueron blancos prioritarios, dada su dependencia operativa y alto volumen de datos críticos.

Las defensas tradicionales ya no son suficientes

Muchas empresas siguen confiando en arquitecturas de seguridad obsoletas: VPNs, firewalls tradicionales y soluciones puntuales como antivirus. Estas tecnologías no están

preparadas para las amenazas actuales como la extorsión con IA, ya que generan puntos ciegos, acceso excesivo y visibilidad limitada.

La solución es clara: adoptar arquitecturas zero trust nativas de la nube, impulsadas por inteligencia artificial. Este enfoque integra la seguridad en todo el ecosistema —usuarios, dispositivos y aplicaciones— sin importar su ubicación, reduciendo riesgos de la extorsión con IA y mejorando la protección.

Cuatro pilares para una defensa moderna contra el ransomware

- 1. Reducción de la superficie de ataque:** ocultar usuarios y aplicaciones detrás de un proxy seguro en la nube elimina direcciones IP públicas y accesos directos, dificultando que los atacantes identifiquen objetivos vulnerables.
- 2. Prevención proactiva:** inspección completa de tráfico TLS/SSL, análisis en tiempo real (sandboxing) y aislamiento de archivos sospechosos ayudan a detener las amenazas antes de que se activen.
- 3. Bloqueo del movimiento lateral:** establecer conexiones directas entre usuarios y aplicaciones limita la propagación de los atacantes. La segmentación basada en IA ajusta los accesos según el contexto, y las

El nuevo manual del ransomware

tecnologías de engaño detectan intrusiones de forma temprana.

- 4. Prevención de exfiltración de datos:** herramientas como DLP (prevención de pérdida de datos), CASB (broker de seguridad en la nube) e inspección avanzada del tráfico ayudan a evitar que la información llegue a manos de los atacantes.

Adaptarse a una nueva realidad

En esta nueva era de extorsión con IA, el ransomware se ha convertido en un arma de precisión que explota tanto debilidades tecnológicas como vulnerabilidades humanas. El paso del cifrado a la filtración de datos, impulsado por la IA generativa y los ataques personalizados, ha hecho que las amenazas sean más rápidas, sigilosas y devastadoras.

A medida que los atacantes evolucionan y se multiplican, las organizaciones deben responder con igual agilidad, reemplazando sus defensas tradicionales por marcos de seguridad inteligentes, integrados y proactivos que permitan anticipar, aislar y neutralizar amenazas antes de que escalen. Y deben hacerlo con urgencia: ya no se trata solo de proteger la operación, sino de garantizar la supervivencia misma.



Tendencias

Un salto cuántico en las capacidades de computación



Por JOHN ROESE,
CTO y CAIO Global de [Dell Technologies](#)

El ámbito de la computación avanza a un ritmo extraordinario y las empresas de todo el mundo se esfuerzan por mantenerse al día. Aunque está claro que la computación cuántica (QC) va a

revolucionar la tecnología, aún no está lista para reemplazar a la computación clásica. En cambio, un enfoque de computación cuántica-clásica híbrida (HQCC), en el que los procesadores cuánticos complementen a los ordenadores clásicos a la hora de abordar los desafíos más complejos, parece ser el camino a seguir.

Según IDC, el mercado global de computación cuántica alcanzará los 8.900 millones de dólares en 2028, lo que pone de relieve la creciente demanda de soluciones mejoradas cuánticamente. Pero ¿qué significa esto para las empresas hoy en día y cómo pueden empezar a aprovechar esta sinergia emergente?

Computación cuántica: la promesa es real, pero también los desafíos

La computación cuántica no se limita a la teoría científica, sino que ya se está probando y aplicando en algunas de las industrias más exigentes. Su capacidad incomparable para evaluar múltiples posibilidades de forma simultánea, la convierte en una buena opción para dominios específicos, desde acelerar el descubrimiento de fármacos hasta permitir un modelado y detección más rápido de los posibles riesgos financieros. Su gran potencial reside en su capacidad para analizar múltiples posibilidades a la vez, lo que la hace ideal ante problemas que involucran numerosas variables y resultados.

Sin embargo, las máquinas cuánticas actuales aún se encuentran en sus primeras etapas de desarrollo, caracterizándose por un número limitado de cúbits y ratios de fidelidad relativamente bajos. Los sistemas requerirán mejoras significativas para lograr aplicaciones

Tendencias

prácticas. Además, los mecanismos de control necesarios para implementar instrucciones son propensos a errores debido a la compleja interacción de los fenómenos cuánticos, lo que dificulta mantener la coherencia y la precisión. La complejidad de los algoritmos cuánticos y la necesidad de amplias herramientas de corrección de errores dificultan escalar el número de cúbits y mejorar de la potencia computacional general.

Además, las limitadas capacidades de los ordenadores cuánticos para resolver problemas de optimización y tareas de aprendizaje

automático, que son aplicaciones críticas en muchos campos, ponen de relieve la apremiante necesidad de enfoques HQCC que puedan aprovechar las fortalezas de ambos paradigmas. Al combinar la potencia de los procesadores cuánticos con la estabilidad y [fiabilidad de los sistemas clásicos](#), HQCC ofrece lo mejor de ambos mundos.

Preparándose para la computación cuántica

Es importante comprender que HQCC no es una alternativa a las operaciones actuales de

Un salto cuántico en las capacidades de computación

Computación de Alto Rendimiento (HPC), sino una mejora. A pesar de su potencial, HQCC presenta algunos obstáculos críticos que deben abordarse, como la interoperabilidad del software, la escasez del talento y los [avances en hardware](#). Teniendo esto en cuenta, las empresas que comiencen a explorar soluciones híbridas ahora, estarán mejor posicionadas a medida que avancen las capacidades cuánticas.

Un sencillo enfoque de tres pasos para empezar:

- 1. Descubrir:** Comenzar con el aprendizaje y la experimentación. La computación cuántica es un campo emergente, por lo que el primer paso para preparar a la empresa es realizar una investigación básica. Una vez que se esté listo para experimentar, habría que considerar usar la emulación para desarrollar, adaptar y optimizar el código para la computación



Al combinar la potencia de los procesadores cuánticos con la estabilidad y fiabilidad de los sistemas clásicos HQCC ofrece lo mejor de ambos mundos



Tendencias

cuántica en una infraestructura clásica, evitando así una gran inversión inicial.

2. Identificar: No todos los problemas son compatibles con la computación cuántica. No conviene usarla para realizar cualquier tipo de cálculo que tenga una única respuesta. Por ejemplo, no se debería usar para calcular los impuestos ni para procesar nóminas. Por otro lado, puede ser muy eficaz para resolver problemas de optimización. La clave está en buscar situaciones difíciles de modelar debido a la gran cantidad de variables. También conviene considerar casos de uso inherentes al negocio, donde la mejora de las operaciones tendría un gran impacto en los resultados.

3. Implementar: Se trata de conseguir una implementación fluida en producción y beneficios reales para el negocio. HQCC ofrece un enfoque flexible para implementar soluciones de computación cuántica en producción. Al combinar el procesamiento clásico con la potencia de la computación cuántica, los Sistemas Híbridos Cuántico-Clásicos (HQCS) permiten a los desarrolladores crear y probar algoritmos cuánticos en un entorno clásico familiar antes de implementarlos en un costoso hardware cuántico. Esto significa que se puede alcanzar una implementación fluida en producción, acelerando la entrada de la organización en la

era de la computación cuántica, mientras se minimizan los riesgos que conlleva adoptar una nueva tecnología.

La intersección de HQCC e IA

La inteligencia artificial (IA) y la computación cuántica convergen cada vez más. A medida que los modelos de IA se vuelven más complejos y los sistemas clásicos comienzan a alcanzar límites de rendimiento y energía, el potencial de las tecnologías híbridas como HQCC, que combina las capacidades de la IA y de la computación cuántica, es inmenso.

La IA mejora la computación cuántica mediante:

- ▶ **Optimización de las cargas de trabajo:** La IA puede asignar tareas de forma inteligente entre procesadores clásicos y cuánticos.
- ▶ **Mejora de la eficiencia de los algoritmos:** La IA puede refinar los algoritmos cuánticos para que sean más eficientes en hardware cuántico.
- ▶ **Aceleración del desarrollo:** La IA permite el progreso en la computación cuántica sin depender de hardware cuántico dedicado.

A su vez, HQCC puede impulsar la IA mediante:

- ▶ **Proporcionar una potencia de cálculo incomparable:** Los ordenadores cuánticos

pueden gestionar cálculos complejos con los que los sistemas clásicos tienen dificultades, lo que permite que los modelos de IA puedan escalar en ámbitos como la ciencia de los materiales y el descubrimiento de fármacos.

- ▶ **Ofrecer mayor eficiencia energética:** Al aprovechar tanto el procesamiento clásico como el cuántico, HQCC puede ofrecer una mayor eficiencia energética para las tareas de IA.

Esta relación bidireccional crea una sinergia entre la IA y la computación cuántica, impulsando el rendimiento de cada campo y abriendo nuevas posibilidades en todas las industrias a medida que continúan madurando.

Un paso inteligente hacia el futuro

La era de la computación híbrida no se trata solo de tecnología, sino de transformación. Debemos imaginar un mundo donde los problemas que antes tardaban años en resolverse ahora se abordan en días o incluso horas. Si conseguimos la perfecta integración de HQCC, esta visión se convertirá rápidamente en realidad. Para las empresas con visión de futuro, implementar soluciones híbridas es el camino para desbloquear el crecimiento, la eficiencia y la innovación a largo plazo.



Entrevista

Paolo Boni, CEO de Inconcert

"Hay ganas de incorporar la IA al CX, pero también muchas dudas"

MANUEL NAVARRO

Especializada en el desarrollo in house de soluciones para la gestión de la experiencia del cliente (CX) Inconcert emplea tecnología cloud potenciada por Inteligencia Artificial generativa para que sus clientes puedan acelerar el ciclo de vida de los clientes. Su ecosistema incluye software de contact center omnicanal, marketing automation, agentes IA, así como sistemas de gestión de calidad con analítica de voz y workforce management. Hablamos con Paolo Boni, CEO de la compañía para conocer cuál es la estrategia de la compañía en el medio plazo y qué impacto está teniendo la IA en el mercado del Customer Experience

¿Cuál es la estrategia a corto/medio plazo de Inconcert? ¿En qué temáticas se están centrando más?

Ahora mismo, estamos enfocados en algo muy claro: consolidarnos y seguir avanzando como referente global en tecnología para la experiencia del cliente. Hace poco hicimos un rebranding que no fue solo un cambio de logo, sino una forma de alinear nuestra identidad con lo que ya éramos desde dentro: una compañía en



Entrevista

Paolo Boni, CEO de Inconcert

crecimiento, con soluciones cada vez más integrales, que acompaña de verdad a las empresas en su evolución en CX.

Estamos trabajando mucho en dos grandes frentes. Por un lado, seguir incorporando inteligencia artificial en nuestras soluciones a todos los niveles: desde asistentes tipo copilot que ayudan al agente humano, hasta agentes IA como Inagent, que son capaces de conversar directamente con los clientes y resolver sus consultas de forma autónoma, sin perder cercanía.

Y por otro, seguimos fortaleciendo la omnicanalidad, que ya no es solo "estar en todos los canales", sino hacer que la experiencia sea fluida, sin cortes. Por ejemplo, este año hemos sumado el canal de RCS, la evolución del tradicional SMS, a Inconnect y seguimos ampliando funciones en WhatsApp, donde somos partners oficiales de Meta.

Al final, nuestro enfoque es simple: ayudar a las empresas a orquestar toda la experiencia del cliente de forma estratégica, desde el lead hasta la postventa, con soluciones que evolucionan a la par que sus necesidades de negocio.

¿Cuáles son las necesidades más habituales de los clientes? ¿Qué errores suelen cometer en sus procesos de digitalización?

La mayoría de clientes vienen con ganas de incorporar inteligencia artificial a sus procesos,

pero también con muchas dudas. Algunos esperan que un agente IA funcione como los bots de antes, solo que son "un poco más listos". Y claro, se sorprenden al ver que esto va mucho más allá: en realidad hablamos de una tecnología completamente distinta, capaz de conversar con naturalidad, adaptarse al contexto y colaborar con agentes humanos.

También es habitual que no sepan por dónde empezar. El error más frecuente es querer implantar la IA sin tener claro para qué ni cómo. Ahí es donde entra nuestro trabajo: escuchar, analizar su operativa y diseñar una solución realista, que empiece por un despliegue concreto, que escale poco a poco, y que combine la IA generativa con reglas de negocio cuando se necesita precisión. Además, integramos nuestras soluciones con bases de conocimiento fiables, definimos KPIs desde el inicio y trabajamos con despliegues que luego pueden escalar progresivamente. Al final, lo importante no es "tener IA", sino saber cómo sacarle valor de forma continua.

Están incorporando la IA generativa en sus soluciones. ¿No hay mucho mito en torno a ella teniendo en cuenta que sólo un 25% de los proyectos llegan a tener una implantación real?

Esa percepción es real y, en parte, lógica. Toda tecnología nueva genera un pico de expectativas

y mitos, muchas veces exagerados. Y cuando esas promesas no se cumplen, llega la frustración. En algunos casos, esto hace que se tomen decisiones a la ligera o que la implementación no esté bien enfocada.

Uno de nuestros grandes retos como proveedores de tecnología es justamente ese: aterrizar la IA al terreno del negocio, explicar con claridad, sin jergas técnicas, y ayudar a los equipos a entender cómo puede mejorar su operativa.

En este sentido, la clave está en adaptar la implantación a cada caso. Hay veces en que con capacitar en el uso de una funcionalidad con IA dentro de nuestros productos basta, como un asistente que ayuda al agente humano a redactar correos o respuestas. En otros casos, estamos hablando de integrar una solución nueva e independiente como los agentes virtuales. En ambos escenarios, lo importante es que no dejamos al cliente solo: tiene siempre a su disposición un equipo técnico, otro de Customer Success, y también un equipo de Knowledge para capacitaciones. Esa cercanía, ese seguimiento continuo, es lo que marca la diferencia.

Y otra cosa: en Inconcert preferimos trabajar por fases, validar cada avance y solo entonces escalar. A veces hay prisa por lanzar algo cuanto antes, pero si no se hace bien desde el inicio, se pierde la confianza en la tecnología muy rápido.

Entrevista

Paolo Boni, CEO de Inconcert

¿Cómo se adaptan a las necesidades cambiantes de sus clientes?

La adaptación no es solo tecnológica, también es humana. Sabemos que cada empresa tiene su propio ritmo de transformación, y lo respetamos: nuestro rol es acompañar, no forzar.

Esa es precisamente una de las fortalezas de nuestro modelo: escuchamos, entendemos y nos alineamos con sus objetivos de negocio, ajustando nuestras soluciones para que evolucionen con ellos. Y no lo hacemos solo en el arranque del proyecto, sino a lo largo del tiempo. Nuestro equipo de Customer Success está muy presente, actuando como una extensión del equipo del cliente.

Al final, a través de la escucha activa identificamos oportunidades, incorporamos mejoras continuas y garantizamos que cada implementación tenga impacto real, más allá de lo técnico. Nos aseguramos de que cada avance aporte valor, no vamos a empujar cambios que no están listos para asumir.

¿Cuál es la estrategia de Inconcert para la integración de sus soluciones con los sistemas existentes de los clientes?

La integración es un punto crítico, y por eso la cuidamos mucho. Todo nuestro ecosistema es 100% cloud y está construido con una arquitectura basada en APIs. Eso significa que podemos integrarnos fácilmente con los CRMs, ERPs y otros

sistemas de negocio, sin necesidad de hacer desarrollos complejos.

Además, nuestras soluciones son modulares: puedes implementar solo lo que necesitas, sin tener que activar toda la suite desde el inicio. Eso da flexibilidad y facilita avanzar paso a paso, según las prioridades del negocio. Y todo esto con garantías de seguridad muy altas: contamos con certificaciones internacionales como las de Cloud Security Alliance, ISO 27000 o PCI-DSS v4 que aseguran una gestión de datos fiable y transparente.

En definitiva, creemos que la clave no es tener muchas herramientas, sino que estén conectadas, compartan información y funcionen como un verdadero ecosistema. Ahí es donde está el valor.

¿Cómo ve el futuro de Inconcert? Puede preguntar a la IA, si quiere

Pues mira, sí le pregunté... y curiosamente no andaba tan desencaminada (ríe). Más allá de la broma, el futuro de Inconcert lo veo claro y alineado con lo que ya somos hoy: una compañía que combina tecnología, visión de negocio y cercanía con el cliente.

Hay tres ejes que seguirán marcando nuestro camino: innovación tecnológica, visión integral de la experiencia del cliente y un enfoque fuerte en integraciones con terceros. Pero si hay un

protagonista indiscutible en ese futuro, es la inteligencia artificial.

La IA está en el centro de lo que viene. Nuestro compromiso es seguir evolucionando nuestras soluciones con IA, pero también continuar ayudando a las empresas a aterrizarla con sentido, desde el valor, no desde la sobreexpectación o hype, como quieras llamarlo.

El sector cambia rápido, y los clientes aún más. Ya no basta con tener un contact center potente o un buen CRM: hay que conectarlo todo. Desde la captación hasta la atención postventa, pasando por el análisis en tiempo real. Y todo eso, sin perder de vista la experiencia del usuario. Por eso, seguiremos apostando fuerte por la interoperabilidad y por soluciones que permitan orquestar toda la CX como un ecosistema unido, en el que la IA, los datos y las personas trabajen al mismo ritmo.

Nuestra misión es ser el socio tecnológico que no solo ofrece software, sino que acompaña, guía y ayuda a crecer en un entorno que cambia cada día. Y hacerlo con inteligencia. Artificial, sí... pero también humana.



Cibercotizante



José Joaquín Flechoso
Presidente de Cibercotizante

Hub de talento para la economía digital

Estamos en una confluencia de dos modelos. Conservamos prácticas laborales de los últimos doscientos años, que conviven con los nuevos patrones de trabajo de la era digital. Las organizaciones se siguen gestionando como sistemas jerarquizados en un mundo de hiperconectividad. Tenemos que remontarnos años atrás para encontrar un cambio histórico de semejante magnitud y en esta transformación, el talento emerge con enorme fuerza. Nunca como ahora se han puesto en valor capacidades humanas más allá de las titulaciones.

La corriente determinista afirma que el talento está en nuestro ADN y que como tal es algo innato, mientras la corriente indeterminista define que es el tiempo de práctica y el esfuerzo, los que hacen que se desarrolle un talento. Conclusión: el talento se entrena. Ambas teorías son válidas, pero creo más aproximado a la realidad una mezcla de ambas, donde nuestro ADN nos da una base de habilidades, que adecuadamente bien desarrolladas, nos convertirán en alguien altamente capacitado.

Si desarrollamos este proceso de definición del talento ¿por qué no capitalizar nuestro estilo de vida y la creatividad que hemos demostrado, como dos de las principales señas de identidad para ello?

España y especialmente las bondades en cuanto a clima, estilo de vida y oferta de ocio, nos permitiría posicionarnos como un foco de atracción de talento foráneo, que además podría propiciar el retorno de talentos españoles que se han ido en los años más duros de la crisis en busca de una oportunidad laboral que nuestro país no les ofrecía. Crear este gran hub de talento, nos posicionaría en un lugar de privilegio en la economía digital.

Pero también asistimos a otra fuga de talento silenciosa y difícil de digerir. Nos referimos a la perdida de talento senior, donde cada vez es mayor el número de profesionales que han debido abandonar, en edades relativamente tempranas el mercado laboral. Encontramos un gran número de ejemplos de grandes empresas (Telefónica, Repsol, banca, líneas aéreas...) donde han aplicado mediante ERES, bajas incentivadas etc., unas importantes reducciones de plantillas donde los más perjudicados han sido los seniors. Con su marcha se pierde el talento de aquellos que acumulan una gran experiencia y atesoran un buen número de contactos imprescindible para las relaciones comerciales, lo cual difícilmente se puede reemplazar con personas más jóvenes.





Las mejores experiencias digitales comienzan con **Liferay DXP**

Diseñado para la complejidad del mundo real. CMS, e-commerce, inteligencia artificial y mucho más.
¡Todo lo que necesitas en una única plataforma!

