Dato, seguridad y cultura: las tres claves del liderazgo tecnológico actual

La IA ha dejado de ser tendencia para convertirse en eje estratégico en empresas y sector público. Esta es una de las principales conclusiones del encuentro ejecutivo "2026 o cómo liderar en la era de la disrupción permanente con la IA y la ciberresiliencia", organizado por DirectorTIC en colaboración con Zscaler, en el que *C-level* de organizaciones como Grupo Elecnor, Gestamp, Globeducate, Embou MASOrange y el Ministerio de Hacienda señalaron que la cultura digital, la soberanía del dato, la ciberresiliencia y el control del uso de herramientas generativas marcan la agenda. En este nuevo escenario, el liderazgo tecnológico exige equilibrar velocidad de transformación con seguridad y cumplimiento normativo. La clave ya no es experimentar, sino estructurar, proteger y escalar con humanos tomando decisiones estratégicas, señalaron los directivos.

En un mundo empresarial de cambios disruptivos constantes, las reglas del juego han cambiado y con ellas los roles de los directivos. Nacen nuevos perfiles, ajustándose a las nuevas necesidades y nuevas maneras de liderar. Pero también nuevos retos como la combinación de la parte de negocio con la tecnológica. Para Alejandro Velilla, CTO de Embou MASOrange, este es el mayor punto de fricción. "Sabemos que hay un gran número de herramientas que pueden hacer nuestro trabajo, o el de nuestros compañeros, más sencillo, pero hay que integrarlas, hacer que sean seguras, comprobar de dónde salen los datos", comenta, al tiempo que avanza que en Embou MASOrange han creado un comité de excelencia de inteligencia artificial con el fin de analizar la viabilidad e integración de todos los proyectos, tanto por la parte técnica como por la de negocio.

A estos desafíos se añade el de la parte de cultura digital, tal y como apunta Jon Blázquez, CIO de Grupo Elecnor, que recuerda la necesidad de perfeccionar las habilidades existentes de los empleados y de capacitarles, remarcando que estos cambios disruptivos constantes nos sitúan en un paradigma diferente: "Nos vemos en una especie de equilibrio entre la necesidad de llevar a cabo una rápida transformación digital de la empresa, sin adquirir una deuda técnica, siendo garantes de los sistemas para que sean ciberresilientes y seguros", confiesa. Aunque todo depende del sector, recuerda Iván Rodríguez, CIO de Globeducate Iberia, miembro de Comité de Ciberseguridad Corporativo y global IT Catalogue manager. "El de la educación es bastante inmovilista, con colegios que han ido creciendo en gran medida e invirtiendo mínimamente. En los que no entienden el valor del coste de la tecnología y en el que hay todo tipo de profesores, incluso a los que no les gusta la tecnología", subraya. Para Ángeles Garat, *lake-*

Ángeles Garat,
lakehouse solutions manager de Gestamp

"Todos los empleados forman parte de la ecuación, y todos pueden convertirse en puerta de entrada si no existe una cultura sólida de prevención"

house solutions manager de Gestamp, el dato, que es la fuente primera para ser cada día más eficientes y competitivos, y la seguridad van de la mano. Este binomio es crucial: lagos de datos bien gobernados que permitan estandarizar y escalar procesos (siempre con ese objetivo de competitividad) con la seguridad dentro de la estrategia.

El enfoque del sector público es diferente al no tener la orientación y exigencia del mercado, comenta Pablo Escudero, subdirector general de sistemas y aplicaciones del Ministerio de Hacienda. Sin embargo, hay dificultades añadidas entre las que enumera dos escenarios restrictivos: el presupuestario (actualmente con los presupuestos prorrogados desde hace tres años y, por lo tanto, haciendo más con menos). Y la demografía del funcionario, notablemente más alta que en el sector privado, "Lo que obliga a pasar de un rol más orientado a la tecnología y a la administración de servicios, a un rol más transformador. Te esfuerzas por conseguir una transformación del personal si quieres tener éxito en la estrategia", admite. Para mejorar la situación, Pablo Escudero indica que la IA es una de las herramientas con la que están trabajando en el ministerio, automatizando procesos burocráticos.

Una IA que, tal y como aconseja Nuria Andrés, *regional manager* de Zscaler, hay que utilizar con control. "En primer lugar hay que tener visibilidad de las aplicaciones de IA que usan los usuarios. En segundo lugar, políticas de control granulares", sostiene.

Manuel Cantonero, *business development&alliance cibersecurity large enterprise account executive* de Zscaler, en la misma línea, explica que también hay que tener en cuenta cuántas IA utiliza tu usuario.

Ambos destacan que Zscaler aplica políticas en tiempo real desde el punto de vista del usuario. Y desde el ámbito de la IA, del *data lake* (donde las empresas tienen datos buenos y limpios) pueden ayudar a evitar el envenenamiento.

IA, de tendencia a impacto real

En la carrera por liderar la inteligencia artificial, el *C-level* es el encargado de trazar el camino, pero ¿en qué procesos se está dando un valor real a la misma? Pablo Escudero expone que el Ministerio de Hacienda cuenta con un modelo de gobernanza entre los diferentes centros con el que se coordinan en la misma línea. "En el mío hemos apostado por la IA, pero planteando límites. También trabajamos con un modelo normativo muy claro donde apostamos por Copilot. Otras herramientas no están permitidas y no alimentamos al modelo general", especifica. Escudero expone la implantación gradual del modelo, primero con los usuarios que tenían inquietudes profesionales y tecnológicas más avanzadas. También utilizan métricas de uso y personas con licencia. En definitiva, subraya que Copilot es una herramienta de ayuda al experto en el análisis financiero de comunidades autónomas y entidades locales". Una herramienta de apoyo a la toma de decisiones y una toma de decisiones que siempre toma el trabajador.

Iván Rodríguez, CIO de Globeducate Iberia, Miembro de Comité de Ciberseguridad Corporativo y Global IT Catalogue Manager

> ""Globeducate cuenta con una figura encargada de normalizar el uso de la IA en los colegios sobre qué deben aprender los alumnos y cómo se les debe enseñar"

"Gestamp cuenta con su propio *chatbot*", afirma Ángeles Garat. Disponemos de un gestor documental al que podemos preguntar directamente sobre nuestros documentos, lo que facilita el acceso a la información interna de forma segura y eficiente. Además, en Gestamp utilizamos la IA desde hace tiempo, sobre todo para mejorar la excelencia operativa y la eficiencia en mantenimiento y calidad... Es una herramienta que nos ayuda a tomar las mejores decisiones. Decisiones basadas en datos. Es decir, todo pasa por el gobierno del dato y por nuestra plataforma de datos, hypatIA. Lo que nos permite generar modelos con una mayor seguridad y escalarlos.", expone.

Globeducate, por su parte, cuenta con una figura encargada de normalizar el uso de la IA en los colegios en la parte educativa: qué deben aprender los alumnos y cómo se les debe enseñar, declara Iván Rodríguez. En la parte de negocio comenta que están desarrollando cua-

Jon Blázquez,
CIO de Grupo Elecnor

"Tenemos un buen elenco de agentes, pero siempre con un enfoque claro: la máquina no toma decisiones sola. Hay un humano al mando"

dros de mandos, usando Copilot como única IA permitida, metiendo análisis de información, unificando todos los datos, trabajando con la estandarización del dato...

En Grupo Elecnor también llevan años trabajando con inteligencia artificial, mucho antes de que la IA generativa acaparara titulares. "Empezamos con *machine learning* y *deep learning*, apoyándonos en un *data warehouse* (que después evolucionó a *data lake* con datos no estructurados), explica Jon Blázquez.

Cuando irrumpió el fenómeno de ChatGPT, en Elecnor optaron por la prudencia. "Vimos a muchas empresas invertir fuertemente sin tener claro el retorno. Decidimos frenar, observar y definir bien nuestra estrategia". Con un entorno tecnológico apoyado principalmente en Google Workspace y el *datalake* sobre Microsoft Fabric junto a Power BI, la compañía apostó por consolidar primero el marco de actuación: política de IA, comité de seguridad y un modelo de gobierno claro.

En Grupo Elecnor usamos lo que nos ofrecen grandes proveedores como Google o Microsoft, con contratos bien cerrados para proteger nuestros datos", reconoce,

A partir de ahí, el foco pasó a las personas. La compañía lanzó un ambicioso programa de capacitación interna, con itinerarios formativos como el Gemini Journey, orientado a integrar la IA en la productividad diaria. Herramientas como NotebookLM, de Google, han tenido, según Blázquez, un impacto decisivo en la adopción interna.

El siguiente peldaño fueron los GPTs personalizados y, más recientemente, los agentes de IA. Todo ello siempre con un enfoque claro: la máquina no toma decisiones sola. Aquí hay un humano al mando", sentencia.

"La clave, insiste Blázquez, es el enfoque humanista. "Esto es como un becario. Confía, pero verifica. El criterio es del humano". Y esa filosofía, asegura, está calando en la organización.

En el caso de Embou MASOrange el reto ha sido diferente. Como compañía digitalmente nativa,

la adopción no necesitaba impulso, sino orden. "Hemos tenido que poner diques. Todo el mundo quiere hacer cosas con IA. La parte de preguntar a la generativa se nos ha quedado pequeña; ahora te piden APIs, integraciones, acceso a datos…", explica Alejandro Velilla. Para canalizar esa energía, el grupo ha reforzado su estructura interna. El equipo "*transformers*", inicialmente centrado en transformación digital, ha ampliado su alcance a transformación digital e IA. Además, se ha creado un centro de excelencia de inteligencia artificial que supervisa iniciativas y valida arquitecturas, usos de datos y proveedores. "Hemos tenido que estructurarlo todo: qué LLMs están permitidos, de dónde puede alimentarse un RAG y qué fuentes son intocables. Incluso se ha habilitado un JIRA específico para canalizar propuestas internas de casos de uso", aclara. "Nuestros desarrollos más relevantes están orientados a mejorar la experiencia del cliente. Recogemos los datos de las principales incidencias para poder alimentar al agente y que actúe como copiloto de los compañeros que atienden al cliente en la parte de ventas, administración o soporte técnico. Puede ayudar a estructurar la conversación con el cliente y a proponer soluciones concretas". Una vez validado el caso de uso, se abre al mercado interno para su despliegue, explica Velilla.

Alejandro Velilla,
CTO de Embou MASOrange

"Uno de los desarrollos más relevantes que hemos llevado a cabo ha sido un agente orientado a mejorar la experiencia de cliente"

Gobernanza y soberanía del dato

En esta carrera por la IA, el dato y su gobernanza se han convertido en elementos primordiales, seguidos de una soberanía que, también, cobra protagonismo. Una gobernanza que en el caso de las empresas que forman parte del debate no es un caballo desbocado, como suelen definir algunas organizaciones. Ángeles Garat reconoce la importancia de tener claro que los datos son de las compañías. "En el caso de Gestamp, en el departamento de IT contamos con la figura del CDO, que lidera el entorno del dato. Disponemos de un *hub* dedicado a nuestro *lakehouse*, hypatIA, donde se centraliza la gobernanza del dato. Además, contamos con

una herramienta que permite conocer qué datos están disponibles en la capa semántica. En el *hub*, también se gestionan los procesos de calidad del dato en el que todos trabajan con el fin de tener todo bajo control. porque,para nosotros, es muy importante quién es el dueño del dato, los controles de calidad que hay que llevar a cabo en torno al dato, su trazabilidad, quién puede utilizarlo... Tenemos una malla de seguridad para acceder a los mismos.", comenta.

La misma senda sigue Grupo Elecnor, con los datos estructurados y no estructurados, controlados. "Cada proyecto tiene su estructura necesaria para que garantice la vigilancia necesaria. Llevamos a cabo auditorías, se mantiene la trazabilidad y se avanza hacia el uso del dato con algoritmos cada vez más enfocados a predecir, resalta Jon Blázquez. Es decir, desde el tradicional *data warehouse* a la predictibilidad.

Desde Globeducate, Iván Rodriguez señala que su desafío no es solo tecnológico, también normativo, cultural y organizativo porque, más allá de la gestión operativa de la información, están asumiendo plenamente el control de las transferencias de datos entre países y colegios. "A día de hoy, parte de esa gestión sigue dependiendo de equipos locales o del propio ecosistema de cada centro", reconoce, siendo uno de los avances más relevantes un proyecto de Power BI que les ha permitido disponer de acceso inmediato y fiable a la información. "Esto ha supuesto un salto cualitativo en visibilidad y control, aunque seguimos trabajando en definir claramente dónde reside el dato y cómo se gestiona de forma global", destaca.

Rodríguez pone el foco en que la normativa europea sobre el uso de inteligencia artificial en menores es especialmente restrictiva, obligándoles a informar a las familias sobre si las herramientas que utilizan incorporan IA, cuando, en muchas ocasiones, ni siquiera los propios proveedores saben con certeza si sus soluciones integran componentes de inteligencia artificial. "Por esta razón, adoptamos una postura muy

Pablo Escudero, subdirector general de sistemas y aplicaciones del Ministerio de Hacienda

"Copilot es una herramienta de ayuda al experto en el análisis financiero de comunidades autónomas y entidades locales"

conservadora: cualquier herramienta que tenga impacto directo en el alumno está sujeta a controles muy estrictos y a una transparencia total", prosigue. "Podemos controlar lo que ocurre dentro de nuestro perímetro, lo que está de nuestro *firewall* hacia adentro, y establecer políticas claras de seguridad para el entorno corporativo. Sin embargo, el uso de herramientas de IA fuera de nuestro alcance, especialmente cuando los alumnos utilizan sus dispositivos en casa, es prácticamente ingobernable. Esa es una de nuestras principales preocupaciones", confiesa.

En el plano interno, uno de sus grandes retos es cultural. Muchos colegios llevan años formando parte del grupo, pero todavía existe la percepción de que los datos son propiedad exclusiva de cada centro. "En este sentido estamos trabajando en educar y concienciar de que el dato ya no es individual, sino corporativo y compartido", sin embargo. este cambio de mentalidad tampoco les resulta fácil. "Contamos con protocolos y procesos definidos para la integración de nuevos

Nuria Andrés,
***regional manager* de Zscaler**

"Hay que utilizar la IA con control, tener visibilidad de las aplicaciones de IA que usan los usuarios y políticas de control granulares"

centros: auditorías de ciberseguridad, revisión y desmantelamiento de infraestructuras heredadas, y alineación con los estándares del grupo. No obstante, hablamos de organizaciones con planes educativos consolidados, currículos definidos y dinámicas internas muy asentadas, por lo que los cambios son necesariamente progresivos". Por otro lado, el perfil de sus usuarios es mayoritariamente local, aunque cuentan con centros internacionales. Un contexto en el que cuando se introduce la inteligencia artificial, algunas familias perciben que puede perderse la cercanía y la proximidad en la relación educativa. Esa sensibilidad forma parte de su realidad, lo que les condiciona cómo comunicarse e implementar estas tecnologías, se lamenta. "Somos plenamente conscientes de que debemos avanzar en el uso de la IA, y ya la estamos aplicando en procesos como admisiones o clasificación. Sin embargo, el equilibrio entre innovación, control normativo, cultura organizativa y percepción de las familias es complejo", mantiene.

Manuel Cantonero, *business development&alliance cibersecurity large enterprise account executive* de Zscaler

"Lo más importante es mantener control absoluto sobre quién accede, desde qué dispositivo y hacia qué destino"

Desde el punto de vista de seguridad y cumplimiento, Globeducate ha desplegado políticas y controles tanto a nivel interno como externo. Y paralelamente siguen trabajando en la educación interna sobre la titularidad corporativa del dato, un reto que se intensifica con el rápido crecimiento del grupo ya que hace 15 años eran seis colegios; hoy más de 60, y el equipo corporativo no ha crecido en la misma proporción. Una de las partes complicadas para Alejandro Velilla en Embou MASOrange ha sido, tras la compra de varias compañías y la fusión de las mismas, integrar la información. "Tenemos muy bien implantado el *data owner* pero llegan compañías con su propia parte de *data*, hay que autentificar, migrar, luchar contra los silos de información...y esa etapa de adaptación lleva tiempo, pero tampoco es infinito·, constata.

Pablo Escudero, por su parte, pone sobre la mesa otra realidad: el paso del sector privado al público es relevante en cuanto a informes, autorizaciones, normas de seguridad. "Todo tiene que tener un cumplimiento normativo muy claro, menciona. Fundamental también la soberanía del dato desde el punto de vista de dónde están alojados los datos, quién accede, quién tiene las claves y de qué jurisdicción estamos hablando", por lo que, en su opinión, "la seguridad del dato tiene que estar muy bien gestionada porque todavía hay riesgos evidentes".

Ventajas de Zscaler

¿Qué ventajas aporta Zscaler a estas necesidades? Ante una de las principales demandas de los clientes: saber dónde están sus datos y dónde se almacenan, especialmente en entornos internacionales con distintas exigencias regulatorias, Nuria Andrés y Manuel Cantonero ponen el acento en que la compañía cuenta con 160 centros de datos distribuidos globalmente, lo que permite asegurar a los clientes, por razones de *compliance*, la localización de sus datos. Además, pone en valor que los datos son propiedad del cliente, que permanecen en su *tenant* y que

no se utilizan para entrenar modelos externos.

A esto hay que sumar la detección avanzada de amenazas y ataques de día cero ya que, a través de su nube, Zscaler procesa 500 billones de transacciones diarias. Ese volumen permite entrenar modelos propios enfocados en detección de anomalías e identificación de ataques de día cero. El objetivo pasa por que cuando una amenaza aparece, pueda bloquearse antes de llegar al dispositivo del cliente, incluso sin necesidad de detonarla en un entorno de *sandboxing*.

En el caso de fusiones y adquisiciones Zscaler permite habilitar un acceso privado y seguro entre compañías en cuestión de días. Y en cuanto al control del uso de IA por parte de los usuarios, evitan un uso descontrolado mediante la supervisión de las herramientas que utilizan los usuarios, el control de qué preguntas se realizan y de la información que suben. También incorporan capacidades de DLP basadas en etiquetas documentales, permitiendo decidir qué información puede compartirse y cuál no.

> "A través de su nube, Zscaler procesa 500 billones de transacciones diarias"

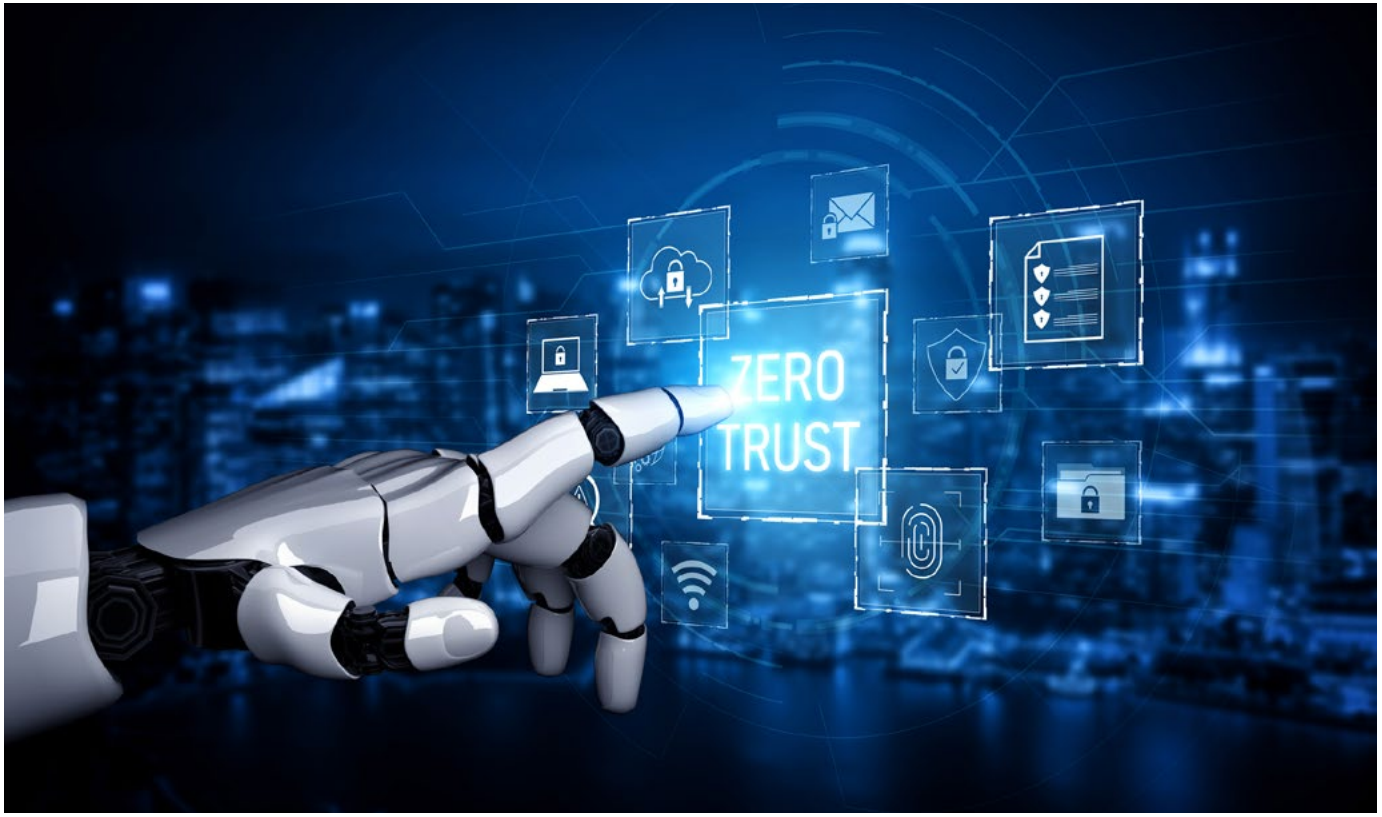
Otro factor importante: pueden controlar las API que están conectadas y qué consultas se hacen a las mismas para buscar información. Mediante inteligencia artificial, también se pueden generar informes sobre uso de licencias no aprovechadas y clasificar el uso de APIs conectadas.

Zero Trust

Durante el evento quedó patente que el antiguo modelo de seguridad "basado en el castillo y la muralla" ha dejado de ser válido. El perímetro físico, que durante años delimitó lo que era seguro y lo que no, prácticamente ha desaparecido. En su lugar, las organizaciones se enfrentan a un entorno híbrido, distribuido y cada vez más dependiente de la identidad como nuevo eje de protección, en línea con los principios de *Zero Trust*.

En el Ministerio de Hacienda el peso del pasado sigue marcando la agenda. La existencia de un amplio legado de aplicaciones, con código en distintos niveles de actualización, representa uno de los principales desafíos. Aunque se apoyan en servicios de auditoría y revisión de seguridad para mejorar la calidad del código, Pablo Escudero reconoce que los sistemas *legacy* continúan siendo un foco relevante de riesgo. A ello se suma el impacto del modelo híbrido, dispositivos corporativos en movilidad, personal externo y servicios que han migrado del entorno on-premise a la nube.

Una preocupación similar se vive en Embou MASOrange, donde el gran reto es la gobernanza de accesos en un ecosistema con fuerte



presencia de terceros y puntos de venta multimarca. Alejandro Velilla señala que la implantación de un modelo de gestión de identidades que obligue a revisar en detalle quién necesitaba realmente acceso y a qué. siempre muestra resistencias, si bien permite depurar accesos innecesarios y reforzar el control.

En Grupo Elecnor el enfoque parte de una premisa clara: la seguridad ya no puede basarse en confiar en lo que está dentro de la red. Su estrategia pivota sobre el análisis de riesgos, identificando los mayores puntos de exposición. La cadena de suministro aparece como uno de los focos principales, junto con la gestión de identidades, que consideran prioritaria. Según señala Jon Blázquez, "La mayoría de los ataques siguen explotando credenciales comprometidas más que técnicas extremadamente sofisticadas. Por ello, reforzar la identidad y elevar la concienciación interna se convierte en una medida clave", advierte.

En Globeducate, donde el entorno tecnológico es menos complejo, el riesgo también se concentra en la suplantación de identidad y el robo de contraseñas, por lo que la organización ha intensificado las acciones de formación, consciente de que el factor humano sigue siendo determinante. Además, Iván Rodríguez señala una preocupación añadida: el uso de dispositivos por parte de menores fuera del entorno protegido del colegio, especialmente en el ámbito doméstico, donde el control es mucho más limitado.

Desde Gestamp, Ángeles Garat incide en que en temas de ciberseguridad es muy importante la cultura interna de la compañía en torno a la prevención y la formación de los empleados. Porque, aunque es responsabilidad del depar-

tamento tecnológico, todos los empleados forman parte de la ecuación y tienen su papel en minimizar los riesgos asociados a la digitalización y el uso de tecnologías.

Todo ello deja patente que *Zero Trust* deja de ser un concepto teórico para convertirse en una necesidad operativa ante un entorno cada vez más distribuido y expuesto.

Cómo ser más resilientes y reducir el riesgo

¿Cómo pueden las empresas aumentar su resiliencia frente a los ciberataques y reducir el riesgo? Para Nuria Andrés la vulnerabilidad humana sigue siendo el principal vector de riesgo, por lo que aconseja repensar la red corporativa. "La red ya no existe", asegura, y por ello "Zscaler conecta directamente a usuarios con aplicaciones y destinos específicos. Así, si se produce un ataque, queda contenido y la empresa mantiene capacidad de reacción", argumenta. Además, despliegan señuelos y entornos falsos para analizar la actividad de los ciberdelincuentes y reforzar la prevención.

> "Las organizaciones necesitan garantizar que sus operaciones continúen incluso si los servicios de seguridad fallan"

Nuria Andrés considera que otro aspecto crítico es la resiliencia operativa. Las organizaciones necesitan garantizar que sus operaciones continúen incluso si los servicios de seguridad fallan. Zscaler proporciona nodos privados y nubes dedicadas para *business continuity*, asegurando que, aunque la plataforma se caiga, los clientes puedan seguir operando sin interrupciones. "La frase que yo uso es: Zscaler desaparece de la faz de la tierra, y los clientes siguen operando", señala la experta en seguridad.

Manuel Cantonero amplía el mensaje, subrayando la importancia de la conexión usuario–dispositivo–aplicación o destino final. Este enfoque permite, por ejemplo, eliminar la dependencia de contraseñas tradicionales: si un usuario intenta acceder desde un dispositivo no autorizado, el acceso queda bloqueado. Incluso cuando se permite la conexión, solo puede interactuar con la aplicación específica, evitando movimientos laterales dentro de la red.

Además, se añade una capa de seguridad continua a lo largo de todo el camino del usuario, combinando inteligencia artificial, análisis de comportamiento y herramientas de prevención de pérdida de datos. "Lo más importante, resume Cantonero, es mantener control absoluto sobre quién accede, desde qué dispositivo y hacia qué destino. Eso es lo que hacemos muy bien en Zscaler y lo que permite a las organizaciones ser realmente resilientes frente a los ataques", finaliza.

Zscaler garantiza la ciberresiliencia 360º

La adopción de la IA en las empresas abre nuevas oportunidades de innovación, pero también plantea importantes retos en materia de seguridad y control de la información. Ante este escenario, Nuria Andrés, *regional sales manager* de Zscaler, defiende una estrategia basada en la plataforma Zero Trust Exchange para equilibrar el impulso tecnológico con la ciberresiliencia.

Nuria Andrés, *regional sales manager* de Zscaler

La estrategia de Zscaler se sustenta en la reducción de riesgos, optimización de costes y aceleración del negocio. La compañía propone hacer invisibles las aplicaciones privadas eliminando la necesidad de direcciones IP públicas, mientras la consolidación tecnológica es otro de los elementos centrales de su propuesta, por poner algunos ejemplos. Además, Nuria Andrés subraya en este vídeo la necesidad de evolucionar el concepto tradicional de *shadow IT* hacia el de *shadow AI*.