FORO TAI
grupotai

Revista digital

FORO TAI

CIBERSEGURIDAD TIC

- ✓ Conoce a los patrocinadores
- ✓ Descubre todo el contenido
- ✓ Accede a los vídeos
- ✓ Todo a un *click*

“El valor de una empresa tecnológicamente moderna y segura”

okta TREND MICRO veeam zscaler

La empresa moderna en busca de la ciberresiliencia

Bajo el título de "El valor de una empresa tecnológicamente moderna y segura" hemos celebrado un nuevo Foro TAI, un encuentro diferente para los que buscan la manera de transformarse para competir mejor en un mundo donde los ciberataques se suceden, y el perímetro de seguridad se ha trasladado al dato y la identidad.

Rosalía Arroyo

Los negocios están cambiando y lo que está en juego nunca ha sido tan importante. Las empresas buscan maneras de innovar con la tecnología, empoderar a empleados y clientes, extraer el máximo valor de los datos, y hacer uso de la Inteligencia Artificial para extraer el conocimiento que les haga destacar.

Las empresas tecnológicamente modernas y seguras son más competitivas, rentables y seguras. Esto las hace más atractivas para los inversores, los clientes y los empleados.

Durante el evento hemos hablado de los grandes retos a los que se enfrentan los responsables de ciberseguridad. Entre otras cosas, ha quedado claro que la ciberseguridad sigue siendo la piedra angular de cualquier negocio.

En este segundo Foro TAI hemos debatido sobre la seguridad de las identidades, la gestión del riegos y postura de ciberseguridad de las empresas, el nuevo paradigma del mundo hiperconectado, o el impacto de la IA como una solución a la eficiencia operativa. Los expertos que nos acompañaron en directo fueron Axier Amo Izarra, Director General de Transparencia y Buen Gobierno del Gobierno de la Rioja; Anto-

nio Galán, CIO de Grupo Hierros Alfonso; Jesús Valverde Romero, CIO & CISO de Isemaren; Alejandro Expósito Esteban, director de operaciones y experto en Innovation digital; Rosalía Machín Prieto, Comandante Jefe de Proyectos TIC, Ministerio del Interior – Secretaría de Estado de Seguridad; Asís Pardo Martín, Co – CEO de Tuio; Luigi Semente, Regional Alliance Manager de Veeam Software; Iván Rodríguez, Solutions Engineer de Okta; Raúl Guillén, Cybersecurity Strategy Director de Trend Micro; y Alberto Maldonado, Regional Sales Director de Zscaler.

Seguridad de las identidades

Los entornos híbridos y *multicloud* presentan una serie de desafíos para la seguridad de las identidades de los usuarios. Estos desafíos se deben a la heterogeneidad de las plataformas y herramientas de gestión, la complejidad de las soluciones de seguridad, y la falta de habilidades de seguridad necesarias. Los entornos híbridos y *multicloud* suelen estar formados por una combinación de plataformas y herramientas de gestión de identidades y accesos (IAM) dispares.

> “La inteligencia artificial semántica es una herramienta que acerca al ciudadano con la institución”
>
> **Axier Amo Izarra,**
> Director General de Transparencia y Buen Gobierno del **Gobierno de la Rioja**

En opinión de Jesús Valverde, CIO & CISO de Isemaren, “la identidad es uno de los vectores de ataque más utilizando por los atacantes, porque una vez que consiguen una identidad, tienen la llave”. Dice también el directivo que hay que centrarse en el concepto de riesgo; “si hay un usuario al que no puedes atribuir nominalmente lo que está haciendo, puede que te estés ahorrando una licencia, pero si ocurre un problema, no vas a saber a quién atribuírselo”. Añade que hay que ir montando un ecosistema que funcione con lo que ya tienes “y que vaya permitiendo poner todas esas capas de seguridad asociadas a la identidad, como esa segunda autenticación de basada en un dispositivo, basada en un contexto… “No puedes pasar de cero a Zero Trust”, asegura, “porque a lo mejor estás poniendo el tejado antes que otros pilares muy fundamentales”.

Antonio Galán, CIO de Grupo Hierros Alfonso que la compañía para la que trabaja, de unos 250 empleados y que está realizando bastantes inversiones en tecnología y ciberseguridad, está dando el salto a la nube y se está enfrentando “a una situación bastante compleja”. La empresa, explicaba su CIO, ha optado por apoyarse en organizaciones externas expertas.

Durante su intervención, comenta Axier Amo Izarra, Director General de Transparencia y Buen Gobierno del Gobierno de la Rioja, que desde que empezaron a trabajar con Aurelia, la

página web semántica de la Diputación Foral de La Rioja, “nos dimos cuenta de que teníamos que unificar información”. El objetivo de Aurelia es proporcionar una plataforma que facilite la búsqueda y el acceso a la información sobre La Rioja. Aurelia se basa en las tecnologías de la web semántica, como RDF y OWL, que permite representar la información de La Rioja de una manera más completa y precisa que las webs tradicionales.

Explica Axier Amo que el problema era “que no nos bastaba con unificar todas esas fuentes de datos que teníamos en diferentes repositorios”, por lo que se ha optó por “hacer nuestra propia cúpula de datos basándonos mucho en *cloud*”. Añade que el proyecto se plantea como un banco de pruebas que pueda ser tomado como referencia por otras comunidades en las que el problema es el mismo: tener datos muy abiertos que están apareciendo en otras páginas y en otros usos.

Asís Pardo Martín, Co-CEO de Tuio, una neoaseguradora 100% digital que nació en 2021, comenta que su empresa tiene una ventaja: “contar con una plantilla pequeña, muy joven y tecnológicamente avanzada”. En opinión del directivo “tener usuarios que son conscientes de que el punto débil de la organización siempre es la persona supone una capa de seguridad”.

“El mayor reto es ir a la nube y controlar el dato

Antonio Galán,
CIO, **Grupo Hierros Alfonso**

Alejandro Expósito Esteban es experto en innovación y operaciones, entre otras. Habla de su experiencia en una empresa en la que no todos los empleados tienen acceso a todos los sistemas. Los datos de alto riesgo “están mucho más cerrados”, asegura, añadiendo que lo mismo ocurre en las plantas de producción: “ningún director de planta de producción quiere es que sus datos salgan, y es muy difícil intentar llevarlos a la nube”.

Asegura Alejandro Expósito que se intentan minimizar los riesgos, donde se incluyen las terceras partes, los proveedores, la cadena de suministro. “Ahí, el principal problema es la gestión de esas identidades. Si se da acceso a un profesional externo a los sistemas, tiene que estar muy controlado que sea él el que accede”, lo que plantea un reto: que una misma persona tenga diferentes identidades, “porque el doctor Gómez en un sistema podría ser el doctor G en otro” y eso “dificulta su seguimiento, así como entender qué está buscando y cómo se le puede ayudar”.

En opinión de Iván Rodríguez, Solutions Engineer de Okta, la problemática a la que se enfrentas las empresas en relación con la seguridad de la identidad es la misma independientemente del tamaño de la empresas. “La diferencia es que a mayor número de empleados o usuarios mayor es el riesgo”, asegura el directivo aña-

diendo que “hay que proteger bien la identidad de los usuarios”.

Okta ofrece una plataforma de IAM integrada que permite a las empresas centralizar la gestión de identidades y accesos en todos los entornos, incluyendo el centro de datos, la nube pública y privada, y las aplicaciones SaaS. La plataforma de Okta proporciona una serie de funciones de IAM, incluyendo, entre otras, la autenticación, autorización, gestión de identidades o análisis de seguridad. Asegura Iván Rodríguez que desde la compañía apuestan por saber que el usuario es quien dice ser “poniendo los mecanismos que necesitemos para poder darle ese acceso”.

Cuando no se trata de un empleado, sino de un tercero, “es lo que llamamos Customer Identity”, y en este caso, “acceden a la aplicación, pero por otro lado”. También responde Iván al reto de que un mismo usuario tenga varias identidades; “con OKTA lo que hacemos es que solo tengas una porque se autentica a través del IdP”, que no es otra cosa una entidad que almacena y verifica la identidad de un usuario. “El que de verdad sabe quién se está autenticando en cada caso es Okta”, asegura el directivo.

“No puedes pasar de cero a Zero Trust”

Jesús Valverde Romero,
CIO & CISO, **Isemaren**

Riesgos y postura de ciberseguridad

Para una empresa es importante saber cuál es su postura de seguridad porque le permite comprender su nivel de exposición a las ciberamenazas. Y al comprender su postura de seguridad, una empresa puede tomar medidas para mejorar su protección y reducir el riesgo de sufrir un ciberataque.

Tras sufrir, el verano pasado, un ataque que afectó a las redes de la Diputación Foral de La Rioja, el Gobierno de La Rioja, el Ayuntamiento de Logroño, y otras instituciones públicas y privadas de la región, dice Axier Amo que sabe “lo que cuesta mantener y levantar una administración”, porque, aunque la Rioja sea una comunidad pequeña, pueden verse afectados 174 ayuntamientos. Ya se sabe que, junto con las normativas, los ciberataques son otro de los elementos que desbloquean presupuestos y ahora se están destinando mucho más presupuesto para mejorar la ciberseguridad de las instituciones; “el nuevo gobierno que está entrando lo ha entendido perfectamente”, asegura el Director General de Transparencia y Buen Gobierno, Gobierno de la Rioja.

Preguntado por cómo se establecen las posturas de seguridad en Tuio, explica Asís Pardo que se pone foco en el diseño de los sistemas. Al respecto asegura que es importante “controlar qué cosas tienen visibilidad sobre qué otras cosas o qué usuarios tienen acceso a qué sitios”, porque “si todo está bien diseñado menos problemas tienes si pasa algo”. El segundo foco es el propio usuario, asegura, repitiendo que tiene una posición ventajosa por el

hecho de que “todos nuestros empleados son nacidos digitales”.

Como experto de seguridad de una empresa multinacional, dice Alejandro Expósito Esteban que en las filiales se tiene poco control sobre las herramientas o procesos de seguridad, y sí de la concienciación sobre esta ciberseguridad. “Intentar hacer que nuestros empleados, que a lo mejor no son tan nativos digitales, se conciencien, aprendan y pongan los medios necesarios para evitar que haya esas intrusiones” es tarea que se deja operar por las filiales, “pero toda la parte de control” se gestiona desde la central.

Asegurando que “nosotros no nos podemos permitir ningún fallo de seguridad”, explica Rosalía Machín Prieto, Comandante Jefe de Proyectos TIC de Ministerio del Interior – Secretaría de Estado de Seguridad, que esta unidad es la responsable de ofrecer asistencia inmediata a la Secretaría de Estado en materia tecnológica de información y comunicaciones, que existe un departamento encargado de todos los sistemas de gran magnitud de Policía Nacional o Guardia Civil, Centro de Inteligencia contra el Crimen Organizado y Terrorismo y todos los organismos

> “La política de retención del dato, da igual dónde esté, es el gran reto”
>
> **Alejandro Expósito Esteban,**
> Digital, Innovation & Business Operations Director

dependientes del Ministerio del Interior. “Lógicamente, cuando hay que dar cobertura a todas las radio telecomunicaciones o a todos los sistemas de información, tenemos un departamento específico que es la seguridad de los sistemas, es decir, la seguridad desde la infraestructura. Utilizamos una red completamente segura: todos los dispositivos, todas las comunicaciones están encriptadas” y por el momento “la poca nube que hay es privada del Ministerio del Interior”, aunque se está explorando cómo trabajar con la nube “que tendría que ser gestionada con los recursos del Ministerio del Interior”.

Sigue explicando la Comandante Jefe de Proyectos TIC del Ministerio del Interior – Secretaría de Estado de Seguridad, que su unidad es la competente en la seguridad de la infraestructura ante cualquier ataque que se pueda dar, pero también se trabaja para proteger el software. Sólo se trabaja en local “porque los datos con los que nosotros trabajamos son especialmente sensibles”, y se es reacio a trabajar con modelos abiertos y empresas que no sean nacionales “para que los datos no estén a disposición de otras entidades”.

En Grupo Hierros Alfonso se apuesta por la concienciación de los usuarios mediante comunicaciones periódicas “que intenten enganchar a la gente a la realidad que estamos viviendo, que es una evolución continua de las amenazas”, dice Antonio Galán, CIO de este grupo empresarial. La forma de abordar la seguridad y tener un control sobre la postura es contar con un fabricante de primer nivel además de “consulto-

rías externas, test de ataques intrusión, y sobre todo estar bien asesorados". El grupo empresarial cuenta con un EDR gestionado "que permite que haya alguien que protege 365/24".

Para Jesús Valverde Romero, CIO & CISO de Isemaren, "el primer paso es definir la postura de seguridad, realizar un análisis de riesgos, y a partir de ahí, definir cuál es el umbral del riesgo aceptado de la organización, o hasta dónde podríamos llegar si ocurre un problema, para después hacer un Plan Director basado en un estándar internacionalmente reconocido, como el esquema Nacional de Seguridad, ISO 27001 o NIST", explica el directivo.

Se apuesta también en Isemaren por conseguir que el usuario deje de ser el eslabón más débil, "para ser esa primera línea de defensa que te alerte cuando hay un problema", además de apoyarte en servicios de seguridad externos, "y a partir de ahí ir mejorando la postura de seguridad".

Recuerda durante su intervención Raúl Guillén, Cybersecurity Strategy Director de Trend Micro, que los ataques han cambiado. Se ha pasado de modelos de ataques indiscriminados y por

"Por el momento la poca nube que hay es privada del Ministerio del Interior"

Rosalía Machín Prieto,
Comandante Jefe de Proyectos TIC, **Ministerio del Interior – Secretaría de Estado de Seguridad**

fuerza bruta a ataques dirigidos "que no siempre van contra la gran empresa", y de ataques que buscan un rédito económico a otros que buscan hacer daño "por estar en un lado o en otro de un conflicto". Está de acuerdo en que lo importante que es establecer medidas de seguridad en la cadena de suministro "porque al final lo que está haciendo es extender de forma masiva y elástica la superficie de ataque" y en que lo primero que se tiene que abordar a la hora de establecer la postura de seguridad es "hacer un levantamiento de activos. Vamos a hacer un levantamiento de riesgos y vamos a analizar cómo esos riesgos de seguridad se traducen a riesgos de negocio".

La aproximación de Trend Micro es "ayudar a los clientes sin modificar su ecosistema de soluciones actuales, porque entendemos que no existe un cliente que tenga todo con Trend Micro", dice Raúl Guillén. La aproximación de la compañía es "establecer modelos de plataforma de seguridad unificada donde tengamos conexiones e interacción con fabricantes líderes de Zero Trust". Explica el directivo de Trend Micro que el concepto de plataforma se alimenta con orquestación y automatización, "pero sobre todo vamos a ser capaces de medir el riesgo en el tiempo", porque lo importante, incide Raúl Guillén, "es cómo evoluciona tu nivel de exposición y de riesgo en el tiempo". Con ese fin, la compañía ha desarrollado una plataforma a la que se incorpora telemetría y *data lake* en múltiples vectores, identidades y orígenes para

Los entornos híbridos combinan tecnología local, nube pública y nube privada. Esta combinación ofrece una serie de ventajas, pero también presenta algunos retos de seguridad

medirla en el tiempo. Y aportar, además, información de valor".

Menciona también la incorporación de inteligencia artificial para que "nos ayude a hacer más eficiente nuestro trabajo. Para que medir el nivel de riesgo durante el tiempo se pueda hacer de una forma sencilla, y veamos si estamos yendo mejor o estamos yendo a peor", y apuesta por seguir el Esquema Nacional de Seguridad (ENS) porque "no hay que inventar la rueda".

La seguridad y disponibilidad de los datos

También se plantea durante el debate cuáles son los principales desafíos que enfrenta una organización al asegurar la disponibilidad de los datos en los entornos híbridos, donde no solo hay que tener en cuenta la heterogeneidad de los entornos, sino la complejidad de las soluciones, la falta de visibilidad o los cambios continuos.

La experiencia de Alejandro Expósito es la de trabajar con muchos tipos de datos y muy segmentados, incluso los que, por ley, se deben tener de por vida. Y es que las empresas pueden estar obligadas a conservar datos durante un periodo determinado, o incluso de forma indefinida, en función de la actividad que desarrollen o de las obligaciones contractuales que tengan con terceros. Por ejemplo, las empresas que prestan servicios de telecomunicaciones están obligadas a conservar los datos de tráfico de sus clientes durante seis meses. Las empresas que gestionan sistemas de seguridad están obligadas a conservar los registros de acceso a los sistemas durante un periodo de tiempo de-

terminado, que puede variar en función de la sensibilidad de los datos que se procesen.

En opinión de Alejandro Expósito, “la política de retención del dato, independientemente de dónde esté, es el mayor reto asociado con la protección del dato”. Apunta también que los datos que tienen que guardarse durante mucho tiempo no suelen almacenarse en la nube, porque “es carísimo”, y añade que, el mayor reto del dato con el que se trabaja habitualmente no es tanto la disponibilidad de ese dato, sino el control del dato “porque el mayor problema dentro de la industria no es el dato que no tienes. El problema es que tengas un dato que no debes tener”.

Hablando de los retos del dato en entornos heterogéneos, menciona Axier Amo Izarra la apertura de los datos debido a la Ley de Transparencia y su impacto desde el punto de vista de la ciberseguridad. Menciona también la dificultad que existe en ocasiones cuando se pasan datos de una Comunidad a otro, lo que le lleva a hablar de la necesidad de contar con protocolos establecidos “por lo menos para intercambiar algunos tipos de datos”.

> “Es importante controlar qué cosas tienen visibilidad sobre qué otras cosas o qué usuarios tienen acceso a qué sitios”
>
> **Asís Pardo Martín,**
> Co – CEO **Tuio**

Hablando de los datos, dice Jesús Valverde Romero que hay que tener en cuenta que la información esté disponible en el momento en que se necesita y no olvidar la que tenemos en manos de un tercero “y que tenemos que protegerla de verdad, con copias de seguridad robustas y confiables, para poder rescatarla si es necesario”.

En pleno proceso de transformación digital, para Antonio Galán, CIO de Grupo Hierros Alfonso, “el reto es ir a la nube y controlar el dato”. Explica Rosalía Machín Prieto que en todo lo relacionado con la calidad del dato, la disponibilidad o integridad, “tenemos que atender a los reglamentos y las direcciones europeas. Para cada sistema de información, para cada proyecto que nosotros trabajamos, tenemos que trasponer esas directivas”. Añade que lo que viene marcado en ese reglamento “es lo que nosotros tenemos que trasladar a nivel técnico a nuestros sistemas de información y comunicaciones. Por ejemplo, en determinados sistemas de información está estipulado que a los seis meses, si no hay un mandamiento judicial o hay una orden de investigación de esa persona, ese dato se tiene que destruir, porque es un dato muy sensible”.

Hablando de la interoperabilidad, explica la Comandante Jefe de Proyectos TIC del Ministerio del Interior – Secretaría de Estado de Seguridad, que lo primero que se busca es la integri-

dad del dato, “porque es lo principal para luego tener otro tipo de aplicaciones, como la integración de procesos de inteligencia artificial o automatización de los sistemas”. Asegura que la interoperabilidad es muy importante para la administración pública, y que hay normativas que abogan por esa interoperabilidad de los sistemas nacionales de la propia administración, tanto a nivel autonómico como en el nivel de Ayuntamientos, como a nivel de administración general del Estado.

Menciona que se necesitan protocolos de comunicación comunes para poder compartir los datos en toda Europa, pero que hay que tener en cuenta que el hecho de que los 27 Estados miembros trabajen con los mismos protocolos de comunicación requiere de grandes inversiones muy fuertes; “lo mismo ocurre si lo trasladamos a nivel nacional. Cada uno trabaja con unos protocolos de comunicación y una infraestructura determinada. Se han ido realizando desarrollos para las necesidades que se tenían en un determinado momento y ahora hay que establecer otros protocolos de comunicación”.

Asegurando que una de cada dos organizaciones ya trabaja con entornos híbridos y que el perímetro de seguridad se ha extendido hacia diferentes lugares, dice Luigi Semente, Regional Alliance Manager de Veeam Software, que existen diferentes herramientas que permiten mejorar el punto más crítico, “que no es otro que la visibilidad”. Añade que la propuesta de Veeam es unificar y simplificar la protección de los datos garantizando la disponibilidad “con la visión de ser parte de un ecosistema”, porque, aseguraba, “uno de los aspectos más relevantes es tener una plataforma que sea abierta y se pueda comunicar con los otros elementos que están en el mapa tecnológico”.

> “Saber no sólo dónde estamos sino hacia dónde vamos es clave para tener un proyecto que me permita tener todos los datos en orden”
>
> **Luigi Semente,**
> Regional Alliance Manager, **Veeam Software**

El concepto de plataforma abierta “permite aprovechar lo mejor de cada casa”, aseguraba Luigi Semente explicando que cuando se trata de la disponibilidad del dato, una plataforma ayuda a hablar con los diferentes actores, desde el CPD a un proveedor de almacenamiento, pasando por un hiperescalar, “e ir utilizando lo que es más conveniente según el caso de uso y aprovechar las inversiones”.

Tiene claro el directivo de Veeam que es relevante conocer cuáles son tus datos y de dónde llegan. Menciona como uso más frecuente en las empresas el de Microsoft 365 para aclarar que es un proveedor de hiperescalar “que te garantiza la disponibilidad de la infraestructura” para añadir que “el dato es responsabilidad del cliente”

Considerando todos los elementos deja claro

Luigi Semente que para Veeam la clave es “simplificar unificando todas las herramientas, hablar con los diferentes actores y saber no sólo dónde estamos, sino hacia dónde vamos. Esa es la clave para tener un proyecto de disponibilidad que me permita de tener todos los datos en orden”.

Sale a colación la importancia de la figura del DPO precisamente ahora que estamos en la era del dato, en la era digital, y cuando se están implantando procesos de IA y otros que están mejorando la utilidad de los datos. “El DPO sería una herramienta esencial en cualquier tipo de organización”, dice Rosalía Machín.

IA, ataques y cuantificación de riesgos

“Tenemos que ser muy precavidos respecto a introducir procesos de inteligencia artificial en todos los sistemas de información”, explica la Comandante Jefe de Proyectos TIC de Ministerio del Interior – Secretaría de Estado de Seguridad cuando planteamos qué uso se está haciendo de la IA para proteger de ataques que muchas veces vienen impulsados por inteligencia artificial, y cómo se cuantifican los riesgos a los que se ven sometidos las empresas. Menciona que no se hace uso de la IA generativa, sino de la IA supervisada, utilizada, por ejemplo, en el sistema de seguimiento VioGén, creado por el Ministerio del Interior en 2007, o para hacer un seguimiento de los llamados ‘vuelos calientes’. Asegura Rosalía Machín que se mantendrá la tendencia de utilizar la IA dentro del Ministerio del Interior, “como herramienta de apoyo a la decisión”, y asegura que hasta que no se consolide la Ley de Inteligencia Artificial por parte de la Comisión Europea, “nosotros no vamos a seguir en otra dirección”.

> “El que de verdad sabe quién se está autenticando en cada caso es Okta”
>
> **Iván Rodríguez,**
> Solutions Engineer, **Okta**

Aclara también la comandante Machín que una cosa es la automatización y otra el análisis con procesos de IA aplicados a sistemas de información de gran magnitud. “No hay, a día de hoy, un caso de éxito en ninguno de los proyectos en los que nosotros hemos intentado aplicarlo”, asegura Rosalía Machín.

Asegurando que la inteligencia artificial tiene que ser una herramienta para que los trabajadores sean más eficientes a la hora de hacer su trabajo, explicaba Jesús Valverde que, en el caso de una empresa como Isemaren, donde no existe un departamento interno con personal y medios suficientes; “lo que se necesita es que el *partner* y la solución con la que estoy trabajando, esté implementada en muchos clientes y sea capaz, utilizando inteligencia artificial, de extraer esa inteligencia de amenazas para protegerme a mí anticipándose mediante los IOCs que puedan estar afectando a otras empresas”. Añade que en Isemaren sí se está haciendo uso de la inteligencia artificial internamente en va-

rios proyectos, uno de los cuales fue crear un *tenant* específico para hacer experimentos con gaseosa y no con datos reales, “porque la mayoría de las herramientas, *plug-ins* o aplicaciones, lo primero que te piden es acceso a los datos”.

Tiene claro Axier Amo Izarra, Director General de Transparencia y Buen Gobierno, Gobierno de la Rioja, que la inteligencia artificial semántica, junto con el conocimiento, lo que aporta es una herramienta que acerca al ciudadano con la institución. Menciona también la ética de la inteligencia artificial, y asegura que es un terreno en el que se camina despacio.

Recordando que el término Inteligencia Artificial es muy amplio, explica Asís Pardo Martín, Co – CEO de Tuio, que el *machine learning* es el uso más extendido porque “es más seguro de aplicar y en usos, como detección de fraude o tarificación, tiene una muy buen aplicación”. Añade que dentro de su compañía se han creado varias líneas de desarrollo con IA generativas “que empezaremos a utilizar en breve, pero siempre como copiloto” porque “siempre es imprescindible esa figura del humano tomando la decisión final”.

> “Nuestra propuesta es establecer modelos de plataforma de seguridad unificada donde tengamos conexiones e interacción con fabricantes líderes de Zero Trust”
>
> **Raúl Guillén,**
> Cybersecurity Strategy Director, **Trend Micro**

Alejandro Expósito ha trabajado con Inteligencia Artificial y asegura que la IA tiene el potencial de revolucionar la investigación. Al automatizar tareas, analizar grandes cantidades de datos y generar nuevas ideas, la IA puede ayudar a los investigadores a encontrar nuevas formas de ahorrar recursos y proteger el medio ambiente. De hecho, según este experto el uso de la IA podrá ahorrar, hasta 2025, 85 billones de dólares en el desarrollo de medicamentos.

Inicia su intervención Alberto Maldonado, Regional Sales Director de Zscaler, asegurando que, dentro del mundo tecnológico, lo que más ha cambiado es el software. Un cambio que ha impactado sobre todo en mejoras en productividad, “y ahora está pasando también algo extraordinario con la inteligencia artificial, que tiene el potencial de impactar y mejorar la productividad del 70 por ciento de todos los empleos del mundo”.

Añade que también ha habido una transformación de las aplicaciones, de los recursos y de cómo se consumen esos recursos, que ha habido una transformación del uso de Internet, y que, a pesar de ello, se siguen utilizando conceptos de hace 25 años, como las VPN.

Zscaler nace de esa transformación de las aplicaciones y de la red, así como del consu-

> “Creemos que estos cambios estructurales en las aplicaciones y en los recursos, también necesitan un cambio radical”

Alberto Maldonado,
Regional Sales Director, **Zscaler**

mo de esas aplicaciones. “Creemos que estos cambios estructurales en las aplicaciones y en los recursos, también necesitan un cambio radical”, asegura el directivo, explicando que lo que ha desarrollado Zscaler es una nube distribuida “donde nosotros somos el *broker* en el medio, de forma que cada una de las transacciones que se realicen con la nube pasen por la nube de Zscaler, que es quien decide si, por política empresarial, un usuario puede acceder a una aplicación o recurso”. Apuesta Zscaler por resolver de golpe los tres elementos fundamentales a los que se enfrenta cualquier empresa: coste, experiencia de usuario y seguridad, explica Maldonado.

A la hora de hablar de Inteligencia Artificial explica Alberto Maldonado que Zscaler puede ayudar a las empresas ofreciendo visibilidad de quién se conecta a qué, y responder preguntas como ¿están mis usuarios utilizando Chat GPT? También comenta el directivo que la compañía lleva realizando unas fuertes inversiones en inteligencia artificial desde hace años y que, teniendo en cuenta la enorme cantidad de transacciones que pasan por su red (300.000 millones de transacciones diarias), son capaces de “calcular la probabilidad de que algo pase en vuestras organizaciones”.

“El valor de Okta es ser neutral”

Asegurando que Okta es la empresa líder en el sector de gestión de identidades, con más de 18.000 clientes, que asegura que “tú eres tú de verdad y eres capaz de entrar a esos recursos que de verdad tienes que entrar”.

Como solución integral en cuanto a gestión de entidades, Okta no solo se dedica a la parte de Identity and Access Management (IAM), sino a la gestión del gobierno de la identidad (IGA), o a la gestión de acceso privilegiado (PAM), todo ello integrado en una única plataforma que permite tener “una visión holística de lo que está ocurriendo en todo momento en la plataforma con respecto a la identidad”.

Preguntado por el diferencial de Okta, asegura Iván Rodríguez que es ser neutral, lo que significa que “nos integramos con cualquier fabricante del mercado”.

Iván Rodríguez, Solutions Engineer **Okta**

“Ayudamos a que el modelo de respuesta y resiliencia de las compañías sea más eficiente”

Asegurando que se busca hacer más eficiente el modelo de respuesta y resiliencia de las empresas, para lo que se parte de un análisis de la postura de seguridad y los riesgos de negocio, asegura Raúl Guillén, Cybersecurity Strategy Director de Trend Micro, que la respuesta pasa por una plataforma unificada.

Menciona un contexto complejo que influye en la seguridad: la polarización geopolítica, que modifica cómo y desde dónde se atacan a las compañías; una cadena de suministro que extiende el nivel de riesgo; una brecha de talento importante; el paradigma del mundo interconectado que hace converger la informática tradicional con la operativa o industrial... “Al final, todo esto provoca que debamos tener múltiples vectores de protección en un modelo donde la eficiencia operativa tiene que ser uno de los principales indicadores”.

Raúl Guillén, Cybersecurity Strategy Director, **Trend Micro**

“Veeam ofrece protección avanzada y gestión inteligente de los datos

El objetivo de Veeam es “garantizar la disponibilidad de los datos de una forma moderna”, dice en el vídeo Luigi Semente, Regional Alliance Manager de Veeam.

Menciona la visibilidad como uno de los principales desafíos a los que se enfrentan las empresas para proteger los datos y habla de simplificar y formar parte del ecosistema como una de las soluciones a estos desafíos.

A la hora de ayudar a proteger los datos, la aproximación de Veeam pasa por “dar liberada a nuestros clientes de elegir cómo proteger sus datos y dónde tener esos datos, cómo mejorar la resiliencia del negocio, cómo dar una mejor continuidad de negocio, y cómo mejorar la postura de seguridad de nuestros clientes”.

Luigi Semente, Regional Alliance Manager, **Veeam Software**

“Para que te ataquen primero te tienen que encontrar”

“Desde Zscaler, nuestra misión es asegurar y permitir que las compañías puedan hacer su trabajo”, lo dice Alberto Maldonado, Regional Sales Director de Zscaler, añadiendo que “para asegurar cambios transformacionales de la tecnología, se necesita un cambio en la arquitectura de seguridad”.

Explica el directivo que Zero Trust Exchange es una plataforma nativa de la nube que conecta y protege a los usuarios, las cargas de trabajo y los dispositivos a través de cualquier red desde cualquier ubicación y que ayuda a resolver tres problemáticas: experiencia de usuario, costes, y riesgos de seguridad.

Respecto a esto último, comenta Maldonado que para que te ataquen primero te tienen que encontrar y “Zscaler reduce tu superficie de ataque porque nos situamos antes”; además, apuesta por Zero Trust Network Access, que permite no conectar a usuarios y recursos directamente a la red.

Alberto Maldonado, Regional Sales Director, **Zscaler**