THE STANDARD CIO | INFORMACIÓN 360° ESTRATEGIA

CIBERSEGURIDAD 2024:

Desafíos y soluciones en la era de la Inteligencia Artificial

> En un paisaje digital cada vez más complejo, la colaboración entre CISOs y CIOs se vuelve imprescindible para enfrentar los desafíos que plantea la Inteligencia Artificial generativa en la ciberseguridad empresarial

Hugo Riveros, Gerente de Ingeniería de Netskope para Latinoamérica.

CISOs y CIOs están cada vez más unidos frente a la junta directiva

Hugo Riveros
Netskpoe

La irrupción de la Inteligencia Artificial generativa está marcando la demanda de las Juntas Diasdrectivas por innovación. Pero, también, representa un grave riesgo a la ciberseguridad de usuarios y empresas.

Los avances de la Inteligencia Artificial generativa (GenIA) están escalando las amenazas de ciberseguridad para las empresas. Esto fue lo primero que destacó el Gerente de Ingeniería de Netskope para Latinoamérica, Hugo Riveros, durante su participación en las primeras Jornadas Digitales sobre Ciberseguridad de The Standard CIO.

Para ilustrar su convicción refirió que basta con ver cómo el muy conocido fraude de simulación de secuestros se ha mudado del ámbito doméstico al corporativo. ¿Cómo? Apoyado en herramientas de suplantación de voz basadas en IA generativa.

Para Riveros, esto es una muestra de cómo la GenIA está llevando la innovación de lado de la ciberdelincuencia, colocando presión adicional tanto sobre el CISO como sobre el CIO.

De hecho, este es el segundo impacto relevante que el especialista de Netskope destacaría sobre los que la GenIA traerá en el ámbito de la ciberseguridad durante para 2024.

“Las juntas directivas están demandando más información tanto de Inteligencia Artificial como de ciberseguridad. Eso hace que tanto el CIO como el CISO sean cada vez más escuchados en esta instancia”, explicó Riveros.

IA y Ciberseguridad: doble desafío

En lo que se refiere a Inteligencia Artificial, Riveros refirió que, el principal desafío que tienen, tanto el CIO como el CISO para satisfacer la necesidad de información, formación e innovación de Junta Directiva es la ciberseguridad.

¿Por qué? Pues porque para aprovechar todas las oportunidades de generación de productos y servicios que permite anticipar esta tecnología, es necesario que se sienten las bases en las organizaciones para cerrar las brechas y neutralizar las amenazas.

Y estas son cada vez mayores porque los ciberdelincuentes utilizan, sin reservas, todas las posibilidades que ofrece la GenIA.

“La junta directiva está demandando entrenamiento para ser más productivos, utilizando estas nuevas herramientas generativas. Pero ello debe hacerse sin resultar peligrosamente expuestos. Ese es el reto que deben resolver juntos el CIO y el CISO”, resaltó Riveros.

GenIA en ciberseguridad: cara y sello

La buena noticia es que queda claro que la GenIA no está sólo del lado de la ciberdelincuencia.

Por el contrario, el especialista hizo notar que ya hay herramientas en el mercado que permiten indicarle a sus clientes dónde están sus brechas en sus sistemas, ya sea en navegación, apps o en programas legados.

“Es fundamental que los ataques de malware generados por GenIA sean combatidos con soluciones que también tengan esta tecnología. Es la forma de que podamos dormir tranquilos”, enfatizó Riveros.

Pero, para que esto sea realmente efectivo es necesario:

- Formar e informar al personal de los riesgos
- Establecer políticas para el uso de la información y los sistemas
- Crear normas que eviten vulnerabilidades en nuestros sistemas como prompts mal construidos
- También llegar a acuerdos en la organización sobre la mejor manera de aprovechar la herramientas, con una mínima exposición

Todas estas tareas deberían estar en la agenda de ciberseguridad para 2024.

Enlace al video

Accede al vídeo de la charla: Nuevos retos ante las amenazas habilitadas por la IA, con Hugo Riveros, Gerente de Ingeniería para Latinoamérica de Netskope.

> 2024 será el año de la autenticación multifactorial, donde la lucha contra el aumento de ataques financieros potenciados por la Inteligencia Artificial será crucial. Las defensas tradicionales serán vulneradas, incluso la identificación biométrica.

Fabio Assolini, Director de Análisis e Investigación de Kaspersky para América Latina.

Kaspersky: Crecen los ataques financieros potenciados por IA

Fabio Assolini
Kaspersky

El liderazgo de Brasil en la generación de malware de última generación, potenciado por IA, mantendrá las amenazas crecientes en la región. Según Kaspersky, la mayoría de los ataques de 2024 tendrán propósitos financieros.

Fabio Assolini, Director de Análisis e Investigación de Kaspersky para América Latina, sostiene que la mayoría de las amenazas de ciberseguridad que se verán en la región este año serán de tipo financiero.

En general, el especialista señala que, para puntualizar el pronóstico de los tipos de ataques que tendremos hay que asumir dos cosas:

- Que los ataques serán del mismo tipo de los que padeció la región durante el año 2023.
- Que, en la mayoría de los ataques porvenir, interviene de una u otra forma, la Inteligencia Artificial.

Una tercera conclusión que puede deducirse de la intervención de Assolini es que el número de fraudes va a aumentar en la región, siempre con la IA generativa (GenIA) como acelerador.

Una cuarta consecuencia de lo que son las proyecciones presentadas por Kaspersky en las Jornadas Digitales de TSCIO sobre Ciberseguridad, es que muchas de las herramientas que la región ha venido cultivando como defensas serán vulneradas por el uso de GenIA.

La autenticación como reto

¿Por qué asegura esto Assolini? Pues, porque la identificación biométrica - una de las estrategias más importantes que se ha venido implementando en la región - ya ha sido vulnerada por talento local.

Así, el director de Kaspersky refirió el caso de un hacker brasileño que hizo público su capacidad para burlar la identificación facial de la banca, utilizando técnicas de deepfake con IA.

“Esto no es un pronóstico. Está ocurriendo en este momento. Crear cuentas bancarias con identidades falsas para realizar fraudes ya es posible, gracias a esta tecnología”, explicó el Director de Análisis e Investigación de amenazas de Kaspersky para América Latina.

Así que, además de las amenazas ya conocidas y que han venido azotando la región, hay que encarar las versiones 2.0 con inteligencia artificial.

Ejemplo de ello (además de la biometría) es el del phishing. Kaspersky anticipa que aumentará el número de campañas anuales debido a que, gracias a la GenIA, los atacantes pueden escribir correos electrónicos como si fueran nativos de un idioma en particular.

Es decir, el mundo de los atacantes ya no tiene fronteras idiomáticas. Otra amenaza que luce exponencial gracias a la IA es la de los objetos conectados que, por ser vulnerables desde su programación, constituyen un blanco fácil.

Contar + identificar = Proteger

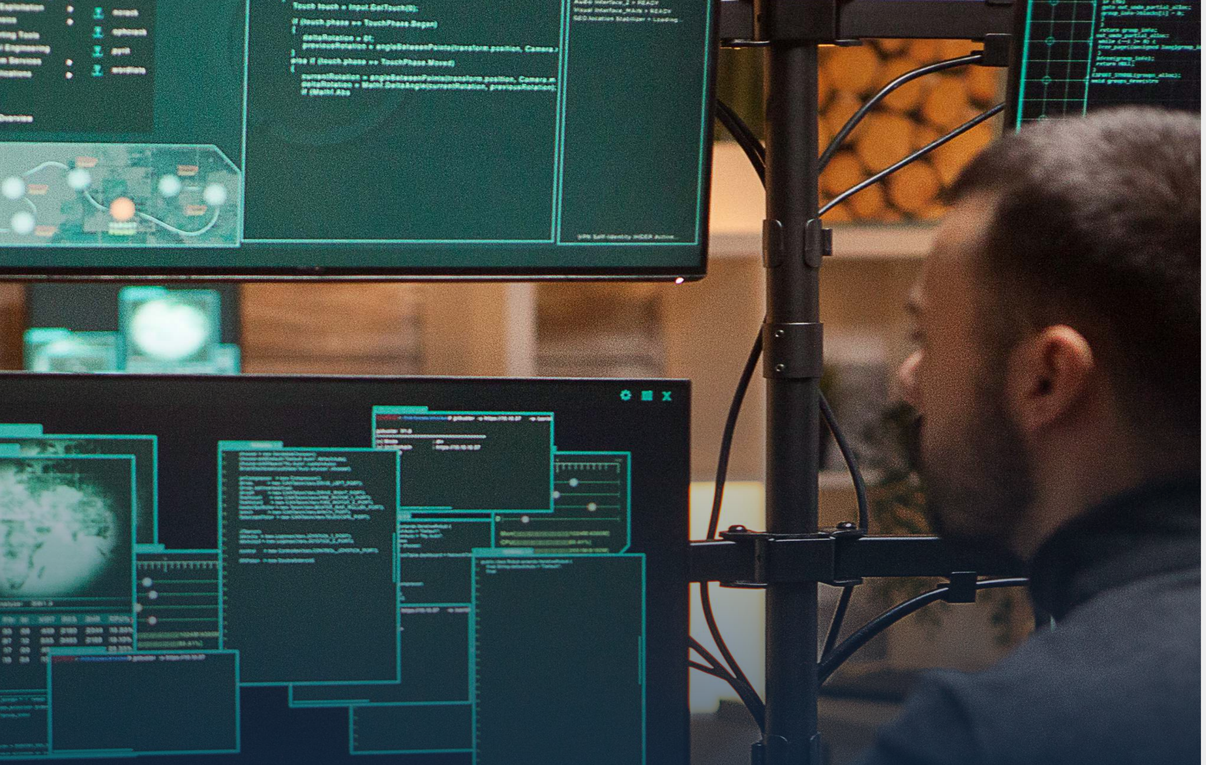
Otra amenaza en ascenso debido a la IA son los objetos conectados, vulnerables desde su programación y por ende, un blanco fácil para los ciberdelincuentes.

Kaspersky anticipa incluso ataques de denegación de servicio distribuido (DDoS) iniciados desde estos dispositivos, subrayando la necesidad de prepararse para amenazas emergentes en el ámbito de la Internet de las cosas (IoT).

Frente a este escenario y la creciente adopción del trabajo híbrido o remoto, Assolini enfatiza la importancia de contar con sistemas de Inteligencia de Amenazas para anticipar y mitigar riesgos. Sin embargo, para que estas medidas sean efectivas, las empresas deben tener un inventario completo de sus activos en red y aplicar políticas de Confianza Cero, asignando privilegios de manera selectiva para reducir el riesgo colectivo de la organización.

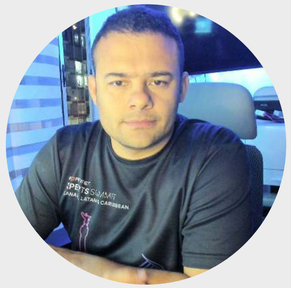
Enlace al video

Accede al vídeo de la charla: Predicciones en ciberseguridad para 2024, con Fabio Assolini Director de Análisis e Investigación de Kaspersky para Latinoamérica.



> La nube no se cuida sola. Con este mantra de David Gallego de Fortinet resalta la importancia de reconocer que la seguridad en la nube requiere una estrategia proactiva. La concientización y la implementación de medidas de seguridad, tanto en entornos on-premise como en la nube, son cruciales para garantizar la eficiencia operativa en un mundo cada vez más digitalizado.
>
> David Gallego, Cloud Business Engineer para Latinoamérica de Fortinet

Ciberseguridad en nube crecerá 60% este año



David Gallego
Fortinet

La nube no es un espacio libre de ciberamenazas y menos con el uso de la Inteligencia Artificial desde el lado oscuro. En 2024, los ataques con IA retarán las defensas de los ecosistemas cloud.

“La nube no se cuida sola”. Aunque esto podría parecer obvio, David Gallego, Cloud Business Development Engineer de Fortinet para Latinoamérica, enfatiza la frase y asegura que es el primer paso para desarrollar una estrategia de ciberseguridad eficiente.

Porque las amenazas han llegado a los ecosistemas de nube. Por lo general, lo hacen de la mano de los usuarios y sus dispositivos.

Tal es la preocupación por mantener los datos de las empresas resguardados que un estudio realizado por Fortinet señala que la seguridad en la nube podría tener un incremento del 60%, sólo en 2024.

Dicha perspectiva supone que ya las empresas han descubierto que los datos no van a estar seguros sólo por estar en la nube. Es decir, muestra un avance en la conciencia hacia lo que, para Gallego, es el primer paso.

El segundo paso para mantener la seguridad de los datos en la nube es atender, formalmente, el asunto de la identidad y la debida autenticación.

“Las empresas no sólo deben cumplir con los requisitos de la legislación, en aquellos países en los que hay. Las empresas deben asegurarse que los usuarios que ingresan a su nube son los que deben utilizarla”, precisó el especialista de Fortinet.

Observabilidad y exclusividad

En este punto, Gallego reconoció que, dependiendo de con cuál modelo migremos a la nube, así será el tipo de mantenimiento, seguridad y responsabilidad que vamos a tener para la gestión.

“La ciberseguridad y sus requerimientos suelen quedar olvidados hasta el final. Es decir, cuando ya se ha migrado y hay que atender al mantenimiento de los datos”, comentó el especialista.

La observabilidad se convierte en un desafío clave, ya que no se puede proteger lo que no se puede ver ni comprender.

Conocer qué datos se están llevando a la nube es fundamental para establecer una estrategia efectiva de ciberseguridad, que a menudo implica considerar varios niveles de seguridad dependiendo del modelo de servicio en la nube (IaaS, SaaS, CPaaS, etc.).

Déficits crecientes

La ampliación de los perímetros debido a la nube presenta desafíos adicionales, especialmente en una región con escasez de talento especializado tanto en ciberseguridad como en computación en la nube.

La convergencia de habilidades en ambos campos es altamente valorada en las organizaciones, y contar con soluciones como las ofrecidas por Fortinet, que se adaptan fácilmente del entorno local a la nube, es una ventaja significativa.

Finalmente, Gallego considera que los elementos imprescindibles en la estrategia de los CIOs para este y todos los años incluye:

- Concientización sobre la responsabilidad compartida en la seguridad de la nube.
- Seguridad tanto en la red on premise como en la nube.
- Esta seguridad en doble ambiente debe verse como crucial para lograr la eficiencia operativa.

Enlace al video

Accede al vídeo de la charla: Ciberseguridad en la Nube: Grandes desafíos, con David Gallego, Cloud Business Development Engineer para Latinoamérica de Fortinet.

> “Las empresas deben avanzar en la comprensión de una cultura de la ciberseguridad, del riesgo, de la prevención. Hay que entender que las personas son la última línea de defensa
>
> Yair Lelis, Director de Ciberseguridad de Cisco México.

La gente, factor clave en la gestión de incidentes

Ricardo Trotti
Nubity

Yair Lelis
Cisco

Según los especialistas de Cisco y Nubity presentes en las Jornadas de Ciberseguridad de The Standard CIO, el mayor desafío para las empresas es entender la necesidad de crear una cultura de ciberseguridad.

Contar con políticas de prevención, planes, simulacros y herramientas es insuficiente si la organización no se alinea en esta estrategia.

Ricardo Trotti, COO de Nubity y Yair Lelis, Director de Ciberseguridad de Cisco México no dejaron espacio para las ilusiones: los incidentes de ciberseguridad van a seguir ocurriendo.

El ransomware y el phishing siguen siendo problemas de impacto creciente, según lo indican las cifras y estudios recientes de Talos que comentó Lelis. En el caso del ransomware, se mueve a sectores con menos capacidad para permitirse fallos, como lo es el sector salud.

En estos casos, señaló el ejecutivo, pasamos directamente de los intentos de amenaza de encriptación a la pura y llana extorsión.

Y esto es parte de lo que seguiremos viendo.

“Estamos ante una película en desarrollo que convive con las realidades cotidianas de las empresas que incluyen la escasez de recursos y su necesidad de asignarlos de la mejor manera”, afirmó el COO de Nubity, Ricardo Trotti.

Una defensa colectiva

Frente a este escenario, las herramientas son insuficientes según destacó el ejecutivo de Nubity. Por ello, se impone que las empresas desarrollen una auténtica cultura que les permita resguardarse de las amenazas y hacerle frente a los incidentes, cuando ocurran, de una manera articulada.

En esto coincide con el ejecutivo de Cisco, así como en la necesidad de desarrollar planes y simulacros de ataques que permitan aprender lo que debe hacerse durante estos incidentes.

No obstante, recordó Trotti que no todas las empresas están en el mismo nivel de madurez.

Por ello los planes tienen que adecuarse a las condiciones de cada empresa.

A ello sumó Yair Lelis que, al igual que una herramienta de recuperación de desastres, es útil contar una póliza de seguros ante ciberataques.

“Esto ayuda siempre que no se vea como un elemento que resuelve el problema o que es suficiente. Las empresas deben avanzar en la comprensión de una cultura de la ciberseguridad, del riesgo, de la prevención. Hay que entender que las personas son la última línea de defensa”, puntualizó el ejecutivo de Cisco.

Para Lelis, esto sólo es posible en una gestión que:

- Realizó un inventario para saber en qué punto está
- Tiene políticas para desarrollar una cultura.
- Cuenta con un plan para saber qué hacer en cada área y cada persona ante un incidente.

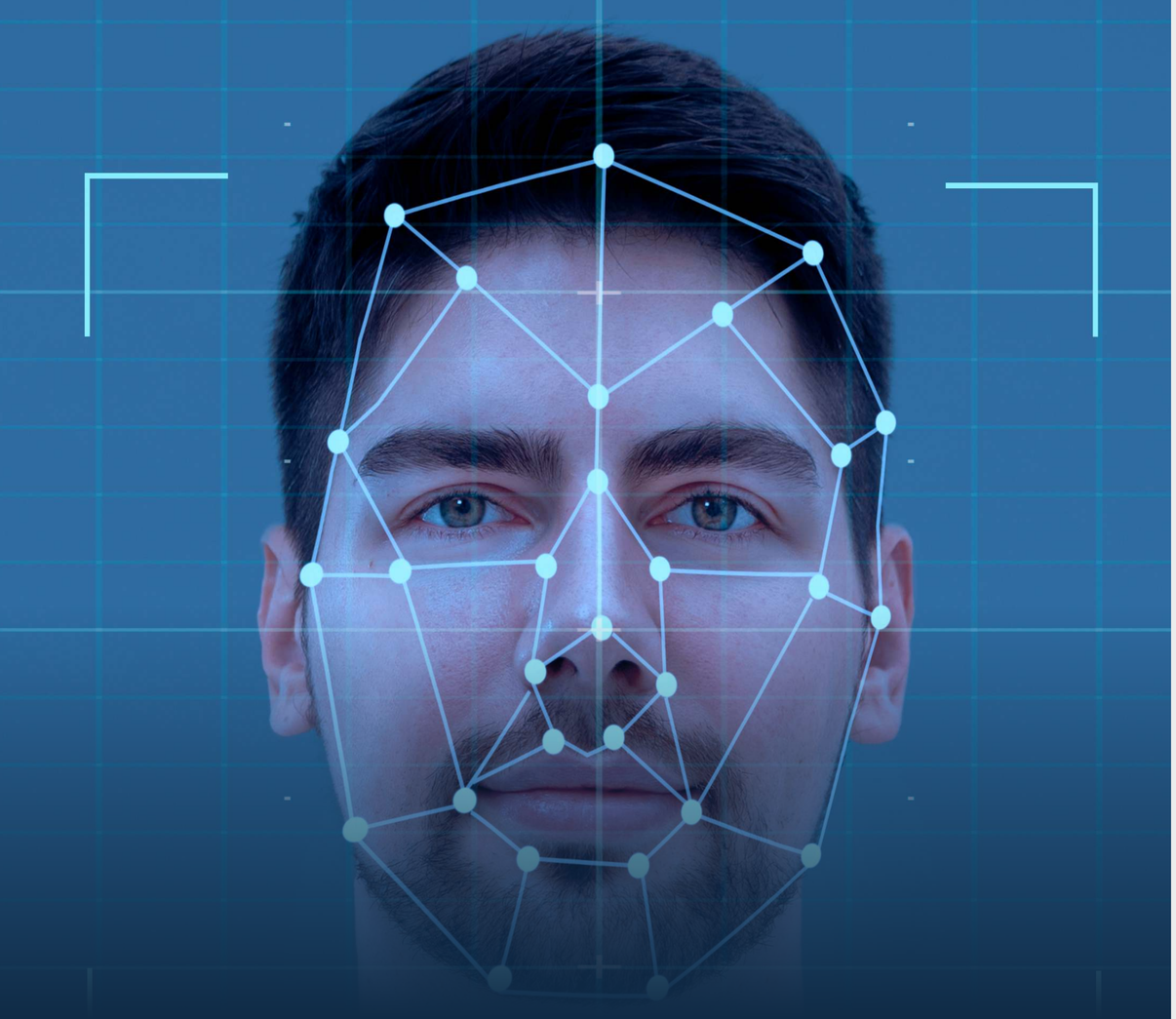
Promover los avances

Los especialistas reconocen la necesidad de una legislación para tipificar las amenazas y responsabilidad entre las empresas en torno a la ciberseguridad. Políticas de Estado para la prevención de ataques como en Israel o una clara discriminación de los delitos como la que existe en Reino Unido, fueron referentes en la conversación.

A Latinoamérica le queda trecho por andar. Por ello, el sector privado debe presionar para lograr propuestas legislativas, en base a la experiencia que ya tenemos.

Enlace al video

Accede al vídeo de la sesión: Gestión de incidentes y respuesta ante ataques; con la participación de Yair Lelis, Director de Ciberseguridad Cisco México y Ricardo Trotti, COO de Nubity.



> Vamos avanzando al mundo sin contraseñas del que hablaba Bill Gates a principios de milenio. Hoy, aunque existen, se combinan con otros factores de autenticación
>
> Sergio Muniz, Jefe de Seguridad y Acceso en Thales Cloud Security

2024: el año de la Gestión de Acceso

Ricardo Robledo
Nubity

Juan Pablo
Yague

Sergio Muniz
Thales

En la sesión final de las I Jornadas de Ciberseguridad de The Standard CIO se abordó el espinoso tema de la identidad digital. Los expertos destacaron el papel crucial de la inteligencia artificial en mejorar los motores de búsqueda y procesamiento de datos biométricos, así como la importancia de estrategias de Zero Trust

En el contexto de las Jornadas Digitales sobre Ciberseguridad, un panel de tres especialistas abordó las complejidades de un mundo que avanza hacia la biometría y la autenticación multifactorial.

Todo ello mientras va quedando atrás el uso de las contraseñas.

Transformación. Esta es la primera conclusión sobre el sector de la identidad y la autenticación que se desprende de la intervención de:

- Sergio Muniz, Jefe de Seguridad y Acceso en Thales Cloud Security
- Juan Pablo Yagüe, Gerente de Identidad Digital de Serban Group
- Y Ricardo Robledo, Director General y Fundador de Tu Identidad

Lo segundo que hay que decir de este sector es que se encuentra en plena expansión, desde el punto de vista de los negocios.

Zero Trust, biometría y tokens

Juan Pablo Yagüe, Gerente de Identidad Digital de Serban Group, señala que es necesario que las empresas establezcan claras políticas de identidad y autenticación. Estas les permitirán reducir los riesgos de filtraciones o accesos indebidos a información sensible.

“La Inteligencia Artificial (IA) está ayudando a mejorar los motores de búsqueda y procesar los datos de identificación biométrica de una manera que avanza, cada día, hasta transformarse en un estándar”, afirmó el ejecutivo de Serban Group.

Yagüe destacó que, al utilizar la IA en soluciones, esta permite adecuar las restricciones de cada usuario y perfil, dependiendo del área e información a la que está accediendo.

Por su parte, Sergio Muniz, Jefe de Seguridad y Acceso en Thales Cloud Security, considera que debe combinarse todo esto con una separación de los tipos de acceso entre colaboradores (nivel Enterprise) y los clientes (más amigable).

“La diversidad de identidades que deben de ser gestionadas, va mucho más allá del consumidor y de los empleados (empleados temporarios, proveedores, distribuidores, kioskos, puntos de venta, brokers, agentes, etc)”.

Apelar a este tipo de políticas integradas con la adopción de estrategias de Zero Trust, les permitirán a las empresas avanzar de la autenticación a una Gestión de Acceso de los datos.

Más elementos, menos riesgo

Para Robledo, aunque parezca que hay mayor complejidad, en realidad, se busca simplificar los procesos para los usuarios porque la gente es el hilo más vulnerable en la ecuación de la ciberseguridad.

Los expertos coinciden en que hay que diversificar el riesgo de los accesos, creando perfiles para que los usuarios accedan y vean toda la información, pero sólo la información que necesitan ver.

Todos los expertos están de acuerdo en que se debe:

- Sacar los procesos manuales y las contraseñas de la ecuación.
- Crear capas de acceso.
- Incorporar lo que la gente ES (biometría) en los mecanismos de Zero Trust.

En cuanto a los dispositivos, es necesario que sean otro factor para autenticar la identidad de los usuarios .

Enlace al video

Accede al vídeo del panel de expertos: Autenticación y Gestión de la Identidad en la era de la IA; con la participación de Sergio Muniz, Jefe de Identidad y Acceso en Thales, Juan Pablo Yagüe, Gerente de Identidad Digital de Grupo Serban y Ricardo Robledo, Director General y Fundador de Tu Identidad.

Dirección Editorial:

Adolfo Manaure

Redacción:

Elibeth Eduardo

Diseño:

Alberto Zavala

Presidente y Editor en Jefe:

Trino Ramos

Publisher:

Walter Mastrapa