DEBATES ciberseguridad TIC

Así se ve el salto hacia el Zero Trust inteligente

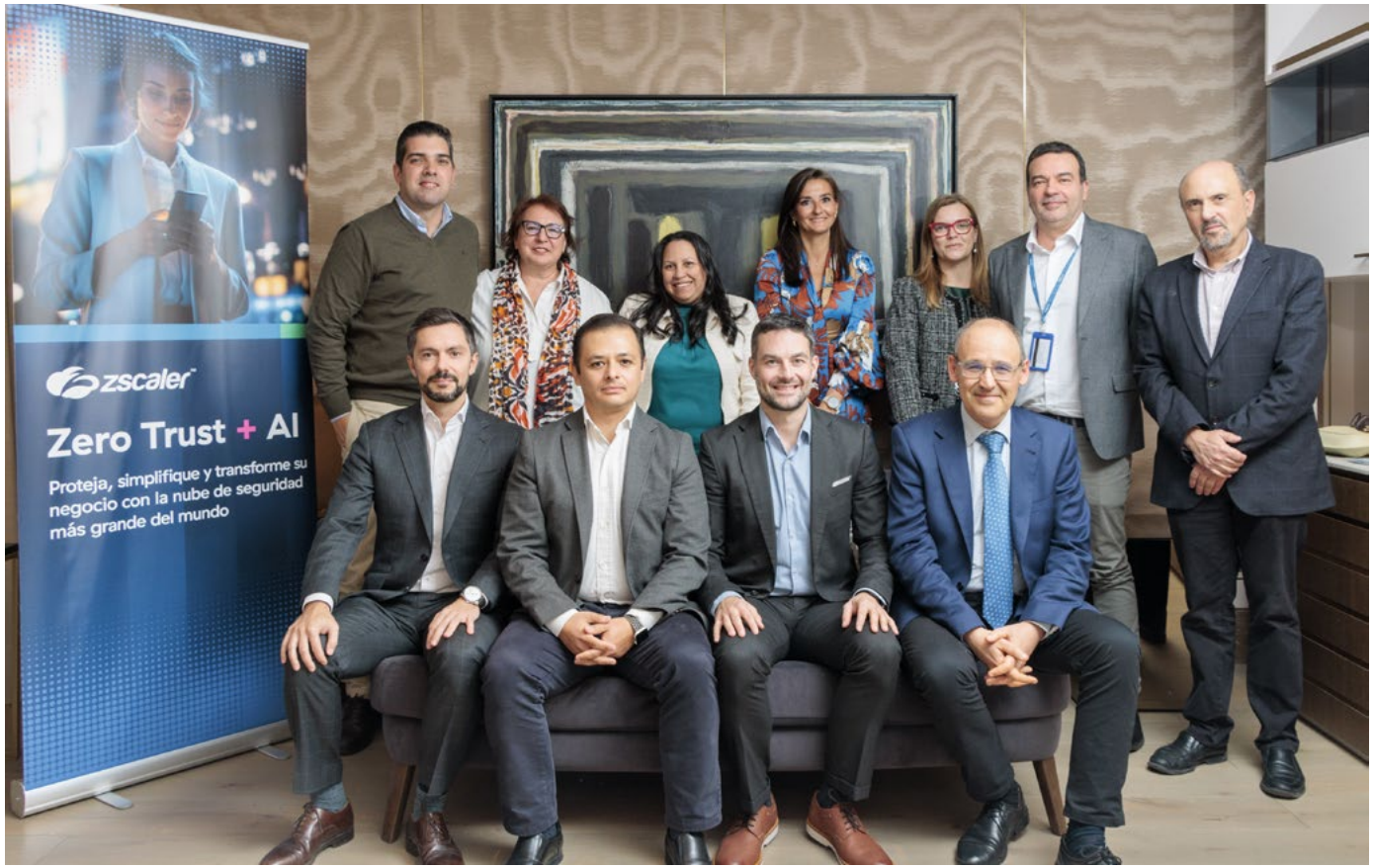
zscaler™

IR A PÁGINA SIGUIENTE

Así se ve el salto hacia el Zero Trust inteligente

En un almuerzo ejecutivo organizado por Ciberseguridad TIC y patrocinado por Zscaler, expertos de la administración pública, grandes empresas, integradores y el mundo académico debatieron sin filtros sobre la desaparición del perímetro, la complejidad tecnológica, la visibilidad, la identidad, la IA generativa y la presión regulatoria. El resultado fue una conversación honesta que refleja el momento de transición estructural que vive la ciberseguridad.

Rosalía Arroyo



La ciberseguridad atraviesa un punto de inflexión: movilidad total, nubes híbridas, datos distribuidos, dispositivos personales, identidades humanas y no humanas, agentes de IA que actúan sin supervisión y una nueva ola regulatoria que endurece responsabilidades. En este contexto, Ciberseguridad TIC celebró el almuerzo ejecutivo “¿Y si la red fuera el problema? Del firewall a la plataforma: el salto hacia el Zero Trust inteligente”, patrocinado por Zscaler, referente en arquitecturas SSE/SASE y acceso seguro basado en la nube.

El objetivo era sencillo: reunir a responsables públicos, CISOs, expertos universitarios e ingenieros de seguridad para entender cómo están abordando la desaparición del períme-

tro, qué retos encuentran en la transición hacia la identidad como núcleo, cómo encajan IA y legacy en el mismo tablero, y hasta qué punto la regulación está reformateando prioridades técnicas.

Los participantes al debate fueron: Alejandro Menéndez, experto en análisis y diseño de soluciones ciberseguridad; Diego Andrés, CISO de Prosegur Alarmas; Pablo Gálvez, Subdirector General Adjunto Unidad de Seguridad de la Información de IGAE/Ministerio de Hacienda; Rafael Rico, CISO de Atento España; Víctor Villagrá, Catedrático y Director del Máster de Ciberseguridad/Subdirector jefe de estudios de la ETS de Ingenieros de Telecomunicación, Universidad Politécnica de Madrid; Ana Sandoval, Computer Science Engineer GASS, Universidad Complutense de Madrid; a los que acompañaron Manuel Cantonero, Sales Account Executive Iberia, y Federico Gimeno, Sales Account Executive Iberia, ambos de Zscaler

Lo que se produjo fue una conversación profunda, cargada de matices técnicos y decisiones reales que hoy se están tomando en empresas, universidades y organismos públicos.

> “Todos tenemos el correo en el móvil, contestamos un Teams en un semáforo... ¿qué red corporativa es esa?”
>
> **Alejandro Menéndez,**
> experto en análisis y diseño de soluciones ciberseguridad

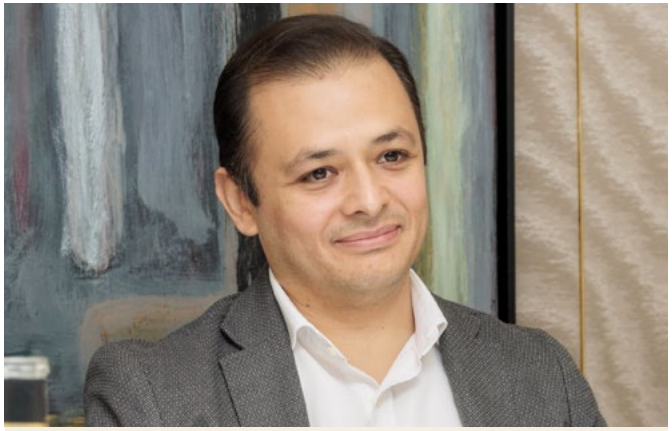
¿Existe aún la “red corporativa”?

El concepto de “red corporativa” fue durante años el eje sobre el que se construyeron arquitecturas, políticas y presupuestos. Pero el teletrabajo masivo, los dispositivos personales, el acceso híbrido y la expansión del cloud han puesto en cuestión esa idea. La primera pregunta del debate buscó aclarar si ese término sigue teniendo sentido... o si es ya un vestigio del pasado.

La primera pregunta planteada durante el debate fue directa: ¿tiene sentido seguir hablando de “red corporativa”?

Alejandro Menéndez no tardó en desmontar el concepto. Recordó que hoy “todos tenemos el correo en el móvil, contestamos un Teams en un semáforo, hacemos llamadas desde el número personal... ¿qué red corporativa es esa?”. Subrayó que el firewall como frontera ya es historia, igual que esa DMZ que hacía de “anillo defensivo”: “Eso ya no tiene sentido. Lo vimos con WannaCry y con tantos ataques que entraron desde dentro. Con robar la credencial de un administrador puedes tomar toda la red”.

Para él, el mensaje es claro: no se puede confiar en la red; sólo se puede confiar en la identidad y en señales contextuales. “No es lo mismo conectarte a las tres de la mañana desde un aeropuerto que desde tu casa a las doce del mediodía.”



> “Muchas de las tecnologías implantadas están subutilizadas; simplificar es necesario”
>
> **Diego Andrés,**
> CISO, **Prosegur Alarmas**

Diego Andrés estuvo de acuerdo, pero introdujo realismo: la desaparición de la red como concepto no implica su desaparición operativa. “Convive el futuro con el legado. No podemos dejar de lado el perímetro en ciertos entornos. Pero sí debemos apoyarnos más en identidad, accesos condicionados y tecnologías modernas para depender menos de lo tradicional”.

En la Administración, el avance es más lento. Pablo Gálvez explicó que la red corporativa sigue viva por cumplimiento del ENS, regulaciones sectoriales y certificaciones que imponen arquitecturas concretas. Pero reconoció que están interesados en la transición hacia modelos donde la identidad pesa más que el segmento de red.

El equipo de Zscaler aportó un dato relevante: la propia IGAE ya está navegando bajo un modelo Zero Trust a través del Exchange de la compañía, sin exponer IPs públicas. Federico Gimeno lo describió así: “No conectamos usuarios a redes; conectamos usuarios a aplicaciones, estén donde estén. Verificamos antes, durante y después”.

Complejidad tecnológica vs. visibilidad: dónde están los verdaderos puntos ciegos

En los últimos años, muchas organizaciones han ido sumando soluciones de seguridad sin una estrategia global. A esto se suma la fragmentación entre entornos híbridos, múltiples nubes, OT, IoT y sistemas legacy. El resultado: un ecosistema difícil de gobernar y con zonas opacas que los atacantes aprovechan. Este bloque se centró en el dilema clave: ¿es el exceso de tecnología o la falta de visibilidad lo que más preocupa?

Rafael Rico fue contundente al asegurar que están relacionadas. “Hemos tenido una obsesión por añadir y añadir tecnología, como si gastar más fuera proteger mejor. Y llega un momento en el que no sabes lo que tienes ni cómo se protege”.

Describió la situación típica de grandes empresas: adquisiciones, movimientos internos, reestructuraciones, cambios de red... y un stack que crece en capas superpuestas. “Eso genera confusión. Y cuando entras en híbridos o en cloud, esa complejidad se multiplica”.

Añadió un concepto potente: “te sobran cosas y a la vez te dejas espacios sin barrer”. Es decir, redundancias y huecos al mismo tiempo.

Ana Sandoval coincidió señalando que la tecnología avanza, pero la complejidad aumenta aún más rápido. Y recordó que el principal activo sigue siendo la información: “Tenemos que

saber dónde está, cómo se comparte y cómo se protege. La complejidad y la falta de visibilidad van juntas".

Alejandro Menéndez profundizó en los problemas operativos: logs incompatibles, formatos antiguos, herramientas que ya no se entienden entre sí. "Es un mar en magnum de datos imposible de ver. Sí, la IA ayuda, pero hay sistemas —como SCADA u OT— que directamente no se pueden monitorizar. Y ahí tienes los puntos ciegos donde el atacante puede estar meses".

Desde Zscaler, Federico Gimeno y Manuel Cantonero defendieron que la visibilidad real sólo llega cuando existe una plataforma única capaz de ver tráfico de usuarios, dispositivos, IoT, OT, nubes, APIs y aplicaciones privadas. "Necesitamos una visión de halcón. Reducir complejidad sin visibilidad no sirve de nada".

¿Ha llegado el momento de simplificar? Menos herramientas, más estrategia

Tras años de inversión —y de capas sobre capas— muchas organizaciones sienten el peso del "sprawl tecnológico": demasiadas soluciones, demasiados contratos y demasiada complejidad para gestionarlo todo. La pregunta era si ya estamos en el punto en el que "menos es más" no es solo un lema, sino una estrategia viable.

"La red corporativa sigue viva por cumplimiento de la legislación, pero estamos interesados en la transición hacia otros modelos"

Pablo Gálvez, Subdirector General Adjunto Unidad de Seguridad de la Información, **IGAE/Ministerio de Hacienda**

El CISO de Prosegur no dudó: "Sí. Muchas de las tecnologías que se adoptan en las diferentes empresas o entidades, son subutilizadas. En ocasiones, no se llega al 50% del uso de sus capacidades. Eso ocupa espacio, inversión, mantenimiento, contratos... Simplificar es necesario". Recordó que la simplificación no es solo técnica: afecta a procesos, a usuarios, a cultura interna. "Es un reto convencer a negocio cuando los cambios pueden generar fricción".

En el sector público, Pablo Gálvez explicó que están transfiriendo servicios al COCS de la Agencia Estatal de Administración Electrónica para reducir carga interna y simplificar, aunque manteniendo otros por ya tener más nivel de seguridad que la facilitada por los equivalentes del COCS.

Los representantes de Zscaler coincidieron en que simplificar no significa "tirarlo todo", sino partir de una estrategia clara: definir la transición, medir qué puede sustituirse, y avanzar con coexistencia y no con ruptura.

Federico Gimeno lo formuló así: "Nadie pasa de 0 a 100. Lo importante es ver Zero Trust como paradigma: sin IPs públicas, con conexión directa a aplicaciones y con verificación continua".

La transición hacia modelos sin perímetro acelera: identidad, dato y visibilidad marcan el nuevo tablero

¿Seguirían existiendo firewalls y VPNs si hoy diseñáramos desde cero?

El firewall y las VPN fueron durante décadas la base de cualquier arquitectura corporativa. Pero la nube, la movilidad y los modelos Zero Trust cuestionan radicalmente su papel. Este bloque planteó un ejercicio: si hoy hubiera que diseñar desde cero, ¿tendrían espacio los mismos elementos?

En opinión de Rafael Rico en entornos legacy, firewalls y VPNs seguirán existiendo. Pero el CISO de Atento España subrayó que el enfoque moderno sería muy diferente: “La oportunidad está en rediseñar pensando en el dato, no en la red”.

Víctor Villagrá destacó la diversidad de escenarios. Desde empresas que mantendrán CPDs propios por razones críticas a otras que externalizarán todo. Además, recordó algo interesante desde la docencia: “Los firewalls más seguros son los transparentes, los que ni siquiera tienen IP pública”.

Para Zscaler, el debate tiene una respuesta clara: las VPNs deben desaparecer por la exposición que generan; los firewalls seguirán para servicios externos (WAF, portales publicables); y el acceso interno debe migrar a Zero Trust sin IPs expuestas.

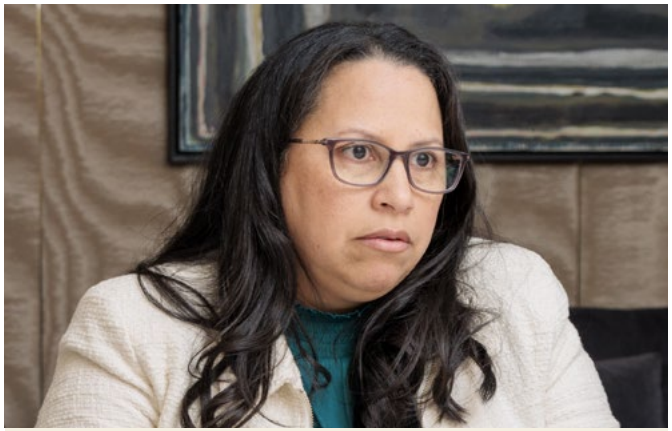
La identidad como perímetro

Con el perímetro diluido, la identidad —humana y no humana— se ha convertido en el nuevo eje de control. Este bloque exploró cómo están gestionando autenticación, acceso, privilegios, agentes de IA y segmentación dinámica en entornos híbridos, OT y cloud.

Ana Sandoval explicó cómo la autenticación ha evolucionado a tokens, desafío-respuesta, verificación continua y control de expiración. Pero insistió en que los sistemas legacy no soportan mecanismos modernos y requieren estar encapsulados con segmentación estricta.

> “Te sobran cosas y, a la vez, te dejas espacios sin barrer”
>
> **Rafael Rico,** CISO, **ATENTO España**

Alejandro Menéndez destacó la fragilidad humana como primer vector de ataque al recordar que “muchas intrusiones vienen por robo de credenciales”. Por eso aplican MFA, controles adaptativos y permisos temporales para tareas concretas.



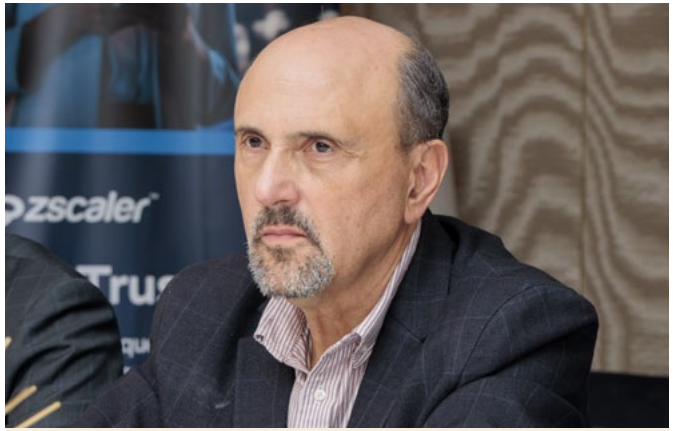
> “Tenemos que saber dónde está la información, cómo se comparte y cómo se protege”

Ana Sandoval,
Computer Science Engineer GASS,
Universidad Complutense de Madrid

Al introducirse el tema de agentes de IA e identidades no humanas, Diego Andrés reconoció que es un territorio todavía en construcción, pero que sólo puede abordarse “si la ciberseguridad nace desde el diseño” y estableciendo procesos y normativas que permitan minimizar de forma progresiva los riesgos que supone la IA.

Zscaler amplió la conversación sobre identidad mostrando cómo, en la práctica, su enfoque va mucho más allá de verificar quién es el usuario. Para ellos, la identidad incluye también desde qué dispositivo se conecta, en qué estado se encuentra ese equipo, qué comportamiento exhibe, qué acciones intenta realizar y cómo se comunican entre sí los procesos automatizados y los propios agentes de IA. Todo ello se combina con políticas específicas para entornos OT e IoT, donde la segmentación y el aislamiento resultan críticos.

A partir de esa visión ampliada, la compañía ha desarrollado capacidades avanzadas que ya están siendo clave en muchos proyectos: detección de prompts maliciosos y usos indebidos de modelos generativos, control y observación del tráfico entre agentes de IA, auditoría y grabación de sesiones en sistemas legacy que requieren supervisión, o la posibilidad de desplegar POPs dentro de APNs privados de operadoras móviles para aplicar seguridad y visibilidad sobre dispositivos IoT sin necesidad de abrir la red. En conjunto, se trata de un enfoque que no solo refuerza la protección, sino que redefine cómo se aplica la seguridad en entornos distribuidos y altamente heterogéneos.

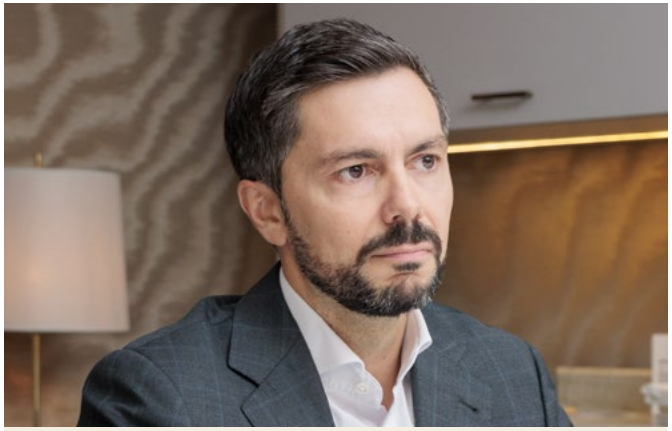


> “Los firewalls más seguros son los transparentes, los que ni siquiera tienen IP pública”

Víctor Villagrá, Catedrático y Director del Máster de Ciberseguridad/Subdirector jefe de estudios de la ETS de Ingenieros de Telecomunicación,
Universidad Politécnica de Madrid

IA generativa: productividad acelerada y riesgo multiplicado

La irrupción de la IA generativa ha desatado



"No conectamos usuarios a redes; conectamos usuarios a aplicaciones, estén donde estén"

Federico Gimeno,
Sales Account Executive Iberia, **Zscaler**

La ciberseguridad entra en una nueva etapa donde simplificar, ver y proteger identidades es más crítico que nunca

innovación... y exposición. Su adopción espontánea, la falta de control, los prompts, los agentes y los modelos propios han creado un nuevo escenario de riesgo. Este bloque analizó cómo están respondiendo CISOs, administración y universidad a esta nueva realidad.

Pablo Gálvez describió su relación con la IA como una "dicotomía": apasionado como usuario, controlador como responsable de ciberseguridad. Ha pedido un portátil paralelo para experimentar con IA y pentesting, pero mantiene límites estrictos en el entorno corporativo.

Rafael Rico expresó el gran temor respecto al shadow IT. Aunque bloqueen usos indebidos, "se buscan la vida para utilizarla". En ATENTO la IA es fundamental para su negocio, desde análisis de llamadas hasta detección de emociones, pero la IA Act exige cautela.

En la universidad, Víctor Villagrá fue aún más explosivo: "La IA está afectando a la formación de manera brutal. Tenemos que rediseñarlo todo. Ya no podemos pedir trabajos como antes. Un alumno puede generarlo todo con IA". El desafío, dijo, es enseñar a usarla como herramienta, no como sustituto.

En el bloque dedicado a inteligencia artificial, Zscaler profundizó en cómo está extendiendo su modelo de seguridad para cubrir un escenario en el que los riesgos ya no proceden solo de usuarios o dispositivos, sino también de las propias herramientas de IA. La compañía explicó que hoy es imprescindible entender qué IAs utilizan los empleados, cómo interactúan con ellas y qué tipo de información podría estar saliendo hacia estos servicios sin control. Por eso han desarrollado capacidades capaces de detectar exfiltraciones a través de prompts, identificar usos inapropiados o sensibles y aplicar políticas de protección del dato basadas en clasificación automática mediante IA.

Otro punto clave es el tráfico entre agentes. Zscaler mostró cómo su plataforma puede analizar y controlar el diálogo entre agentes de IA, detectar comportamientos anómalos en estos intercambios y aplicar restricciones cuando una interacción pueda comprometer datos o procesos internos. Para las organizaciones que

entrenan o despliegan sus propios modelos, la compañía permite incluso integrarse mediante SDK en motores de IA propios, garantizando visibilidad y gobierno desde el origen del modelo hasta su operación.

Finalmente, destacaron la capacidad de monitorizar el tráfico y el comportamiento hacia modelos externos, incluidos los grandes LLM disponibles en la nube. Esto permite no solo ver qué se consulta, sino también prevenir que un usuario —o un agente automatizado— acabe enviando información sensible a una IA pública o a un servicio que no cumpla los requisitos de seguridad de la organización. En conjunto, es una aproximación que aborda el riesgo de la IA desde todos los ángulos, entendiendo que el control ya no puede limitarse a bloquear herramientas, sino a gobernar su uso de forma inteligente.

NIS2, DORA y AI Act: regulación como acelerador

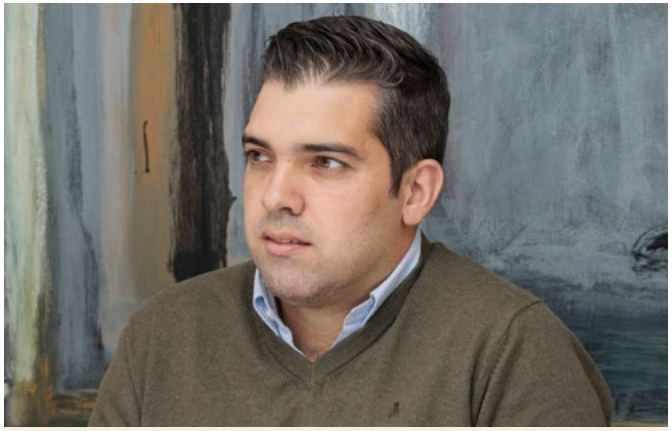
La nueva regulación europea no solo endurece requisitos: redefine responsabilidades, obliga a revisar arquitecturas, exige trazabilidad y pone

> Las organizaciones afrontan un punto de inflexión: la red deja de ser el centro y la seguridad se redefine desde la identidad, la visibilidad y la resiliencia operativa

la resiliencia en el centro. Este bloque analizó cómo estas normas están impulsando cambios estructurales en las organizaciones.

Ana Sandoval explicó que estas normas exigen no solo más seguridad, sino cambiar la mentalidad hacia resiliencia, trazabilidad y diseño seguro: Zero Trust, segmentación, mínimo privilegio.

Alejandro Menéndez centró su análisis en la IA y recordó casos reales: Samsung subiendo código fuente a un LLM, prompts que permiten saltar barreras o incluso usar ChatGPT para hackear webs mediante ingeniería social conversacional. Y destacó una preocupación grave:



> “Nadie pasa de 0 a 100. Lo importante es ver Zero Trust como un paradigma”
>
> **Manuel Cantonero,**
> Sales Account Executive Iberia, **Zscaler**

“Debería haber responsabilidad legal clara para proveedores de IA cuando se pierden datos.”

En este punto, Diego Andrés fue especialmente claro: reconoció que las normativas pueden resultar incómodas. Explicó que estos marcos regulatorios ofrecen a los responsables de seguridad un verdadero margen de acción, obligan a mantener planes estratégicos vivos, fuerzan a

priorizar lo relevante y ayudan a descubrir puntos débiles que de otra forma podrían permanecer ocultos.

Recordó además que los atacantes continuarán explotando cualquier nueva tecnología —IA, cloud, automatización— con la misma rapidez con la que se adopta, por lo que la regulación no es un obstáculo, sino una capa adicional de defensa que contribuye a elevar el nivel de madurez y resiliencia de todo el ecosistema.

Zscaler insistió en que su plataforma incorpora controles de DLP, telemetría, flujos de auditoría y políticas que facilitan el cumplimiento de ENS, NIS2 o DORA sin multiplicar procesos.

Redefiniendo los cimientos

El almuerzo dejó una imagen clara: la ciberseguridad está redefiniendo sus cimientos. Ya no se trata de proteger redes, sino identidades, datos y flujos. Ya no se trata de añadir capas, sino de simplificar sin perder control. La visibilidad ya no es un lujo, sino el requisito previo para cualquier decisión. La IA no es una herramienta más, sino el próximo gran vector de productividad y de riesgo.

Si tuvierais que definir la "seguridad ideal" para los próximos tres años, ¿qué palabras elegiríais?

- **Ana Sandoval,** Computer Science Engineer GASS, **Universidad Complutense de Madrid.** ➔ **Autenticación y verificación continua.**
- **Federico Gimeno,** Sales Account Executive Iberia, **Zscaler.** ➔ **Visibilidad y simplificación.**
- **Víctor Villagrá,** Catedrático y Director del Máster de Ciberseguridad/Subdirector jefe de estudios de la ETS de Ingenieros de Telecomunicación**, Universidad Politécnica de Madrid.** ➔ **Transparencia, confianza y fiabilidad.**
- **Rafael Rico,** CISO, **ATENTO España.** ➔ **Respuesta, resiliencia y rediseño.**
- **Pablo Gálvez,** Subdirector General Adjunto Unidad de Seguridad de la Información, **IGAE/Ministerio de Hacienda.** ➔ **Resiliencia, simplicidad, y proactividad.**
- **Manuel Cantonero,** Sales Account Executive Iberia, **Zscaler.** ➔ **Identidad, dato y respuesta.**
- **Diego Andrés,** CISO, **Prosegur.** ➔ **Visbilidad, identidad y resiliencia**
- **Alejandro Menéndez,** experto en análisis y diseño de soluciones ciberseguridad. ➔ **Resiliencia, verificabilidad y trazabilidad.**

Y en este contexto, la regulación no es una carga, sino el marco que permitirá sostener arquitecturas más resilientes en los próximos años.

El futuro, según todos los participantes, será un equilibrio entre verificación continua, experiencia de usuario fluida, simplificación operativa y responsabilidad compartida. Un futuro donde la red ya no importa: lo que importa es quién eres, qué haces y cómo se comporta cada pieza del sistema. CST

IR A PÁGINA ANTERIOR