SEPTIEMBRE 2025/ VOLUME 1

HACK THE ROAD CYBER SECURITY

MAGAZINE

LEÓN GUANAJUATO
LA COMUNIDAD DE CIBERSEGURIDAD SE REUNE

BRUNCH & BYTES 2025
CIBERSEGURIDAD EN LA TERRAZA

¿TU EMPRESA ESTÁ REALMENTE PROTEGIDA?
FELIX LOPEZ PEÑA

NO TODO ES CÓDIGO Y FIREWALLS

MESA REDONDA SECURITY AWARENESS
JONATHAN DÍAZ, ANA LAURA MENA Y ALBERTO ACEVES

HACK THE ROAD
CYBERSECURITY TOUR IN MEXICO

¿Te has dado cuenta de que los eventos más grandes de ciberseguridad en México suceden, casi siempre, en la misma ubicación? La necesidad de conectar, aprender y compartir know-how es una constante en todo el país, pero las oportunidades no siempre están bien distribuidas.

De esta necesidad nace Hack The Road

Una iniciativa pionera diseñada para romper el centralismo y llevar eventos de primer nivel a diferentes estados de la república. Nuestra misión es doble: crear comunidad en las regiones y visibilizar el talento local de profesionales que están haciendo una diferencia real en la seguridad de las organizaciones.

La Primera Parada: León, Guanajuato.

Nuestra primera edición recorrerá el camino hasta la vibrante ciudad de **León, Guanajuato**. Donde se reunieron algunas de las mentes más brillantes de la industria para compartir, debatir y anticipar el futuro de la ciberseguridad.

CYBER COMPLIANCE COMO VENTAJA COMPETITIVA

grios@cybernuvol.com

¿TE GUSTARÍA EVALUAR TU POSTURA DE CUMPLIMIENTO?

Es en este punto donde el Cyber Compliance o Cibercumplimiento deja de ser un simple checklist de auditoría y se convierte en el pilar fundamental de tu estrategia de negocio y en una poderosa ventaja competitiva. Para profundizar en este tema crucial, contamos con la valiosa perspectiva de Gisela Ríos Villa, una Auditora Certificada con más de 20 años de experiencia en cumplimiento normativo. Desde Tijuana, Gisela ha liderado proyectos en un espectro impresionante de frameworks y regulaciones.

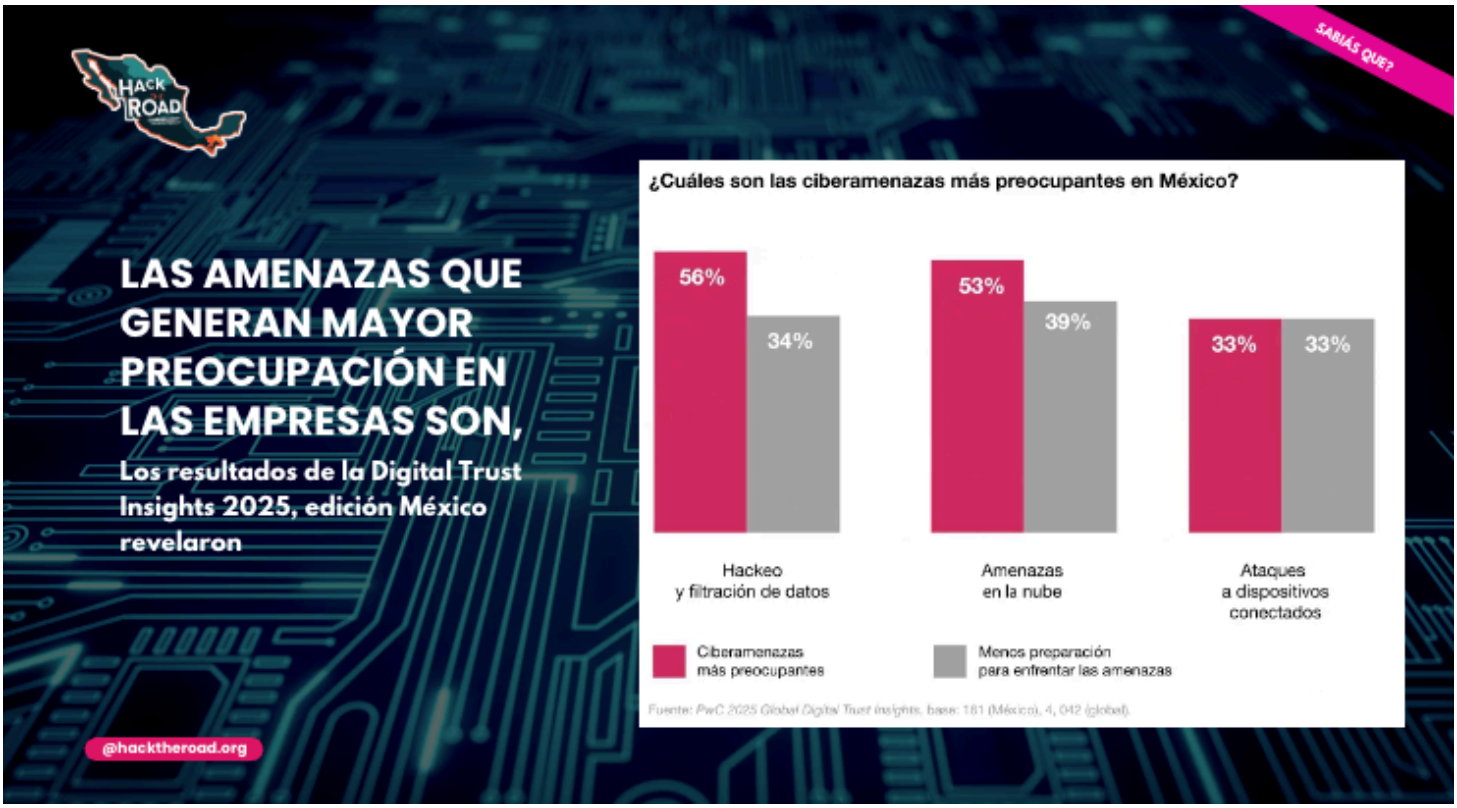
Gisela nos recalca: "Hoy, el cumplimiento no debe verse como un gasto, sino como una inversión estratégica. Cuando un cliente me pregunta por qué debería certificarse en PCI DSS si no es obligatorio para su tamaño, mi respuesta siempre es la misma: '¿Estás dispuesto a asumir el riesgo de que los datos de las tarjetas de crédito de tus clientes sean robados? ¿Y el costo de las multas y la pérdida de confianza?' Un programa de compliance bien implementado es un escudo que protege tanto al negocio como a sus clientes. Es el mensaje claro de que haces las cosas bien, y eso, en el mercado actual, vale oro."

La migración a la nube es solo el primer paso. El paso decisivo es gobernarla y protegerla de manera efectiva. **Integrar el Cyber Compliance en el ADN de tu organización** no es solo sobre evitar multas; se trata de construir una marca sólida, resiliente y preparada para el futuro. Como bien lo ejemplifica la trayectoria de expertos como Gisela, la seguridad y el cumplimiento son disciplinas que, cuando se abrazan proactivamente, dejan de ser una carga para convertirse en el motor de la ventaja competitiva más valiosa en la economía digital: la confianza.

LA CIBERSEGURIDAD ENFRENTA UNA TRANSFORMACIÓN DEBIDO A LA IA GENERATIVA

Global X Management Company LLC (“Global X ETFs”)

¿CUALES SON LAS CIBERAMENAZAS MÁS PREOCUPANTES EN MÉXICO?



PricewaterhouseCoopers, S.C.

AI-POWERED, UNIFIED SECOPS: PROTEGIENDO LA INNOVACIÓN EN LA ERA DE LA IA

Daniel E. Lopez
Microsoft Cybersecurity Architect Expert
dlopez@cybernuvol.com

Cimentar los Fundamentos. Clasificación y Etiquetado de Datos

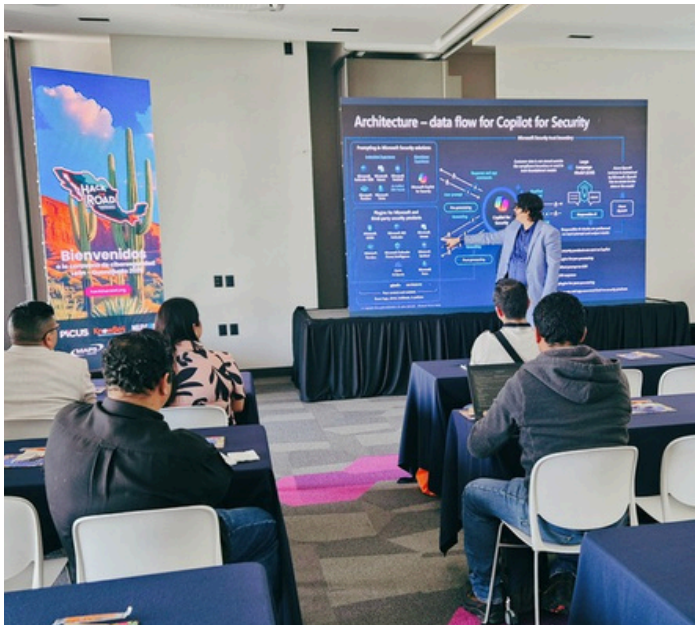
Este es el paso cero, el más crítico y a menudo el más olvidado. Sin una clasificación rigurosa de la información, cualquier iniciativa de IA se construye sobre cimientos de arena.

- **¿Por qué es esencial?** La IA "aprende" y "toma decisiones" basándose en los datos que consume. Si no puede entender qué datos son confidenciales, públicos o regulados, no podrá protegerlos adecuadamente. **Sin un etiquetado correcto, es imposible aplicar políticas de seguridad, prevenir fugas de datos o cumplir con regulaciones.**
- **Acción clave:** Las empresas deben implementar herramientas de **Information Protection** (como Microsoft Purview Information Protection) para:
  - **Clasificar automáticamente** la información confidencial (PII, financiera, intelectual) en todo su entorno (nube, endpoints, on-premise).
  - **Aplicar etiquetas de confidencialidad** que se adjuntan a los datos allá donde vayan, como un semáforo que indica cómo deben ser manejados.
  - **Establecer políticas de protección** basadas en esas etiquetas (cifrado, restricciones de acceso, marcado visual en documentos).

Sin este paso, la IA no nos entiende. Un modelo de IA que procesa un documento sin una etiqueta de clasificación no puede saber si está manejando el plan estratégico de la empresa o una nota informal. La clasificación es el lenguaje común entre los humanos y la IA para gestionar el riesgo.

Como destacó Daniel en su ponencia

La seguridad en la era de la IA requiere un enfoque dual: entender sus peligros y aprovechar su poder para defendernos. Herramientas como Microsoft Security Copilot nos permiten escalar esta defensa, actuando como un arquitecto de seguridad inteligente que transforma datos en insights accionables. Microsoft ofrece las herramientas y el marco para hacerlo, pero la clave está en la gobernanza proactiva y la cultura de seguridad.



Microsoft Security Copilot: El Arquitecto de tu Defensa con IA

Para el Director de Seguridad que navega a diario entre la complejidad técnica y la presión estratégica, la promesa de la inteligencia artificial genera tanto interés como escepticismo. Surgen preguntas inevitables sobre la confidencialidad de los datos y la verdadera utilidad operativa. Microsoft Security Copilot se ha diseñado precisamente para responder a esas inquietudes, no como una herramienta más, sino como un arquitecto de defensa que opera bajo un principio inquebrantable: su información siempre será suya. Toda interacción, cada prompt que se introduce y cada hallazgo que se genera, permanece confinada dentro de los límites de su entorno de Microsoft 365, sin ser utilizado para entrenar modelos externos, garantizando así el cumplimiento de sus políticas de gobierno y soberanía de datos.

Iván Magallanes Morón
Director Tecnologias de la Información, Grupo Andrea

22 de Septiembre, 2025

CIBERSEGURIDAD EN EL RETAIL: DOS PILARES DE DEFENSA EN GRUPO ANDREA

En la era digital, donde el retail se mueve a la velocidad de un clic, la ciberseguridad ha dejado de ser un tema técnico para convertirse en el corazón de la confianza con nuestros clientes. En **Grupo Andrea,** hemos entendido que proteger los datos y las transacciones no es solo una cuestión de compliance, sino un pilar estratégico para el crecimiento sostenible.

Frente a un panorama de amenazas cada vez más sofisticado, hemos implementado una estrategia proactiva basada en estándares internacionales como ISO 27001. Hoy quiero compartir dos casos concretos que han transformado nuestra postura de seguridad y cuyo impacto es claramente medible.

🛡️ Caso 1: Implementación de solución EDR de última generación

Grupo Andrea enfrentaba limitaciones con su antivirus tradicional, lo que quedó evidenciado tras contener un intento real de ransomware con apoyo externo. Este incidente fue el impulso definitivo para alinear nuestra estrategia con el roadmap de ciberseguridad 2024–2027 y adoptar una solución moderna de Endpoint Detection and Response (EDR). Esta tecnología no solo busca y bloquea malware, sino que monitoriza continuamente cada dispositivo, detectando comportamientos sospechosos y permitiendo una respuesta rápida y automatizada.

El impacto medible ha sido transformador:

- **Respuesta Ágil:** Redujimos el tiempo de respuesta ante incidentes de 24 horas a apenas 4 horas, minimizando potenciales daños.
- **Visibilidad Total:** Incrementamos nuestra cobertura de protección efectiva de un 20% a un sólido 70%, ganando control sobre nuestra superficie de ataque.
- **Cumplimiento y Confianza:** Fortalecimos nuestro cumplimiento normativo y mejoramos significativamente nuestra postura ante auditorías.
- **ROI Tangible:** El proyecto demostró un retorno financiero positivo en menos de dos años.

🔐 Caso 2: Fortalecimiento del SOC y protección de aplicaciones críticas

La defensa perimetral es vital, pero la verdadera resiliencia se construye desde dentro. Por ello, nuestro segundo pilar se centró en fortalecer nuestro **Centro de Operaciones de Seguridad (SOC)** interno. Utilizando la herramienta BANYAX, hemos logrado un hito crucial: alcanzar un 90% de cobertura en el monitoreo de nuestros activos críticos.

Esto significa que nuestro equipo tiene una visión en tiempo real de lo que ocurre en el corazón de nuestras operaciones. Paralelamente, adoptamos un enfoque ofensivo para proteger nuestras aplicaciones más sensibles. Realizamos pruebas de penetración (pentesting) internas sobre dos pilares del negocio: la app móvil APAY y el sistema SPI2.

Los resultados han reforzado nuestra arquitectura de seguridad:

- **Prevención de Riesgos:** Identificamos y mitigamos vulnerabilidades altas y críticas en aplicaciones clave, previniendo potenciales filtraciones de datos o interrupciones del servicio.
- **Decisiones Informadas:** Afinamos los reportes de seguridad para la alta dirección, transformando datos técnicos en información estratégica para la toma de decisiones.
- **Protección Integral:** Activamos módulos de seguridad avanzados en plataformas críticas como VTEX (comercio electrónico) y Symantec, creando una defensa en profundidad.

BALANCE ENTRE INNOVACIÓN Y SEGURIDAD

En el retail moderno, la dicotomía entre innovación ágil y seguridad robusta es un falso dilema. En **Grupo Andrea,** hemos comprendido que la seguridad no es un obstáculo para la transformación digital, sino su habilitador fundamental. La clave no está en frenar los proyectos, sino en integrar los controles de manera inteligente desde su concepción.

Hemos establecido principios estratégicos que orientan cada iniciativa de transformación, asegurando que la agilidad y la seguridad avancen en la misma dirección:

- Cloud First, SaaS First, API First: para facilitar la escalabilidad y flexibilidad.
- Event Driven y Data Driven: para responder ágilmente a los cambios del entorno comercial.
- Observability y resiliencia: para tomar decisiones informadas y mantener la estabilidad operativa.
- Identity Federated: para mejorar la experiencia del usuario y fortalecer la seguridad.

La tecnología por sí sola no es suficiente. El éxito de esta integración depende de una fuerte alineación organizacional. Lo logramos mediante:

- Gestión del cambio alineada desde Dirección General.
- Comunicación efectiva entre TI y negocio.
- Modelo de partner advisor que acompaña en decisiones estratégicas, no solo en implementación.

🛡️ **Seguridad como habilitador, no como freno**
En los reportes de avance del proyecto Oracle Retail, se menciona que la seguridad no se trata como una barrera, sino como un habilitador de innovación. Se integran controles desde el diseño funcional y técnico, y se revisan en sesiones periódicas de seguimiento.

🧠 **Reuniones de seguimiento y decisiones ágiles**
Las sesiones de seguimiento organizadas por el PM permiten revisar avances, identificar desviaciones y tomar decisiones clave en tiempo real. Aunque no están transcritas, los correos y minutas compartidas evidencian un enfoque colaborativo entre Oracle y **Grupo Andrea** para mantener el ritmo de innovación sin perder control sobre riesgos.

DESARROLLO CONTINUO: LA IA COMO NUEVO CAMPO DE BATALLA EN CIBERSEGURIDAD EN LA INDUSTRIA DEL RETAIL

🔮 **Visión estratégica: IA como eje de la ciberseguridad moderna**
La integración de IA en el análisis de comportamiento, automatización del SOC (SOAR), simulaciones de crisis y monitoreo avanzado será clave para el periodo 2025–2030. Esta visión se alinea con los pilares definidos en el roadmap de ciberseguridad del grupo, que prioriza:

- Threat Intelligence con IA para detección proactiva.
- Automatización de respuesta ante incidentes.
- Capacitación continua y certificaciones especializadas.
- Simulaciones de phishing y ataques dirigidos para fortalecer la resiliencia.

🧠 **Especialización recomendada: IA aplicada a la ciberseguridad**
Destaca la necesidad de formar perfiles híbridos que dominen tanto la ciberseguridad como el machine learning.

Este tipo de formación permitiría a **Grupo Andrea** contar con especialistas capaces de diseñar soluciones adaptativas, anticiparse a ataques y optimizar el uso del presupuesto de seguridad. **La próxima frontera no es tecnológica, sino de talento y preparación.**

LO NUEVO EN KNOWBE4: LA EVOLUCIÓN HACIA LA RESPUESTA PROACTIVA

KnowBe4 es famoso por sus simulaciones de phishing y capacitaciones interactivas que reducen mediblemente el índice de clicks maliciosos. Sin embargo, su verdadero valor reside en integrar este entrenamiento con herramientas operativas que abordan el ciclo completo de la amenaza.

KnowBe4 no se limita a la prevención; está evolucionando hacia una plataforma integral de Security Culture & Defense Platform. Entre sus innovaciones más recientes destacan:

- **AI-Driven Phishing Detection:** Utiliza inteligencia artificial para generar simulaciones de phishing hiperrealistas basadas en amenazas actuales, preparando a los usuarios para los ataques más sofisticados.
- **Security Coach Integration:** Esta función permite corrección en tiempo real. Si un empleado comete un error (como descargar un archivo riesgoso), recibe una micro-lección instantánea y personalizada, reforzando el aprendizaje en el momento exacto.
- **PhishER:** Se trata de un sistema de priorización y gestión de incidentes de correo que permite a los analistas: Clasificar rápidamente, utiliza reglas personalizables y análisis automático, permite tomar acciones inmediatas, como poner en cuarentena correos maliciosos.

Al integrar KnowBe4 a través de un partner especializado como Nuvol, las empresas no solo adquieren una herramienta, sino un programa estratégico con acompañamiento continuo.

Cateryn Farfán
Security Awareness Specialsit
cfarfan@cybernuvol.com

Six-Month Phishing Snapshot

17.3% increase in phishing emails (vs. previous six months)

Between Sep 15, 2024, and Feb 14, 2025

57.9% were sent from compromised accounts

11.4% within the supply chain

25.9% contained attachments

20% relied solely on social engineering

54.9% contained a phishing hyperlink payload

The most phished day

16 December 2024

82.6% of phishing emails utilized AI

53.5% YoY increase!

81.9% of victims had their email addresses leaked in previous data breaches

On average, phishing emails contained **1058 characters (~188 words)**

The top three words used in phishing emails:

1. Urgent
2. Review
3. Sign

New starters typically received a phishing email after 3 weeks

The top cryptocurrencies demanded during extortion are:

bitcoin MONERO XRP

DE MITOS A ÉXITOS: EL FACTOR HUMANO COMO LA ESTRATEGIA GANADORA EN CIBERSEGURIDAD

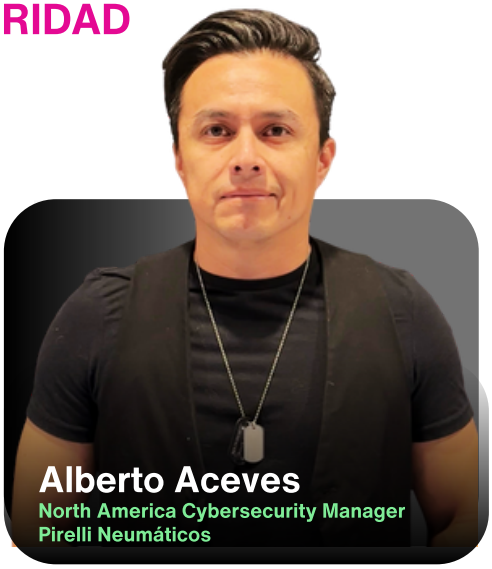
La reciente mesa redonda despejó el camino, demostrando que las estrategias más exitosas son aquellas que priorizan a las personas. Los insights de Ana Laura Mena Líder de Ciberseguridad de Grupo Charly, Alberto Aceves North America Cybersecurity de Pirelli y Jonathan Coordinador de Seguridad Informática de Flecha Amarilla pintaron un panorama claro: la obligación debe ceder paso a la adopción genuina.

VISIBILIDAD DATA-DRIVEN Y APRENDIZAJE CON PROPÓSITO

Ana Laura Mena de Grupo Charly compartió una estrategia basada en dos pilares: **datos y empatía.**

- La automatización de reportes mediante un BOT les brinda a la gerencia visibilidad total sobre el panorama de riesgos: quiénes son los “clickers” en simulaciones de phishing, los reincidentes y el cumplimiento de capacitaciones. Pero los datos sólo son útiles con una acción inteligente.
- Su segundo pilar es brillante: en lugar de reprender, reúnen a los “clickers” físicamente un viernes al mes. “Hablamos de ciberseguridad para que no solo se lleven el conocimiento de la empresa, sino que vean cómo les ayuda en su día a día”, explicó Mena. Este enfoque transforma la seguridad de una política corporativa abstracta en un beneficio tangible para su vida personal (proteger su banca online, redes sociales, etc.), logrando una adopción mucho más auténtica y duradera.

CYBER CHISME: HUMANIZANDO LA CIBERSEGURIDAD



Si el enfoque de Grupo Charly es correctivo, el de Alberto Aceves de Pirelli es **proactivo y coloquial.**

Su estrategia se basa en borrar la barrera del tecnicismo. Alberto se acerca a cada área de la empresa: Finanzas, RH, Producción y les habla en su propio lenguaje.

Convierte las alertas de seguridad en historias, en lo que él llama “cyber chisme”. “Trato de que las personas se rían, entiendan y vean el valor de una forma amigable”, comentó. Este método, centrado en la conexión humana, hace que el mensaje sea memorable y rompe el mito de que la ciberseguridad es un tema solo para IT.

Crucialmente, esta estrategia está respaldada por un compromiso inquebrantable de la alta dirección. En Pirelli, la seguridad es tan prioritaria que cualquier proveedor externo debe pasar por sus controles de ciberseguridad. Esto posiciona al área de seguridad no como un costo, sino como un socio estratégico que aporta valor en las decisiones de negocio y vela por el bienestar integral de la empresa.

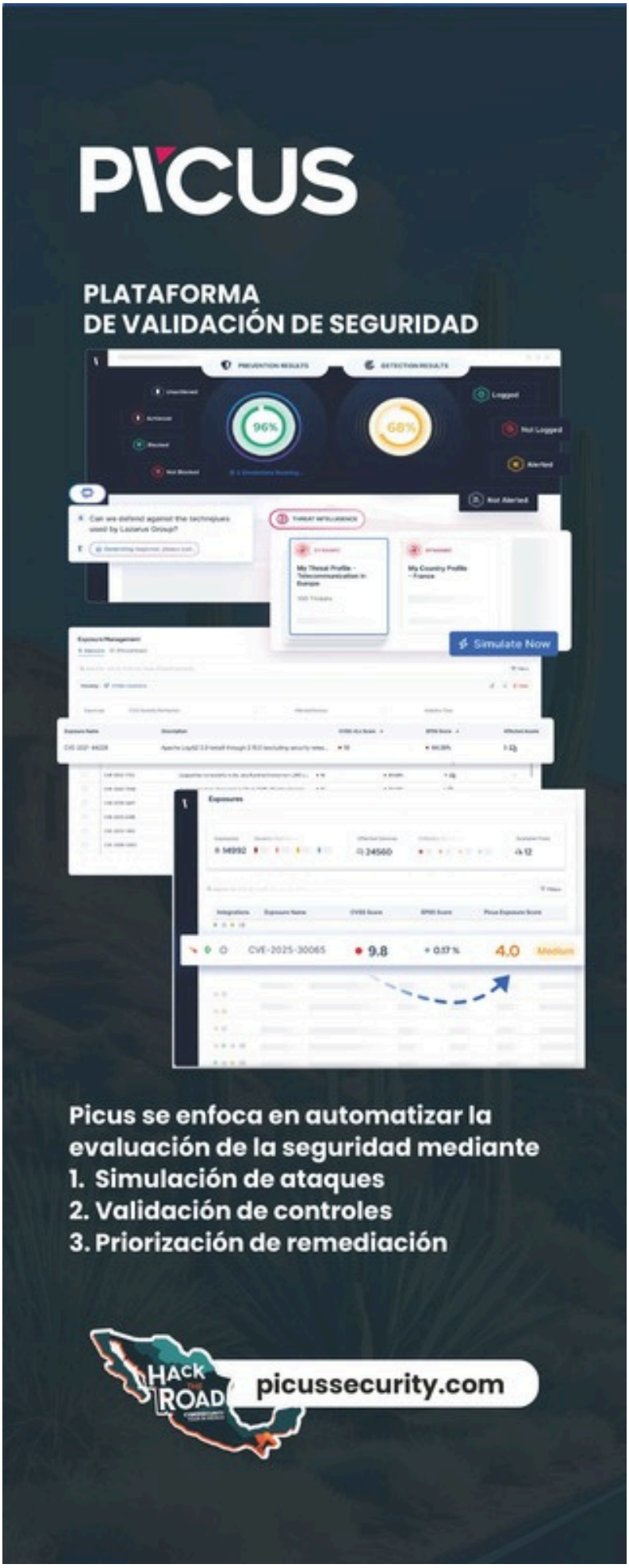
ENFOQUE GRANULAR Y GAMIFICACIÓN

Jonathan de Flecha Amarilla presentó una estrategia más granular: **el enfoque en usuarios de alto riesgo.**

- Segmentación del Riesgo: Identifican y se enfocan específicamente en los usuarios de alto riesgo (aquellos que más frecuentemente fallan en pruebas de phishing o no cumplen con las políticas).
- Reducción Continua: Trabajan mes a mes con este grupo objetivo con el fin específico de disminuir su nivel de riesgo de manera medible.
- Gamificación: Utilizan técnicas de gamificación para hacer la capacitación más engaging y efectiva para este grupo difícil de alcanzar.

Conocimiento para la Vida, al igual que Ana Laura, fomentan que los empleados apliquen estos conocimientos en su día a día, reforzando el valor personal de la ciberseguridad.

No hay una Solución Única, las estrategias deben adaptarse a la cultura de la empresa. Flecha Amarilla se enfoca en un grupo de riesgo, Pirelli en la comunicación masiva y Grupo Charly en la data y las sesiones correctivas. Todas son válidas según el contexto.



LA ILUSIÓN DE LA SEGURIDAD: DEL DISCURSO A LA REALIDAD

López Peña inició su sesión cuestionando el statu quo: "Todos hablamos de controles de seguridad, herramientas y procesos… pero ¿cómo sabes si realmente estás protegido?". Señaló que muchas organizaciones operan bajo una ilusión de seguridad, donde la inversión en tecnología se confunde con eficacia real. La ausencia de un incidente no significa inmunidad; a menudo, solo significa que aún no te han atacado de la manera correcta.

El Paradigma de la Validación Continua: El "Chequeo Médico" de tu Ciberseguridad.
El eje de su presentación giró en torno a un cambio de mentalidad crucial: pasar de la prevención basada en supuestos a la **validación continua basada en evidencias**.

"¿Desde cuándo no nos hacemos un análisis o examen? Es lo mismo con la ciberseguridad", afirmó. Así como una persona se realiza análisis de sangre y estudios para verificar su salud, las organizaciones deben realizar **"chequeos" regulares y exhaustivos** de sus defensas.

Esto implica: Simular ataques reales, medir la resiliencia real, cerrar brechas de forma proactiva.

Líderes empresariales, expertos en TI y ciberseguridad se dieron cita para fortalecer las defensas digitales de la región y convertir la protección de datos en una ventaja competitiva.

León, Guanajuato, 11 de Septiembre 2025.
El panorama de la ciberseguridad en México evoluciona a un ritmo vertiginoso, y la comunidad de León, Gto., ha respondido con unión y conocimiento. El evento Hack The Road celebró con éxito su edición en la ciudad, reuniendo a los principales actores del sector en un foro de colaboración, aprendizaje y networking de alto nivel.

La fotografía que acompaña este artículo es un testimonio del compromiso colectivo. En ella, se encuentra representado un ecosistema completo: desde las empresas que mueven la economía local y nacional hasta los profesionales que protegen su infraestructura digital. Agradecemos la invaluable participación de organizaciones como **Ricoh Impresoras, Sucahersa, Grupo Andrea, Congreso del Estado de Guanajuato, Flecha Amarilla, Grupo Charly, Cooperativa de Desarrollo, HDI Seguros, Médica Campestre, Caja Popular Mexicana, BanBajio, Tovar Abogados, Irish IO, Rent a Hacker, Duriva, etc.**

El evento congregó a un selecto grupo de profesionales, incluyendo **Coordinadores de Seguridad Informática, Auditores Internos, CISOs, Analistas de Arquitectura, Especialistas en Seguridad, CIOs, Ingenieros en Sistemas, Jefes de Seguridad Informática, Analistas de Seguridad y el Director de Tecnologías y Gobierno Digital**, quienes enriquecieron las discusiones con sus perspectivas únicas.

Juan Carlos Vega
Fundador Nuvol Cybersecurity
jvega@cybernuvol.com

NUVOL: LA DIFERENCIA ESTÁ EN EL ACOMPAÑAMIENTO CONTINUO

Juan Carlos Vega, fundador y CEO de la compañía, enfatizó que el elemento diferenciador de Nuvol es el acompañamiento continuo a través de Gerentes de Servicios de Ciberseguridad (CSM) dedicados para cada una de sus soluciones.

No solo vendemos herramientas; somos una extensión de su equipo de ciberseguridad", afirmó Vega. "Nuestro compromiso es entender los desafíos específicos de cada cliente para ofrecer soluciones integradas y un soporte estratégico continuo, asegurando que maximicen su postura de seguridad.

Para cumplir con esta promesa, Nuvol se alía exclusivamente con marcas líderes reconocidas por analistas globales como Gartner y Forrester.

Estrategia Digital

22 de Septiembre, 2025

En un mundo donde la transformación digital redefine los límites de la administración pública, la seguridad de la información se erige como el pilar fundamental para garantizar no solo la eficiencia, sino también la confianza ciudadana. **El Congreso del Estado de Guanajuato,** consciente de este imperativo, ha emprendido una estrategia integral de ciberseguridad.

Al frente de esta crucial misión se encuentra el **Mtro. Mario Alberto Díaz Muñoz,** Coordinador de Seguridad y Aplicaciones, un líder cuya visión trasciende la mera implementación tecnológica. Para él, la verdadera fortaleza de cualquier sistema reside en las personas. En esta entrevista exclusiva con Cateryn Farfán, el Mtro. Díaz Muñoz desglosa los objetivos centrales de una estrategia que prioriza la creación de una cultura de prevención entre cada colaborador del Poder Legislativo, demostrando cómo la ciberseguridad es, en esencia, el guardián de la democracia digital. A continuación, la conversación.

Mtro. Mario Alberto Diaz Muñoz
Coordinador de Seguridad y Aplicaciones. Congreso del Estado de Guanajuato

Visión y Liderazgo: ¿Cuál es el objetivo principal de la estrategia de ciberseguridad del Congreso? ¿Cómo se alinea con la modernización y transparencia de la labor legislativa?

Cateryn, te platico: el objetivo principal de nuestra estrategia de ciberseguridad en el Congreso es proteger la información que le pertenece a los ciudadanos y, al mismo tiempo, lograr que la labor legislativa sea más moderna, abierta y transparente. Y la verdad, no todo se reduce a la tecnología; lo más importante son las personas y la forma en que la usan con responsabilidad. Cada colaborador juega un papel clave en este esfuerzo.

Por eso, cada año organizamos la **Semana de la Seguridad, donde capacitamos a todos en temas de ciberseguridad**. De hecho, el próximo mes tendremos la edición en este 2025. Es una iniciativa sencilla, pero muy poderosa, porque lo que buscamos es crear una verdadera cultura de prevención. Al final del día, la confianza digital se construye con pequeñas acciones: desde cuidar una contraseña hasta manejar con responsabilidad la información legislativa.

Logros y Milestones: ¿De qué avance o implementación concreta te siente más orgulloso tu equipo?

Cateryn, te comparto que los logros en materia digital han sido siempre fruto del trabajo en equipo entre la Dirección de Innovación y Desarrollo Tecnológico y las distintas áreas del Congreso. **Uno de los hitos más importantes fue el sistema para leyes de ingresos municipales,** que incluso fue reconocido por Microsoft como caso de éxito y con el que obtuvimos el premio 'Innovación Pública' Mentefactura 2023.

Hoy seguimos marcando pauta, participando en los Premios de Ciberseguridad AMCS 2025, de los cuales muy pronto conoceremos los resultados. Además, nos consolidamos como Autoridad Certificadora del Poder Legislativo, con el desarrollo del sistema de Notificaciones Electrónicas, que ya utilizan municipios, organismos autónomos y los tres poderes del Estado.

A esto se suma el distintivo M100 por el uso de software 100% legal (Microsoft), además de varios desarrollos internos que fortalecen la operación diaria del Congreso. Fuimos certificados como Great Place to Work y por ultimo NMX-R-025-SCFI en Igualdad Laboral y No Discriminación. Todo esto, Cateryn, refleja que la innovación y la seguridad digital son parte esencial de nuestra misión de servir con transparencia y generar confianza en la ciudadanía.

Desafíos Únicos: ¿Cuáles son los retos específicos de proteger una institución legislativa, comparado con el sector privado u otras dependencias de gobierno?

Cateryn, proteger una institución legislativa como el Congreso en el ámbito digital es un reto muy particular. No se trata solo de cuidar equipos o sistemas, sino de resguardar información sensible que influye directamente en la vida pública y en las decisiones que afectan a toda la sociedad. **A diferencia del sector privado, donde muchas veces los ataques buscan un beneficio económico, aquí también entran en juego factores políticos y sociales, lo que vuelve la tarea mucho más compleja**

Por eso, la seguridad informática no puede quedarse únicamente en las herramientas tecnológicas; necesita de una estrategia integral que combine prevención, capacitación y resiliencia institucional.

La meta siempre debe ser clara: garantizar que la información esté protegida y que el Congreso pueda seguir trabajando con transparencia y confianza, incluso frente a las amenazas digitales más avanzadas. Y te digo algo muy importante: nada de esto sería posible sin usuarios preparados y conscientes.

Por eso reciben capacitación constante no solo en temas de seguridad informática, sino también en ofimática y otros temas que fortalecen su trabajo diario. Al final, cada colaborador se convierte en la primera línea de defensa de la institución.

Cooperación: ¿Cómo es la colaboración en materia de seguridad con otras entidades del gobierno estatal o federal?

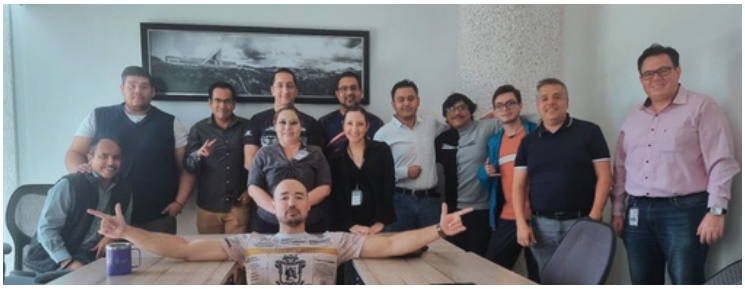
Cateryn, la ciberseguridad no es un trabajo que uno pueda hacer solo, siempre va acompañado de un gran equipo. En mi caso, comienza desde mi coordinación de Seguridad y Aplicaciones, donde lo que busco es impulsar a cada compañero para que dé lo mejor de sí, y juntos podamos construir un entorno más seguro para el Congreso. Te platico que nuestra relación con otras dependencias de gobierno, la comunicación es muy cercana, y eso nos permite apoyarnos, compartir experiencias y aprender unos de otros. **Esa confianza entre instituciones se ha convertido en una gran fortaleza,** porque cuando trabajamos unidos, los retos se vuelven más fáciles de enfrentar y el objetivo es el mismo: proteger a las instituciones y, con ello, a la ciudadanía.

Además, hemos logrado una relación muy abierta entre las Direcciones de Tecnologías de la Información, siempre con disposición para coordinarnos y sumar esfuerzos. Participamos en eventos y conferencias organizados por fabricantes y asociaciones que nos mantienen actualizados y nos permiten fortalecer nuestra visión. Un ejemplo muy claro fue el evento Hack the Road, en el que estuvimos hace apenas unas semanas. Ahí convivimos con colegas de ciberseguridad, intercambiamos ideas y nos nutrimos de experiencias reales. Estos espacios son clave para crecer como comunidad y estar mejor preparados frente a cualquier amenaza digital.

Mirada al Futuro: ¿Hacia dónde se dirige la ciberseguridad en el Congreso del Estado de Guanajuato? ¿Qué proyectos vienen en el horizonte?

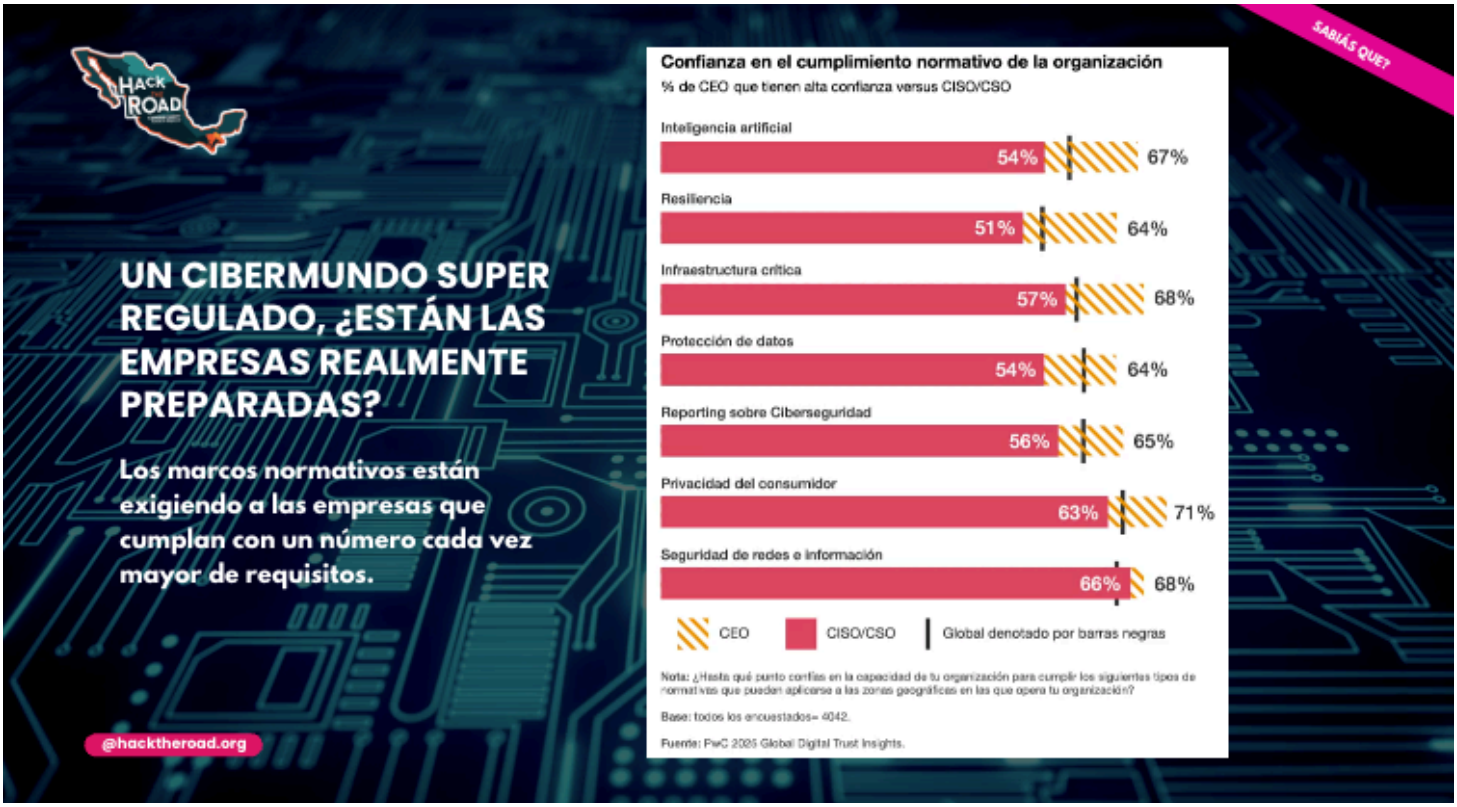
Cateryn, para cerrar, te comparto que el futuro de la ciberseguridad en el Congreso del Estado de Guanajuato está en seguir innovando. No podemos quedarnos quietos, porque las amenazas evolucionan todos los días, y la mejor manera de enfrentarlas es con preparación y con visión. Queremos aprovechar tecnologías como la inteligencia artificial, no solo en los sistemas, sino también como apoyo a los usuarios, ayudándolos a ser más conscientes y capaces en su vida digital. Sabemos que los retos no se van a detener, por eso nuestra apuesta es seguirnos preparando constantemente, tanto de manera individual como institucional. **Entre mejor formados estemos, más fuerte será nuestra capacidad de respuesta**.

Antes de terminar, **quiero agradecer profundamente a mi familia, a mi esposa y a mis hijos,** porque ellos son mi motor, mi inspiración y la razón principal por la que cada día busco dar lo mejor de mí. Su apoyo incondicional ha sido fundamental para poder avanzar en este camino con firmeza y entusiasmo.



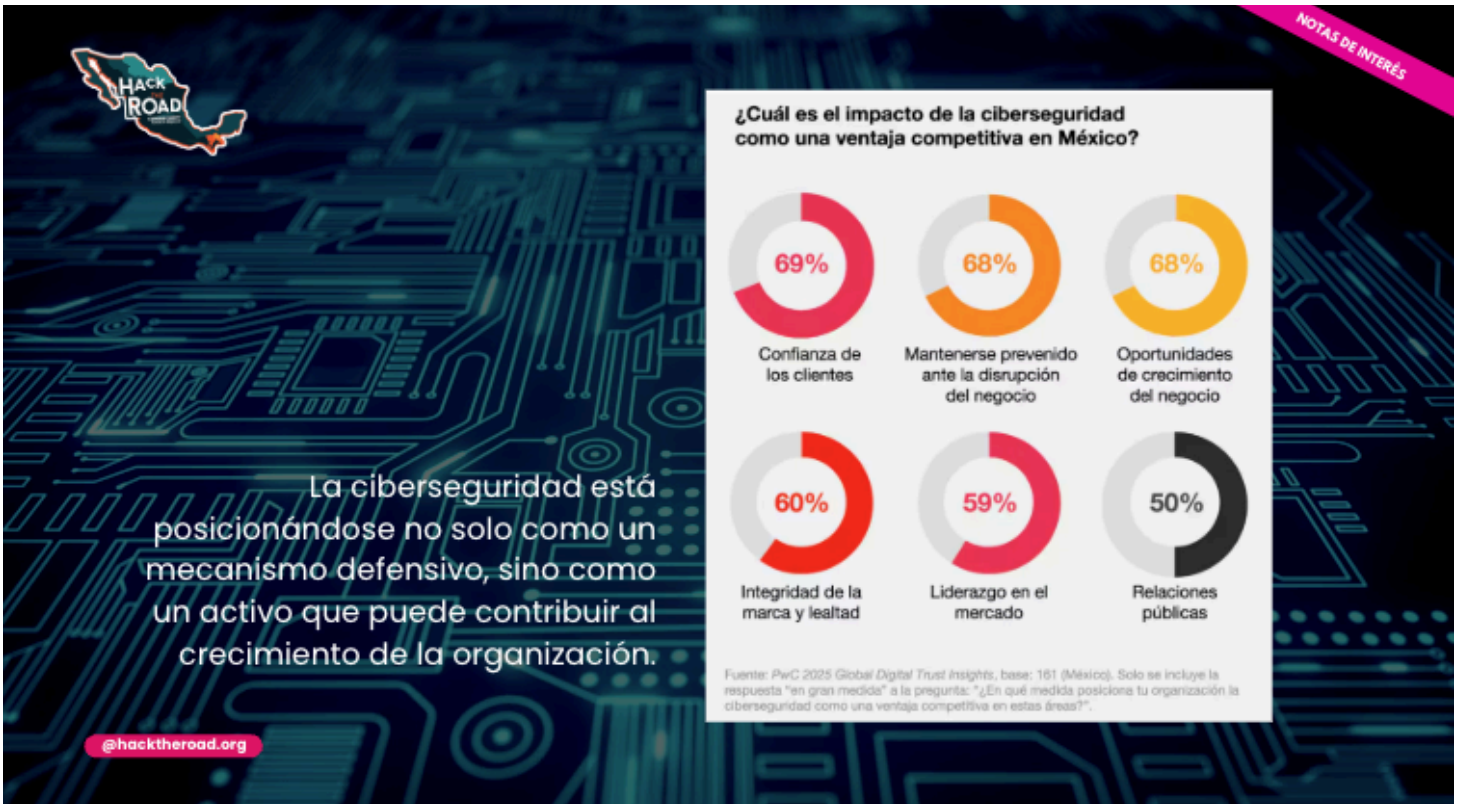
Por último, Cateryn, quiero reconocer con mucho orgullo el esfuerzo y la dedicación de mis compañeros de la Dirección de Innovación y Desarrollo Tecnológico: **Gabriela Farfán, Paulina Villegas, Víctor Lozano, Eduardo Rocha, David Anaya, Noé Herrera, Esteban Valtierra, Jorge Ávila, Pablo Herrera, Julio García, Jair Chávez y Héctor Meza.** Gracias a cada uno de ustedes hemos logrado consolidar un gran equipo en todas las coordinaciones, trabajando hombro con hombro para ofrecer un servicio de calidad a los usuarios del Congreso. **¡Es un honor compartir este camino con ustedes! ¡Avante!**

CUMPLIMIENTO – ¿ESTÁN LAS EMPRESAS REALMENTE PREPARADAS?

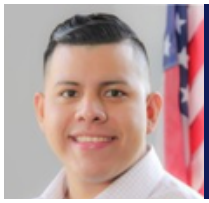


PricewaterhouseCoopers, S.C. / Reporte 2025

¿CUAL ES EL IMPACTO DE LA CIBERSEGURIDAD COMO UNA VENTAJA COMPETITIVA?



PricewaterhouseCoopers, S.C. / Reporte 2025



Josh Martinez
Proficio Regional Sales Manager- NorthEast II
jmartinez@proficio.com

Para las empresas de la región que buscan escalar su seguridad, cumplir con regulaciones y proteger su reputación, el SOC as a Service de PROFICIO se posiciona como la solución integral, humana y tecnológicamente superior.

PROFICIO FORTALECE LA CIBERSEGURIDAD EN EL BAJÍO

SOC as a Service, la Solución para Empresas que Buscan Protección Avanzada y un Aliado Estratégico

La verdadera diferenciación de PROFICIO radica en su modelo de servicio centrado en el partnership. No solo se vende una herramienta; se ofrece una extensión dedicada de su equipo de ciberseguridad.

El pilar de este valor agregado es la figura del Customer Success Manager (CSM) dedicado. A diferencia de otros proveedores que ofrecen soporte genérico, cada cliente de PROFICIO cuenta con un CSM especializado que se convierte en un miembro integrado de su organización.

1. **Apoyo en la Gestión de Alertas:** Actúa como un primer punto de contacto experto, priorizando incidentes y coordinando la respuesta entre el SOC de PROFICIO y el equipo interno del cliente.
2. **Entendimiento de Reportes:** Traduce los hallazgos técnicos del SOC en lenguaje de negocio, ayudando a los líderes a comprender el panorama de riesgos y el ROI de su inversión en seguridad.
3. **Guía Estratégica:** Proporciona recomendaciones accionables para mejorar la postura de seguridad basándose en los insights obtenidos de la monitorización continua.
4. **Onboarding y Capacitación:** Asegura una implementación fluida del servicio y capacita a los equipos locales para maximizar su valor.

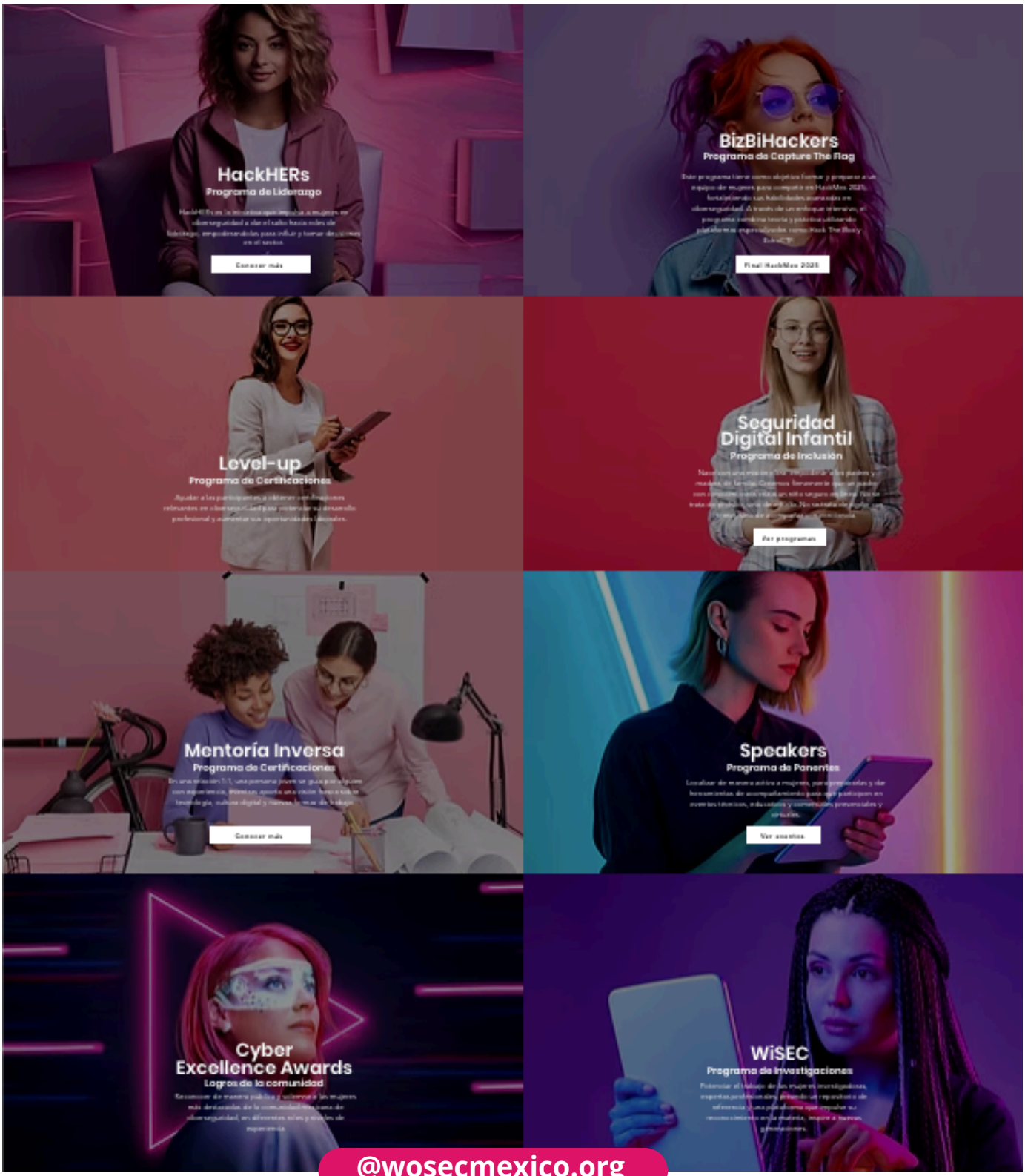
Mujeres Transformando el Panorama de la Ciberseguridad en León

@hacktheroad.org

León, Guanajuato, 11 de Septiembre 2025.
En un ámbito históricamente dominado por hombres, el talento femenino en ciberseguridad emerge con fuerza, liderazgo y una visión única e invaluable. Este encuentro refuerza una verdad poderosa: el futuro de la ciberseguridad es diverso, colaborativo y está lleno de talento femenino. Agradecemos profundamente a cada una de ellas por compartir su conocimiento y su pasión:

- Gisela Ríos, con su expertise en Cumplimiento, nos recordó la crucial importancia de alinear los procesos con los marcos normativos.
- Lizbeth Márquez, CISO de HDI Seguros, compartió la visión estratégica desde una de las aseguradoras más importantes, liderando la protección de datos en un sector crítico.
- La mesa redonda sobre Security Awareness (Concientización en Seguridad) estuvo en las mejores manos con Ana Laura Mena, Líder de Ciberseguridad, y Cateryn Farfán de WoSEC Mexico, quienes destacaron que el eslabón humano puede ser la mayor fortaleza cuando está bien informado.
- Alma, Coordinadora de Seguridad Informática de Cooperativa de Desarrollo, junto con Kathia y Mónica, Especialistas en Seguridad Informática de Caja Popular Mexicana, nos brindaron una perspectiva esencial sobre la protección de los sectores financieros populares y cooperativos, tan vitales para nuestra comunidad.
- Como invitada especial, Nathziri Tovar de Tovar Abogados elevó la conversación con su ponencia “De la Brecha al Tribunal: La Nueva Era de la Ciberseguridad como Obligación Legal en México”, un recordatorio crucial de que los incidentes de seguridad hoy tienen repercusiones legales tangibles.
- Fanny y Rosa de Maps Disruptivo nos guiaron a través de las capacidades de PICUS Security, demostrando herramientas disruptivas para la validación de controles de seguridad. Una mención especial para Bianca, quien recién se suma a esta comunidad, demostrando que el interés por esta apasionante campo sigue creciendo y Nancy Salazar de Tekis Services.

WoSEC México es más que una comunidad; es un motor de cambio que empodera a las mujeres, construye una red de apoyo sólida y enriquece el ecosistema de ciberseguridad en el país con talento diverso y perspectivas únicas. Conoce sus programas:



@wosecmexico.org

Comentarios de la Comunidad

Alma Oliva · 1er
Cybersecurity Engineer | Securing ...
1 minuto ·

Ayer tuve la oportunidad de asistir a HACK THE ROAD - CYBERSECURITY MEXICO y realmente fue una experiencia muy provechosa. Las ponencias fueron excelentes, aportando ideas y experiencias muy valiosas.
Un gusto coincidir con tantas personas llenas de experiencia, conocimiento y ambición, con quienes ahora podemos formar comunidad en el Bajío y sus alrededores.
Gracias al equipo de HACK THE ROAD - CYBERSECURITY MEXICO, a Cateryn Farfán por la invitación y a los sponsors que lo hicieron posible .
El evento fue una combinación perfecta: un poco de todo, en un ambiente profesional, amable y divertido.
Es curioso ver cómo, aunque venimos de sectores distintos, los retos del día a día tienen mucho en común y podemos aprender unos de otros.
Espero con entusiasmo los próximos eventos y que sigamos creando espacios así de enriquecedores que nos recuerdan que el conocimiento crece cuando se comparte. Sigamos construyendo comunidad.

#HackTheRoad #CybersecurityMéxico #Ciberseguridad #Proficio #MDR #SOC #LeónGto #Ciberprotección #TI #SeguridadInformática #Mujeresenciberseguridad #WoSECMexico

Nancy N. Salazar 👩‍🦰🍭💕 · 1er
🌈 Analista de Planeación Estratégica Digit...
Ir a mi sitio web
1 semana ·

✨En efecto, el evento de #HacktheRoad no sólo se trató de código y ciberseguridad 👩‍💻, también compartimos una experiencia de parrilla que estuvo genial.🔥🥩🔪🍽

⭐ Muchas gracias al equipo de Hack The Road - Cybersecurity México por rifársela en la organización, y gracias también a Cateryn Farfán por la invitación y por la buena vibra de crear comunidad.❤️🦄💻✨

Mario Alberto Díaz Muñoz · 1er
Especialista en Ciberseguridad | ISO 27001 | ISO 22301 | Ethical ...
1 semana ·

muy contento de este primer encuentro con colegas en temas de ciberseguridad

Comentarios de la Comunidad

Iván Magallanes Morón · 1er
CIO, CTO, CDTO, CISO
1 semana • Editado •

Excelente iniciativa para ir haciendo comunidad en el bajío. La Ciberseguridad es primero. #hacktheroad

Hack The Road - Cybersecurity México
460 seguidores
1 semana • Editado •

Ayer vivimos una jornada extraordinaria. Mi más sincero agradecimiento a cada una de las personas que formó parte de 🚀 Hack The Road - Cybersecurity México 2025 ... más

Josh Martinez · 1er
I help protect companies from Cybersecuri...
1 semana • Editado •

Last week, I had the privilege of representing PROFICIO at our partner Nuvol's Hack The Road - Cybersecurity México conference in Guanajuato, Mexico 🇲🇽. It was an incredible experience meeting and learning from some truly world class executives.

One of the things I love about this industry is that no matter where we are in the world, we all speak the same cybersecurity language, protecting organizations, sharing knowledge, and building stronger defenses together.

And of course... only in Mexico do you start the day with chilaquiles for breakfast at 7am 🌄 and end it with an unforgettable grilling experience 🔥🥩

Fun fact: Guanajuato is known as the leather capital of LATAM and I can confirm the craftsmanship is impressive ‼️

No todo es firewalls y código.

Gracias Comunidad de León

El pasado 11 de septiembre, León, Guanajuato, se vistió de gala para ser el escenario de un sueño hecho realidad: la primera edición de Hack The Road. H**oy, queremos dedicar estas líneas a expresar nuestro más sincero y profundo agradecimiento a cada persona que se sumó, participó y creyó en esta iniciativa. Su energía y entusiasmo fueron la fuerza vital que convirtió una idea en un espacio vibrante y lleno de posibilidades.**

En Hack The Road, tenemos la convicción de que el crecimiento en ciberseguridad se da en comunidad. Por eso, nuestro objetivo central fue crear un espacio donde pudieran converger conversaciones técnicas profundas, el apoyo de especialistas y la oportunidad de tejer una red de contactos valiosa.

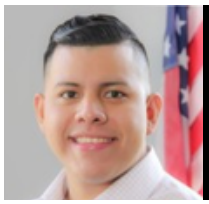
Queremos que esta comunidad sea un pilar para:

- Compartir aprendizajes a través de charlas y talleres accesibles.
- Visibilizar el increíble talento en ciberseguridad que existe en León, Guanajuato.
- Conectar a estudiantes, profesionales emergentes y expertos consolidados.
- Apoyarnos mutuamente en nuestros logros y proyectos.
- Desarrollar habilidades de la mano de otras comunidades y especialistas.

Agradecemos a cada participante por confiar en nosotros y por ser parte activa de las dinámicas. Su curiosidad y participación fueron el termómetro del éxito del evento. A los ponentes y especialistas, gracias por compartir su expertise y por tender la mano para futuras colaboraciones; su apoyo es invaluable.

El cierre de esta primera edición no es un adiós, sino un "¡aquí estamos!". Este es solo el primer paso en un camino que deseamos recorrer juntos. Los comentarios, las nuevas conexiones y la energía generada son el combustible que nos impulsa a seguir creando espacios de valor. Gracias por confiar en Hack The Road. Fue un honor compartir con ustedes este momento histórico para nuestra comunidad. ¡Estén atentos porque esto no para aquí!

Directorio



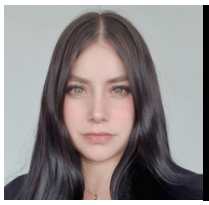
Josh Martinez
Proficio Regional Sales Manager- NorthEast II
jmartinez@proficio.com

Daniel E. López
Microsoft Cybersecurity Architect Expert
dlopez@cybernuvol.com

Gisela Rios Villa
Compliance and Regulatory Expert
grios@cybernuvol.com

Félix López Peña
CTO
felix.lopez@maps.com.mx

Carlos Lozano
Ethical Hacker & Consultor Seguridad Informática
augusto@rentahacker.com.mx



Nathziri Tovar
Abogada Digital
ntovar@tovarabogados.mx

Alejandro Jocsan
Perito Informático
jocsan@duriva.com

Juan Carlos Vega
Fundador Nuvol Cybersecurity
jvega@cybernuvol.com

Cateryn Farfán
Coordinadora Hack The Road
mexico@hacktheroad.org

La Caravana de ciberseguridad
León - Guanajuato 2025

@HACKTHEROAD.ORG