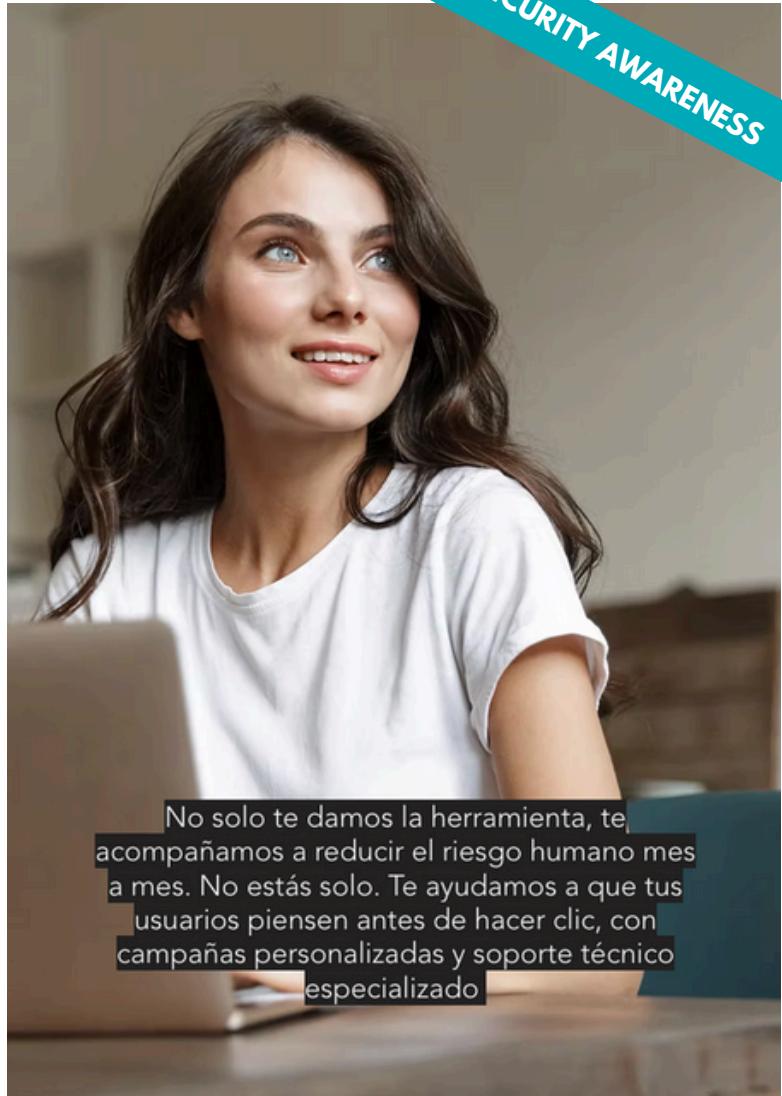


Plataformas de Security Awareness autogestionadas

¿Cansado de implementar herramientas de concienciación que no generan resultados? **Nuvol se encarga de todo:** desde la configuración hasta el análisis de métricas, con un equipo dedicado a reducir tu riesgo humano.

- Administramos la herramienta por ti: configuraciones, métricas y ajustes según tus objetivos.
- Know-how local: Expertos en LATAM que entienden riesgos regionales
- Soporte proactivo: reuniones mensuales, informes de progreso y mejora continua.
- Entendemos los desafíos de ciberseguridad en LATAM y adaptamos las estrategias a tu cultura organizacional.

Security Awareness no es un software, es un proceso. En Nuvol, lo hacemos realidad contigo



Nuvol es partner de las Principales Plataformas de Security Awareness

Nuvol es partner de las Principales Plataformas de Security Awareness

Llevamos más de 7 años ayudando a organizaciones en Latinoamérica a fortalecer su Security Awareness con estrategias efectivas y adaptadas a sus necesidades. Con más de 57 clientes en Panamá, México, Colombia y otros países, hemos apoyado a empresas de diversos sectores a reducir su riesgo humano y reforzar su postura de seguridad.

En Nuvol, somos partner oficial de las plataformas líderes en el mercado:



Nuestra Misión: Reducir el Riesgo Organizacional

Nuestra experiencia con múltiples plataformas nos permite ofrecer soluciones personalizadas, diseñadas para integrarse sin problemas con los objetivos de las áreas de Ciberseguridad y TI. No solo implementamos herramientas, sino que creamos una cultura de seguridad en tus usuarios finales, con métricas claras y resultados medibles.



¿Cuál es la mejor herramienta?

Depende de las necesidades de cada cliente. Lo más importante es que Nuvol tiene el Know-How para implementarlas correctamente, maximizando su potencial y asegurando resultados.

¿Por Qué Elegir Nuvol para tu Security Awareness?

Acompañamiento Continuo y Proactivo

- Campañas mensuales personalizadas: Diseñamos y ejecutamos simulaciones de phishing adaptadas a tus riesgos reales.
- Optimización constante: Aseguramos que la plataforma elegida (KnowBe4, HoxHunt o Smartfense) rinda al máximo.
- Métricas accionables: Reportes claros que miden progreso y áreas de mejora.

Customer Success Manager (CSM) Dedicado

- Un experto asignado a tu cuenta: Garantiza continuidad y alineación con tus objetivos.
- Soporte estratégico: No solo resolvemos dudas, mejoramos tu estrategia internamente.
- Nuestro éxito se mide con el tuyo: Si tus KPIs de riesgo no bajan, nosotros no cumplimos

Compromiso Real con los Resultados

- No somos un vendedor más, somos un equipo extendido: Nos sumamos a tus iniciativas internas.
- Enfoque práctico: Combina tecnología + cambio cultural



Uno de los principios de KnowBe4 es continuamente



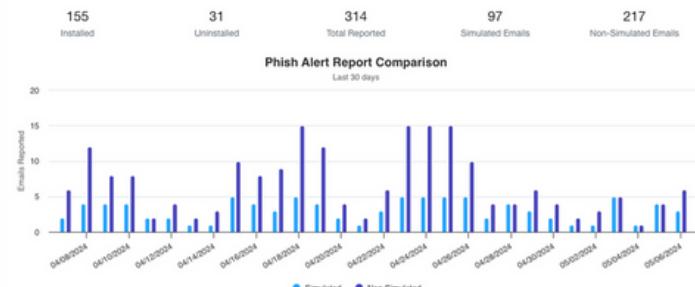
- 1. Entrenar a los usuarios:** KnowBe4 cuenta con la biblioteca más grande de contenido sobre conciencia de seguridad. Contenido en video tipo Netflix, módulos interactivos, videojuegos, carteles, etc. (más adelante hablaremos de él)
- 2. Probar a los usuarios con campañas de phishing simulado:** para medir los conocimientos aprendidos de los usuarios se envían pruebas de phishing. Phishing simulados totalmente automatizados y con plantillas que se pueden adaptar o regionalizar.
- 3. Analizar los resultados:** estadísticas e informes gráficos de alto nivel, incluso tendrá una línea de tiempo por cada usuario, grupo o departamento.

The dashboard includes sections for My Dashboard (highlighted) and Team Dashboard. It shows a message about completed training, 26 unread messages, and a personal risk score of 38.8. It also displays a bar chart of Phish Alert Report Comparison and a stacked bar chart of Phishing Security Tests - Last 6 Months.

Category	Value
Installed	155
Uninstalled	31
Total Reported	314
Simulated Emails	97
Non-Simulated Emails	217

Category	Value
Clicks	~30%
QR Codes Scanned	~10%
Attachments Opened	~5%
Macro Enabled	~5%
Callback Data Entered	~5%
Reported	~5%
Data Entered	~5%
Phish-prone %	~5%

Phish Alert Button



Phishing



Your Organization
Account Average
Last Campaign
Industry Benchmarks
Industry
Organization
Program Manager

"Seguridad informática que transforma conductas: Más protección, menos riesgos"

Smartfense es la plataforma para brindar al usuario final una experiencia única y entretenida para fortalecer de manera positiva la concienciación en seguridad informática.

Para las áreas de seguridad informática la plataforma nos proporciona todos los Indicadores que necesitamos.

- KPI Riesgo Organacional
- Reportes de campañas de phishing
- Reporte de campañas de capacitación
- Grado de conocimiento de los usuarios sobre políticas
- Reporte Gamificación
- Mapa de Calor que señala nivel de riesgo

The dashboard shows a user profile icon, progress bar (15%), and various activity counts: Módulos Interactivos (Asignados: 0), Videos (Asignados: 0), Newsletter (Asignados: 0), Encuestas (Asignados: 0). It also displays a cartoon character cheering at a desk with a laptop, and a message: "No tienes contenidos pendientes." Below this are sections for "Contenidos disponibles" and "Contenidos finalizados", each listing several items with star ratings.

Herramientas de Educación y Refuerzo

Todos los contenidos de la plataforma pueden editarse, utilizarse como plantillas para la creación de otros, o bien crearse nuevos desde cero.

Videos

The interface shows a sidebar with navigation options like 'Módulos', 'Reportes', 'Análisis', 'Aprendizaje', 'Newsletter', 'Encuestas', 'Plantillas', and 'Configuración'. The main area displays a list of video modules with preview thumbnails and titles such as 'CÁVALO EN TRABAJO', 'PERDIDOS', 'TÍTULOS DE CINE', 'LA VIDA EN EL MUNDO', and 'EL JUEGO DE LOS CIBERMONJAS'.

Videojuegos

The interface shows a sidebar with navigation options like 'Módulos', 'Reportes', 'Análisis', 'Aprendizaje', 'Newsletter', 'Encuestas', and 'Configuración'. The main area displays a game titled 'Pass Slam' showing a tennis court with players and a scoreboard.

Módulos Interactivos

The interface shows a sidebar with navigation options like 'Módulos', 'Reportes', 'Análisis', 'Aprendizaje', 'Newsletter', 'Encuestas', and 'Configuración'. The main area displays a module titled 'El CiberMachismo' with a comic strip featuring characters and text in Spanish.

Newsletter

The interface shows a sidebar with navigation options like 'Módulos', 'Reportes', 'Análisis', 'Aprendizaje', 'Newsletter', 'Encuestas', and 'Configuración'. The main area displays a newsletter section with various news items and images.

Presentamos AI Phishing Coach: capacitación personalizada y autónoma en concientización sobre seguridad.

Descubra cómo Abnormal transforma la capacitación en seguridad con simulaciones de phishing personalizadas, entrenamiento en tiempo real y gestión de programas totalmente autónoma.



[Setup Training](#)

[Download Video](#)

Coaching Strategy

Customized security training for Enterprise Corp employees.

Construction Industry Focus

- Incorporates Enterprise Corp's specific project management workflows and document handling protocols
- Features screenshots of actual construction project management systems for contextual learning

Content Delivery

- Examples feature industry-specific threats targeting construction businesses and project bids
- Optimized for both office and field devices to support regional offices and construction sites

Selecting Real Attack

AI chose a relevant real attack from recent stopped threats.

Data Sources:

- Threat Log (last 30 days)
- 783 attacks

Found Attack Details:

Subject: Urgent: Verify Your Account
Recipient: michael.thompson@company.com
Time Received: Aug 1, 10:23am EST

 **Sarah Chen**
Principal Engineer

Email: sarah.chen@company.com

Manager: Michael Thompson

Team: Platform Engineering

Generating Coaching Strategy

AI is analyzing user behaviors to create personalized coaching.

Types of Attacks User Has Encountered:

- Social Engineering:
- Spear Phishing:

Training Content

Threat Awareness

- Understanding and identifying phishing emails and social engineering attacks
- Recognizing malware, ransomware, and other cyber threats
- Insider threat awareness and prevention strategies
- QR code security and safe scanning practices

Best Practices

- Password management and multi-factor authentication
- Safe social media usage in professional contexts
- Secure use of devices and applications
- Remote work security guidelines

Compliance and Incident Response

- Overview of relevant privacy regulations
- Industry-specific compliance requirements
- Incident reporting procedures
- Your role in the incident response process

Emerging Security Challenges

- AI-based security threats and defenses
- Protection against generative AI tools
- Cyberbullying prevention and response
- Shadow IT risks and management

If you would like to make changes to your video, please reach out to Abnormal Support.

AI Phishing Coach cambia eso con simulaciones de phishing personalizadas basadas en datos de amenazas específicos de los empleados. Gracias a la integración segura de la API de Abnormal AI, AI Phishing Coach aprovecha el contexto organizacional, como la función laboral y los patrones de comunicación habituales, para adaptar mejor la capacitación.

Esto significa que los empleados reciben pruebas y capacitación sobre los tipos de ataques que probablemente verán en la práctica. Esto comienza con el análisis de amenazas reales y remediadas en el Registro de Amenazas. Los ataques se seleccionan y se neutralizan para enviarse a cada empleado como simulaciones basadas en:

- Rol y responsabilidades del empleado
- Los tipos de ataques dirigidos a un empleado y sus pares en roles similares en la organización
- Participación y tendencias de capacitación previa (es decir, sensibilidad específica del rol a las amenazas, resultados de simulaciones previas, cambios de comportamiento observados, etc.)