¿Cómo proteger los negocios en la era de la Inteligencia Artificial?

- *Claro empresas y Cisco presentaron soluciones y estrategias de ciberseguridad para proteger a las organizaciones frente a los nuevos desafíos que plantea la Inteligencia Artificial.*

Jueves, 26 de noviembre del 2026. La adopción de la Inteligencia Artificial está transformando el entorno empresarial, impulsando la productividad y la automatización. De acuerdo con el informe AI Index Report 2026[1] de la Universidad de Stanford, el uso de herramientas de IA generativa en las organizaciones se incrementó significativamente durante el último año, impulsando mejoras en productividad, automatización y análisis de información. Sin embargo, también plantea nuevos desafíos de ciberseguridad relacionados con la protección de datos, los accesos no autorizados y la continuidad operativa.

Este escenario cobra mayor relevancia con la IA agéntica, cuyos sistemas pueden ejecutar tareas, conectarse a aplicaciones e interactuar con información corporativa. Por ello, las empresas necesitan fortalecer sus controles y garantizar que cada identidad, humana o no humana, tenga únicamente los permisos necesarios y sea monitoreada continuamente.

Frente a este contexto, especialistas de Claro empresas y Cisco analizaron, durante una nueva edición del Tech Night, cómo el modelo de seguridad Zero Trust permite proteger a las organizaciones en un entorno digital cada vez más complejo.

Como parte del encuentro, presentaron Cisco Secure Access y Cisco Duo, dos soluciones integradas que permiten controlar quién o qué accede a los recursos corporativos, desde dónde y a qué información.

Cisco Secure Access es una solución de seguridad en la nube que protege el acceso de usuarios y agentes de IA a aplicaciones, datos e internet. Entre sus principales capacidades destacan:

- Restringe el acceso a aplicaciones autorizadas y reduce la superficie de ataque.
- Integra tecnologías ZTNA, SWG, CASB, DLP y firewall como servicio.
- Identifica herramientas de IA generativa autorizadas y no autorizadas (*shadow AI*).
- Establece políticas para el uso seguro de la IA y ayuda a prevenir la exposición de información confidencial.

Por su parte, Cisco Duo protege los recursos empresariales mediante la verificación continua de identidades, dispositivos y niveles de riesgo. Sus funcionalidades incluyen:

- Autenticación multifactor resistente al phishing.
- Verificación de la seguridad de los dispositivos.
- Políticas de acceso adaptativas según el nivel de riesgo.
- Detección de privilegios excesivos y comportamientos anómalos.
- Control de usuarios y agentes digitales bajo el principio de mínimo privilegio.

Durante la jornada, ambas compañías destacaron que la seguridad debe evolucionar al mismo ritmo que la tecnología, con estrategias que permitan reducir vulnerabilidades, proteger la información y mantener la continuidad de las operaciones.

En esa línea, Claro empresas integra capacidades de conectividad, infraestructura, nube y ciberseguridad, junto con aliados tecnológicos especializados, para acompañar a las organizaciones en su transformación digital y ayudarlas a innovar de manera segura.

El Tech Night reunió a líderes de tecnología, ciberseguridad y transformación digital, quienes compartieron experiencias y analizaron los desafíos que plantea la Inteligencia Artificial para la protección de los negocios.

Fuente:

[1] https://hai.stanford.edu/ai-index/2026-ai-index-report

Acerca de América Móvil
América Móvil es el proveedor líder de servicios integrados de telecomunicaciones en América Latina. A través del desarrollo de una plataforma integrada de telecomunicaciones de clase mundial, la compañía ofrece a sus clientes un amplio portafolio de servicios de valor agregado y soluciones avanzadas de comunicación en 23 países de América y Europa. Al cierre de junio de 2026, América Móvil contaba con 414.5 millones de accesos totales, incluyendo 334.3 millones de suscriptores móviles y 80.1 millones de unidades generadoras de ingresos de línea fija (RGUs). Conozca más en www.americamovil.com