OlimpIA | Sentry

El ciberataque no avisa, pero sí **impacta tu operación.**

Descubre cómo un **Centro de Operaciones de Seguridad (SOC)** opera con inteligencia artificial y expertos que protegen la continuidad de tu negocio.

La nueva realidad: los ataques ocurren todos los días

Las amenazas digitales dejaron de ser un problema exclusivo de grandes compañías. Actualmente, cualquier organización **(sin importar su tamaño o sector)** puede convertirse en objetivo de ataques que buscan interrumpir operaciones, secuestrar información o afectar la confianza de clientes y usuarios.

Por eso, la pregunta ya no es si una organización será atacada, sino **qué tan preparada está para detectarlo y responder a tiempo.**

La velocidad marca la diferencia

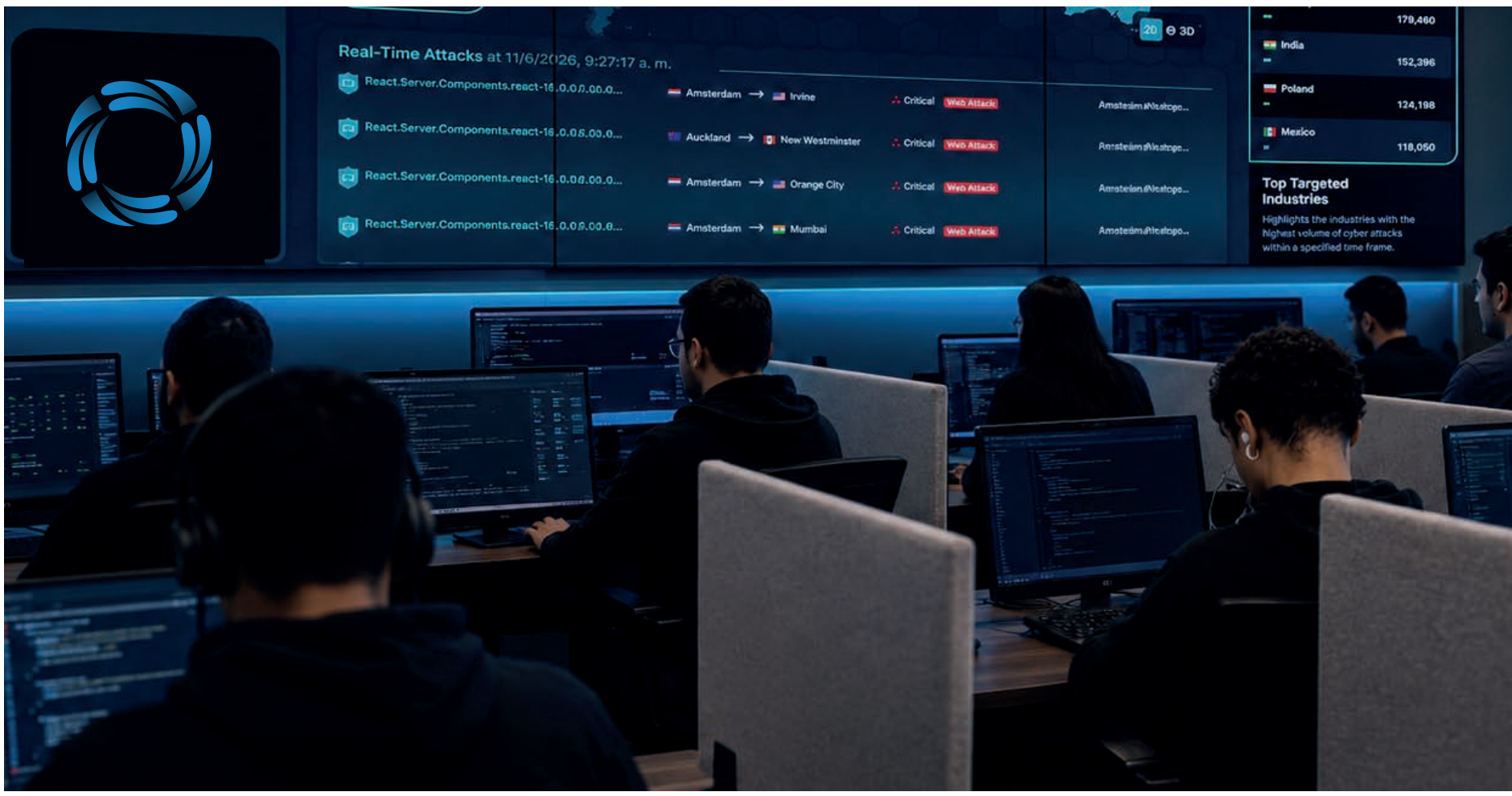
En ciberseguridad, el tiempo lo es todo. Es así como un incidente de seguridad puede generarse en cuestión de segundos.

Cuanto más tiempo permanezca una amenaza activa:

- Más tiempo sin detección = **mayor impacto operativo.**
- Mayor exposición = **más pérdidas económicas.**
- Mayor duración = **mayor daño reputacional.**

La capacidad de **monitorear, analizar y responder de manera continua** se ha convertido en uno de los factores más importantes dentro de cualquier estrategia moderna de seguridad digital.

¿Qué es un SOC y por qué es tan importante?



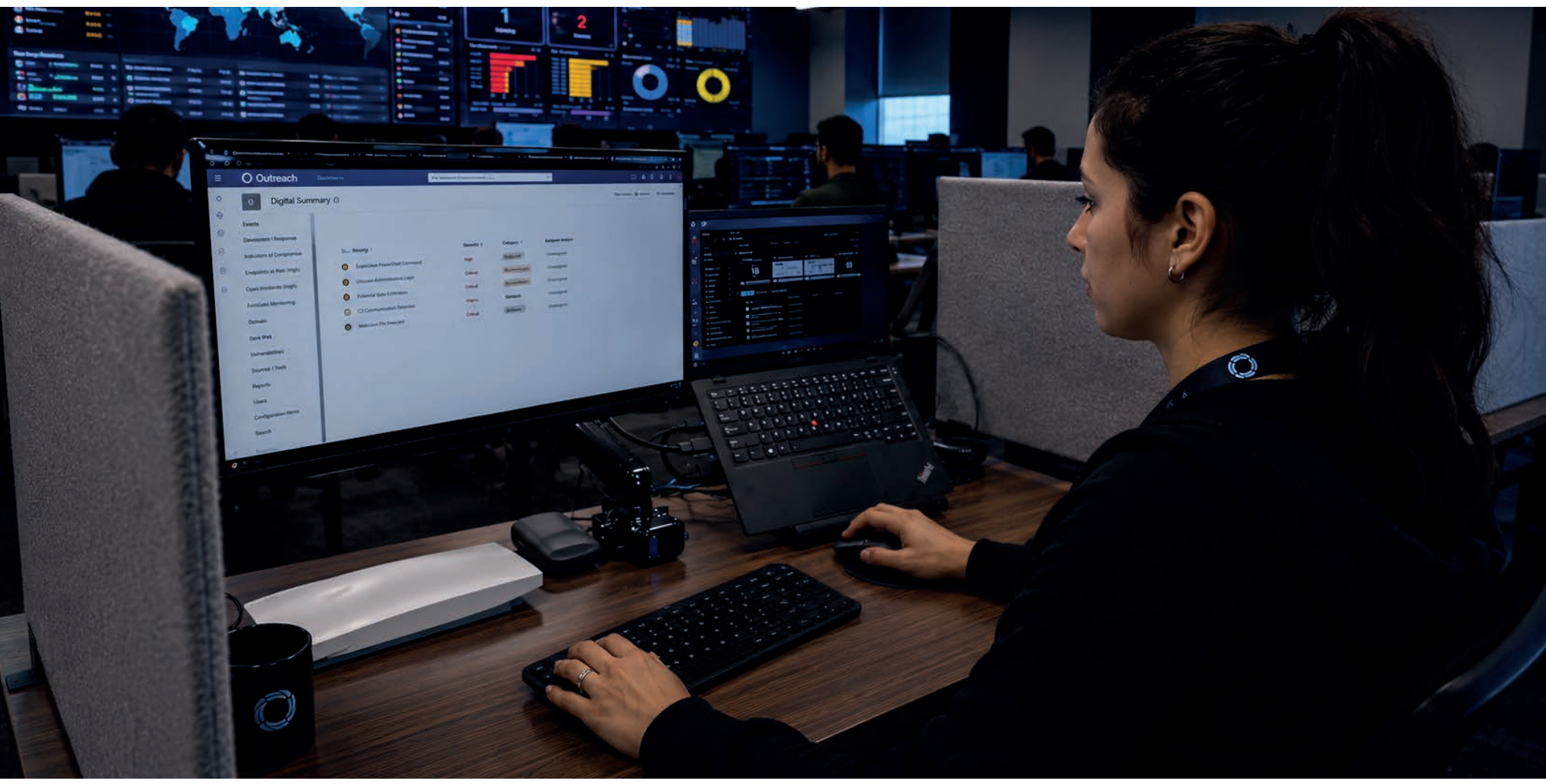
Un **Security Operation Center (SOC)** es el núcleo donde personas, procesos y tecnología trabajan de forma coordinada para monitorear y proteger **24/7 la seguridad digital de una organización.**

Funciona como una sala de control digital, desde donde se supervisa continuamente todo lo que ocurre en el entorno web, permitiendo detectar y responder a amenazas en tiempo real.

En OlimpIA contamos con el SOC más moderno del país, donde más de **30 expertos** en ciberseguridad analizan y correlacionan eventos de seguridad de manera continua, apoyados por la **inteligencia artificial y automatización avanzada.**

¿Qué hacemos desde **nuestro SOC?**

- **Monitoreo y detección:** supervisión constante de plataformas, entornos cloud y sistemas críticos para identificar riesgos y reducir la exposición a fraude.
- **Análisis de amenazas:** validación experta combinada con capacidades automatizadas para acelerar la respuesta.
- **Clasificación y priorización:** identificación del nivel de criticidad de cada incidente



- **Playbooks de respuesta:** ejecución de protocolos específicos según el tipo de ataque (ransomware, phishing, intrusión, entre otros).
- **Escalada y coordinación:** trabajo conjunto con los equipos del cliente para contener el riesgo de forma efectiva.
- **Reportes de incidentes:** generación de informes técnicos y ejecutivos, incluyendo lecciones aprendidas para fortalecer la seguridad.

Retos que enfrenta un SOC moderno

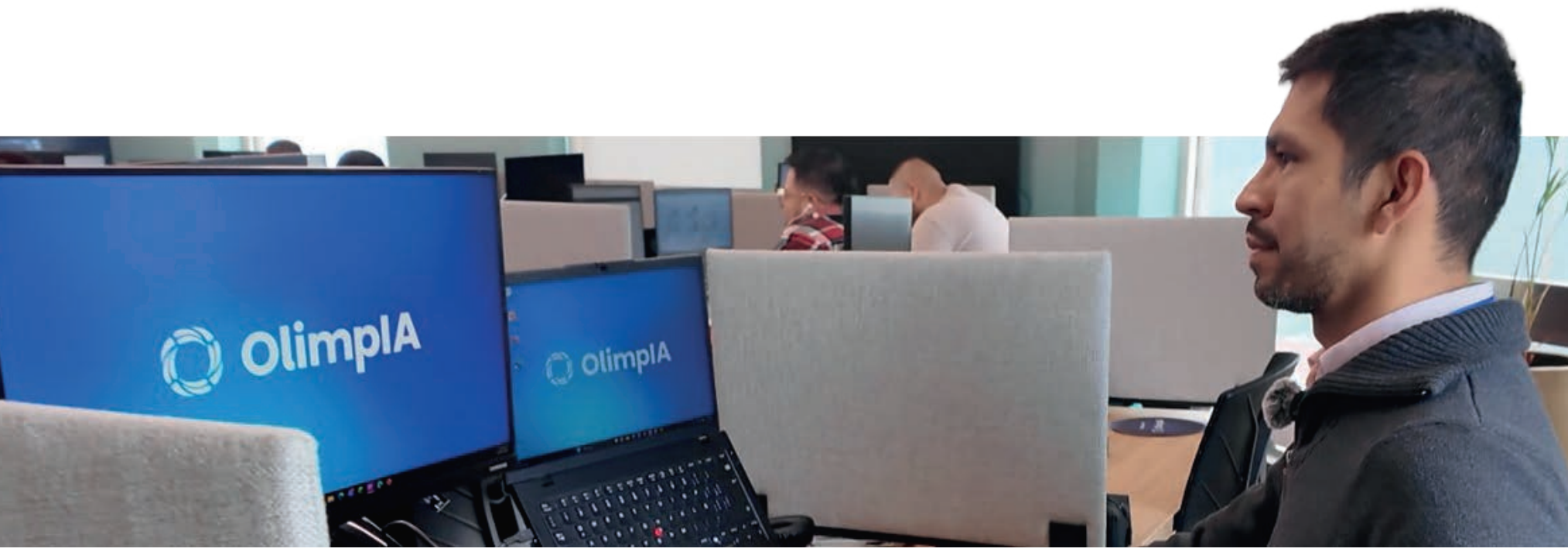
- Gestionar **alertas y ataques** cada vez más sofisticados y automatizados.
- Mantener la capacidad de **monitoreo y respuesta en tiempo real, sin interrupciones.**
- Integrar herramientas de nueva **generación con inteligencia artificial y alta disponibilidad**

El poder de combinar experiencia humana e **inteligencia artificial**

La ciberseguridad moderna no depende únicamente de la tecnología. Las organizaciones más preparadas combinan:

- Inteligencia artificial, que **analiza grandes volúmenes de datos en segundos**
- **Expertos en ciberseguridad,** que interpretan el contexto y toman decisiones estratégicas

La combinación de ambas capacidades permite respuestas más rápidas y precisas, pues la IA identifica patrones y señales de alerta, mientras que **los analistas convierten esa información en acciones que protegen el negocio.**



El SOC de OlimpIA: vigilancia permanente de operaciones críticas

Detrás de cada alerta existe un equipo de especialistas que **analiza información crítica, valida riesgos** y **coordina acciones de respuesta.**

Para fortalecer la protección de nuestros clientes, en OlimpIA contamos con importantes **alianzas con fabricantes globales como:**

CHECK POINT™ CROWDSTRIKE radware IBM®

Este enfoque permite mitigar riesgos como:

- Ransomware.
- Phishing.
- Accesos no autorizados.

Prevén amenazas con **OlimpIA.**

Clic aquí

¿Cómo funciona **la protección en tiempo real?**

Cada día, **el SOC procesa y analiza millones de eventos de seguridad** provenientes de múltiples plataformas tecnológicas.

Cuando se detecta una alerta, los analistas la clasifican, evalúan su criticidad y activan protocolos de respuesta orientados a reducir el riesgo de amenazas como ransomware, phishing o accesos no autorizados.

Contar con un Centro de Operaciones en Seguridad especializado permite:

- **Evita interrupciones críticas** mediante detección temprana.
- **Reduce pérdidas económicas** al acortar tiempos de respuesta.
- Garantiza **continuidad del negocio.**
- **Mejora la visibilidad** sobre riesgos digitales.
- **Protege información** estratégica.
- Incorpora **conocimiento experto** sin ampliar equipos internos.

La **ciberseguridad** deja de ser un costo y se convierte en un habilitador del negocio.

La confianza también se protege

La transformación digital ha convertido la ciberseguridad en un componente esencial para la continuidad y el **crecimiento de las organizaciones.**

Más allá de proteger sistemas, **un SOC protege la confianza y la capacidad de operar** en un entorno cada vez más conectado.

En **OlimpIA,** la ciberseguridad se transforma en inteligencia para anticiparse a los riesgos y proteger lo que realmente importa: la operación de sus clientes.

Organicemos una cita para que visites el SOC más alto del país, ubicado en la Torre Colpatria: