OlimpIA | Sentry

Ciberseguridad en universidades:

¿Cómo **proteger** a tu **institución** en el **siglo XXI?**

¿SABÍAS QUE...?

El **80% de las universidades en el mundo** ha enfrentado incidentes de ciberseguridad en los últimos tres años.

Fuente: Educause Cybersecurity Report 2024.

La universidad del siglo XXI funciona como una auténtica ciudad digital.

Miles de estudiantes acceden a plataformas académicas,

docentes cargan información de alto valor, administrativos gestionan pagos y matrículas en línea, mientras investigadores comparten hallazgos con impacto global. A esto se le suma la diversidad de dispositivos conectados a la red universitaria: laptops, tablets, teléfonos e incluso equipos de laboratorio con acceso a internet.

Este ecosistema académico, tan dinámico como diverso,

se convierte en una superficie de ataque amplia que los ciberdelincuentes buscan aprovechar. Desde el robo de credenciales hasta ataques masivos de ransomware, las amenazas digitales a las universidades son cada vez más frecuentes y sofisticadas.

Por eso, la **ciberseguridad en educación superior** no es solo un requisito técnico: **es una responsabilidad institucional** que garantiza la confianza de la comunidad académica, protege la reputación y asegura la continuidad de la misión educativa e investigativa.

Principales amenazas en universidades

Por su naturaleza resulta un ecosistema atractivo para los ciberatacantes que buscan información valiosa como datos personales. A continuación, te presentamos las principales amenazas que hoy enfrentan las instituciones de educación superior:

Ransomware

Consiste en un software malicioso que cifra la información de los servidores y exige un pago, generalmente en criptomonedas, para devolver el acceso. En las universidades, este tipo de ataque puede paralizar desde sistemas de matrícula y calificaciones hasta plataformas de investigación. De igual manera, interrumpe la operación académica e incluso afecta la reputación institucional frente a estudiantes y aliados nacionales e internacionales. La prevención con respaldos seguros, actualizaciones constantes y segmentación de redes es esencial para reducir el riesgo.

Phishing

Es una de las amenazas más frecuentes en el ámbito universitario. Consiste en **correos o mensajes que simulan provenir de áreas oficiales de la institución,** como la oficina de registro o el departamento financiero, para engañar a estudiantes o docentes y robar sus credenciales. Estos accesos fraudulentos pueden derivar en robo de identidad, acceso a expedientes académicos o suplantación de personal directivo. La educación digital e implementación de filtros inteligentes son herramientas clave para detener este riesgo.

Ingeniería social

Utiliza la persuasión y manipulación psicológica para convencer a los usuarios de entregar información confidencial o ejecutar acciones que abran las puertas a intrusos.
Por ejemplo, un atacante puede hacerse pasar por personal de soporte para pedir contraseñas o simular ser un profesor que solicita acceso urgente a un sistema. Las campañas de concienciación y simulacros prácticos fortalecen la capacidad de respuesta de la comunidad universitaria.

Fuga de datos

Las universidades gestionan información de alto valor, como expedientes académicos, datos financieros, investigaciones científicas y proyectos con impacto internacional. Una fuga de datos por ataque externo o descuido interno expone la información a usos indebidos.
En conjunto, estas amenazas representan un reto para las instituciones de universidades, pero también una oportunidad para **fortalecer su infraestructura digital y posicionarse como referentes en protección del conocimiento.**

TE PUEDE INTERESAR:

Conoce las principales modalidades de ciberataques en Colombia

Casos reales de ataques en universidades colombianas y aprendizajes clave

Fortalecer la seguridad digital **es un proceso continuo que mejora cuando se aprende de experiencias concretas.** Estos casos reales, conocidos a vox populi, reflejan cómo instituciones del país han enfrentado con éxito incidentes cibernéticos y fortalecido su resiliencia:

Universidad El Bosque

En junio de 2021, la Universidad El Bosque sufrió un ciberataque que comprometió plataformas académicas, correos institucionales y hasta su perfil oficial de Twitter. Algunos estudiantes compartieron que recibieron comunicaciones falsas simulando cancelaciones de clases o eliminación de información académica.

A los pocos días, la universidad logró recuperar el control gracias a su infraestructura informática de primer nivel y al trabajo del personal especializado.

Fuente: Diario El País, 2021.

Aprendizajes contundentes

Desarrollo de infraestructura informática robusta.

Importancia del personal técnico especializado y de protocolos forenses confiables.

Universidad Nacional de Colombia

En marzo de 2023, la institución detectó un ataque de ransomware que impactó su infraestructura informática, principalmente los servidores que soportaban servicios académicos, administrativos y de pago. Para contener la amenaza, la universidad aisló los sistemas afectados, asegurando que no entrara ni saliera información. Aunque la operación informática seguía en proceso de recuperación, no se registraron fugas de datos sensibles. También se fortalecieron cortafuegos, antivirus y se inició el desarrollo de un Centro de Operaciones de Seguridad (SOC).

Fuente: Revista Semana, 2023.

Aprendizajes contundentes

Contención inmediata y aislamiento efectivo de los sistemas.

Proyección clara hacia un centro que monitoree continuamente la seguridad digital.

Checklist

de **señales** de que tu universidad necesita **reforzar** **la seguridad**

¿Te identificas con algunas de estas?

- [ ] **Dependencia de contraseñas simples o repetidas.**
- [ ] **Copias de seguridad poco frecuentes o sin verificación.**
- [ ] **Procesos de acceso con baja trazabilidad.**
- [ ] **Políticas de ciberseguridad poco claras o desactualizadas.**
- [ ] **Ausencia de simulacros de ataque o pruebas de respuesta.**

Identificar estas señales a tiempo **permite tomar decisiones estratégicas y fortalecer la seguridad** antes de enfrentarse a incidentes graves.

DATOS QUE DEBES CONOCER

El Global Threat Report 2025 de CrowdStrike destaca que **el sector educativo colombiano se encuentra entre los 10 más atacados del mundo.**

Durante 2024, los tiempos de compromiso (intervalo de tiempo que transcurre desde el inicio de un ciberataque hasta que se detecta y se toman medidas) bajaron de 62 a apenas 48 minutos; en algunos casos, solo fueron unos segundos, gracias al uso de inteligencia artificial y tácticas automatizadas como phishing dirigido.

Infraestructura crítica
de una universidad en el siglo XXI

No se limita a servidores físicos, abarca todos los sistemas que sostienen la vida académica y administrativa. Entre los más estratégicos están:

Plataformas de matrícula y calificaciones:
El corazón del proceso académico.

Sistemas de e-learning:
Esenciales en modelos híbridos y virtuales.

Correo institucional y herramientas de colaboración:
Canales oficiales de comunicación.

Bases de datos de investigación y patentes:
Información de alto valor científico y económico.

Redes de conectividad WiFi:
Miles de dispositivos conectados en simultáneo.

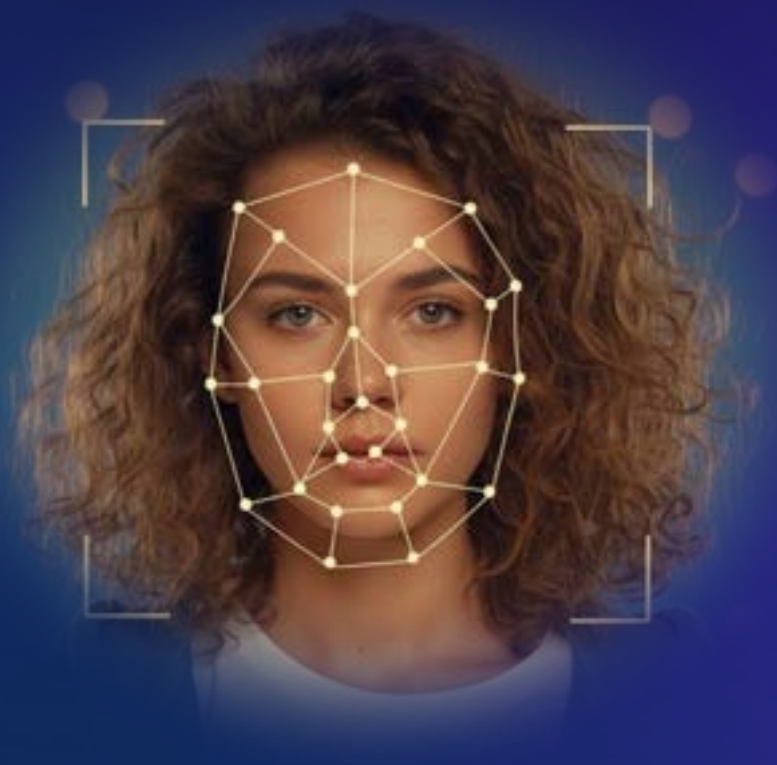
Cada componente **requiere un plan de seguridad integral** que asegure **disponibilidad, confidencialidad y trazabilidad de la información.**

¿Cómo **OlimpIA ayuda a las universidades a avanzar** hacia un modelo integral de **seguridad digital?**

La ciberseguridad moderna en las universidades debe integrar tecnología, procesos y cultura. Por eso, acompañamos a las instituciones de educación superior a través de **OlimpIA Sentry,** un portafolio integral de ciberseguridad diseñado para fortalecer cada capa de protección digital:

Validamos la identidad digital de manera **confiable,**

garantizando que cada usuario sea quien dice ser. Implementamos biometría facial y dactilar, impulsadas con inteligencia artificial para prevenir intentos de suplantación.



Aplicamos autenticación **multifactor** (MFA)

para reforzar la seguridad más allá de las contraseñas. Nuestras soluciones blindan accesos críticos y disminuyen los riesgos de intrusión.

Monitoreamos en **tiempo real**

para detectar anomalías antes de que escalen a incidentes graves. Nuestro CyberSOC 24/7 ofrece alertas tempranas, análisis continuo y respuesta inmediata ante amenazas.

Protegemos dispositivos y endpoints

mediante políticas de acceso seguro. Cada computador, tablet o servidor universitario se mantiene dentro de un perímetro digital confiable.

Formamos a la comunidad universitaria en ciberseguridad,

desde estudiantes hasta profesores y administrativos. Así promovemos una cultura digital en la que cada actor es parte activa de la defensa institucional.

Anticipamos amenazas a través de **modelos predictivos** y estrategias

de cacería avanzada. Esto permite identificar riesgos incluso antes de que se materialicen.

Supervisamos activos digitales

desde estudiantes hasta profesores y administrativos. Así promovemos una cultura digital en la que cada actor es parte activa de la defensa institucional.

Consolidamos una **estrategia** de ConflAnza Digital

adaptada al core de cada institución educativa. Este enfoque asegura continuidad académica y fortalece la reputación de la universidad en el entorno digital.

Hacia una U segura, innovadora y confiable

La universidad del siglo XXI debe proteger el conocimiento, impulsar la innovación y construir ConfIAnza Digital.

En OlimpIA sabemos que la ciberseguridad es el pilar que respalda la continuidad académica y la reputación institucional. Nuestras soluciones en ciberseguridad están diseñadas para que las instituciones de educación superior avancen en su transformación digital.

Conoce más sobre

OlimpIA | Sentry