

El **Mundial 2026** también se juega en el **terreno** **digital.**

Los ataques contra
organizaciones
deportivas **crecieron**
112% en los últimos
años.

Así se protege uno de
los **eventos más**
importantes del
planeta frente a las
amenazas digitales.

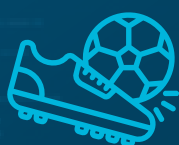


La competencia que **millones no ven.**

Mientras millones de personas siguen cada partido, otra competencia se desarrolla de forma paralela fuera de las canchas: **la lucha por proteger la infraestructura digital que hace posible el torneo.**



De acuerdo con datos de **Surfshark**, los ataques dirigidos a organizaciones deportivas **crecieron un 112%** en los últimos años.



Mientras que el fútbol concentra el **52% de los incidentes de seguridad** registrados en el sector.

La magnitud tecnológica de un Mundial convierte a la **ciberseguridad** en un componente tan importante como **la logística, las comunicaciones o la organización deportiva.**



Un **ecosistema digital** bajo presión.

Un Mundial no solo reúne **selecciones** y **aficionados**. También conecta:

- Plataformas de **streaming**.
- Sistemas de **venta de entradas**.
- Patrocinadores.
- **Operadores** tecnológicos.
- Casas de **apuestas**.
- Millones de **usuarios interactuando en tiempo real**.

Este ecosistema **mueve enormes volúmenes de información y transacciones**, convirtiéndose en un objetivo atractivo para **ciberdelincuentes** que buscan obtener **beneficios económicos**, generar **afectaciones operativas** o comprometer **información sensible**.





Las **amenazas** que juegan **fuera** de la cancha.

Entre los **riesgos con mayor potencial** de impacto durante una **competición de alcance global** se encuentran:



Ataques DDoS contra plataformas de transmisión y venta de entradas.



Campañas de phishing que suplantán marcas oficiales.



Secuestro de sistemas mediante **ransomware**.



Espionaje digital para obtener información estratégica.



Fraudes relacionados con **apuestas deportivas y promociones falsas**.



Compromiso de cuentas corporativas y redes sociales.

La **sofisticación de estas amenazas** exige capacidades de detección y respuesta cada vez más avanzadas. Por eso, **la verificación de canales oficiales** y el uso de mecanismos de autenticación fortalecidos continúan siendo algunas de las medidas **más efectivas para reducir estos riesgos**.



La **inteligencia artificial** cambia las reglas del juego.

La **inteligencia artificial** se ha convertido en una de las principales herramientas para fortalecer la **seguridad digital**.

Su capacidad para **analizar grandes volúmenes de información en tiempo real** permite identificar **patrones sospechosos, anticipar amenazas y automatizar respuestas** ante posibles incidentes.

Gracias a estas capacidades, organizaciones de diferentes sectores pueden **mejorar significativamente** sus tiempos de **detección y reacción** frente a **riesgos digitales**.





Proteger información también es proteger resultados.

El impacto de un **ciberataque** no se limita a la **infraestructura tecnológica**.

Información médica de jugadores, **análisis de rendimiento**, estrategias deportivas, **sistemas de comunicación**, acreditaciones y **operaciones logísticas** forman parte de los activos que requieren **protección permanente** durante una competición global.

Según el **National Cyber Security Centre (NCSC)**, hasta el **70%** de las organizaciones deportivas sufren al menos un ciberataque al año, lo que demuestra la **importancia de proteger información crítica** para preservar la integridad de la competencia.





Lo que la **Copa del Mundo le enseña** a las organizaciones.

Los **desafíos de ciberseguridad** que enfrenta un Mundial son similares a los que enfrentan diariamente **empresas, entidades públicas y organizaciones** de múltiples sectores.

La principal lección es clara: la ciberseguridad debe abordarse como una estrategia integral que combine **tecnología, inteligencia de amenazas, monitoreo permanente y educación digital.**

La prevención sigue siendo la mejor herramienta para **reducir riesgos.**



¡Qué **no metan** un gol! Defiende con **ciberseguridad**.

La **transformación digital** ha ampliado las oportunidades de **conexión, innovación y crecimiento**, pero también ha incrementado la **exposición a nuevas amenazas**.

El **Mundial 2026** demuestra que la capacidad para **anticipar** riesgos, **proteger** información y **responder** oportunamente se ha convertido en un factor determinante para cualquier organización.

En **Olimpia**, la **ciberseguridad** se entiende como un habilitador de confianza digital que permite **proteger operaciones, usuarios e información** en un entorno cada vez más conectado.

Más información:

www.olimpiait.com



Olimpia | Sentry

