ayesa

Ciberseguridad 2025

Predicciones y tendencias clave

ayesa.com

Ciberseguridad 2025:
Predicciones y tendencias clave

Escenario complejo y en evolución

La ciberseguridad en 2025 se presenta como un ámbito crítico y dinámico, marcado por la rápida evolución de las amenazas y la complejidad de las estrategias de defensa. A medida que la tecnología sigue avanzando a un ritmo sin precedentes, las organizaciones enfrentan un entorno digital más interconectado, pero también más vulnerable. Los ciberdelincuentes, impulsados por la innovación tecnológica, están llevando sus tácticas a un nuevo nivel de sofisticación, aprovechando herramientas avanzadas que desafían las capacidades de las soluciones de seguridad tradicionales.

La transformación digital, acelerada por la adopción masiva de tecnologías como la nube, el Internet de las Cosas (IoT) y los sistemas híbridos, ha ampliado significativamente la superficie de ataque. Las empresas y organismos públicos se encuentran ahora ante el desafío de gestionar infraestructuras distribuidas y complejas que, aunque ofrecen grandes beneficios operativos, también exponen puntos débiles que pueden ser explotados. La seguridad ya no se limita a proteger perímetros definidos; ahora abarca una red global de interacciones, accesos remotos y ecosistemas compartidos.

En este escenario, los ciberdelincuentes no solo aprovechan vulnerabilidades técnicas, sino que también recurren a técnicas más elaboradas de ingeniería social para explotar el factor humano. Esto subraya la importancia de una estrategia de seguridad integral que combine tecnología avanzada con educación y concienciación dentro de las organizaciones. La innovación por sí sola no es suficiente; se necesita un enfoque holístico que considere a las personas, los procesos y las tecnologías como un todo interdependiente.

Además, la naturaleza global de las amenazas actuales ha evidenciado la necesidad de una colaboración más estrecha entre sectores, gobiernos y regiones. La ciberseguridad ya no puede ser vista como una responsabilidad aislada de las empresas; se ha convertido en un esfuerzo colectivo que requiere compartir información, experiencias y mejores prácticas. Este enfoque colaborativo será esencial para anticipar amenazas emergentes y responder eficazmente a incidentes en un entorno cada vez más interconectado.

La resiliencia también cobra una importancia creciente en el panorama de la ciberseguridad. No se trata solo de prevenir ataques, sino de estar preparados para responder y recuperarse rápidamente ante cualquier interrupción. Las organizaciones deben desarrollar capacidades robustas de continuidad del negocio que les permitan mitigar el impacto de los incidentes y garantizar la operatividad en todo momento. Esto incluye desde la planificación de contingencias hasta la implementación de simulacros regulares que fortalezcan su capacidad de respuesta.

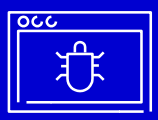
En definitiva, el 2025 marcará un punto de inflexión para la ciberseguridad, donde la combinación de innovación tecnológica, formación continua y colaboración estratégica determinará el éxito de las organizaciones en su esfuerzo por proteger activos críticos y construir un entorno digital más seguro. Adaptarse a este escenario complejo y en constante cambio no será una opción, sino una necesidad para garantizar la sostenibilidad y competitividad en un mundo digital.

Proliferación de ataques impulsados por inteligencia artificial (IA)

La inteligencia artificial se ha convertido en una herramienta fundamental tanto para mejorar las defensas cibernéticas como para desarrollar ciberataques más sofisticados. En 2025, veremos una aceleración en el uso de IA por parte de los ciberdelincuentes, quienes la utilizarán para:

Automatizar ataques de phishing a gran escala

personalizando mensajes en tiempo real basándose en datos robados.



Diseñar malware adaptable

que aprende y evoluciona para evadir los sistemas de detección tradicionales.

Llevar a cabo análisis masivos de datos

identificando patrones y puntos vulnerables en redes complejas.

Por otro lado, las organizaciones recurrirán a la IA para fortalecer sus sistemas de seguridad, implementando soluciones que analicen anomalías en tiempo real, anticipen posibles amenazas y refuercen su capacidad de respuesta ante incidentes. Sin embargo, la carrera entre defensores y atacantes será un campo de batalla dinámico, donde los ciberdelincuentes seguirán intentando superar las medidas más avanzadas.

La IA no solo está cambiando las reglas del juego en términos de velocidad y precisión de los ataques, sino también en la capacidad de los atacantes para personalizar campañas específicas basadas en análisis de comportamiento. Además, los ciberdelincuentes están empezando a utilizar sistemas generativos como deep learning para crear engaños más convincentes, como imágenes, textos o voces simuladas. Para contrarrestar esta amenaza, las organizaciones deberán invertir en sistemas de detección basados en inteligencia artificial que sean capaces de analizar patrones y prever movimientos del atacante.

Evolución del ransomware y amenazas a la cadena de suministro

El ransomware continuará evolucionando como una de las amenazas más devastadoras. En 2025, se espera que los ciberdelincuentes dirijan sus ataques hacia cadenas de suministro críticas, utilizando técnicas cada vez más avanzadas para interrumpir operaciones esenciales. Los nuevos enfoques incluirán:

Uso de 'ransomware como servicio' (RaaS)

democratizando el acceso a herramientas de ataque para delincuentes sin experiencia.

Implementación de deepfakes

para manipular identidades y obtener acceso a sistemas restringidos.

Campañas dirigidas a proveedores de software y hardware

para introducir vulnerabilidades en sus productos.

La importancia de proteger la cadena de suministro será fundamental, ya que un solo punto de falla podría desencadenar consecuencias catastróficas en múltiples sectores, incluyendo el financiero, energético y sanitario.

La profesionalización del ransomware, combinada con la falta de preparación de las pequeñas y medianas empresas, expone aún más las cadenas de suministro críticas. Los ataques dirigidos a los proveedores menores pueden desencadenar una reacción en cadena con consecuencias globales. Además, la digitalización acelerada está creando nuevas dependencias tecnológicas, lo que subraya la necesidad de implementar estrategias de segmentación de redes y controles de acceso estrictos para minimizar riesgos.

Crecimiento de vulnerabilidades en entornos de nube y dispositivos IoT

La adopción masiva de servicios en la nube y dispositivos de Internet de las Cosas (IoT) seguirá expandiendo la superficie de ataque. Los ciberdelincuentes se enfocarán en explotar configuraciones mal gestionadas, credenciales débiles y falta de actualizaciones. En este contexto, se prevén varios retos:

La complejidad de gestionar infraestructuras híbridas

que combinan soluciones locales y en la nube.

El aumento de ataques dirigidos a dispositivos IoT

utilizados en sectores críticos como la salud y la manufactura.

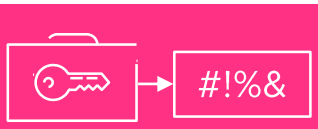
La necesidad de implantar soluciones de seguridad específicas

para entornos multinube.

Además de los riesgos de configuración, la proliferación de dispositivos IoT no seguros está creando una red de puntos vulnerables que los ciberdelincuentes pueden explotar. Muchos dispositivos carecen de estándares de seguridad robustos, lo que aumenta las posibilidades de acceso no autorizado. Las organizaciones deben priorizar herramientas de monitorización que analicen constantemente los comportamientos de red en busca de irregularidades y actualizaciones frecuentes para mitigar estos riesgos.

Amenazas emergentes de la computación cuántica

Aunque la computación cuántica aún está en una etapa inicial, su potencial para romper los métodos de cifrado actuales representa una preocupación significativa. En 2025, se anticipa un mayor enfoque en:



Desarrollo de algoritmos criptográficos

resistentes a la computación cuántica.

Actualización de protocolos de seguridad

en sectores como la banca, el comercio electrónico y las telecomunicaciones.

Aumento de la inversión en investigación

para prever los riesgos asociados con esta tecnología.

La computación cuántica también plantea desafíos en términos de infraestructura, ya que las organizaciones deben adaptar sus sistemas a tecnologías aún en evolución. Este cambio implicará costos significativos en actualizaciones y formación técnica. Los gobiernos y entidades privadas deberán colaborar en estándares globales para garantizar que las soluciones cuántico-resistentes sean adoptadas de manera uniforme y eficaz.

Escasez de talento en ciberseguridad

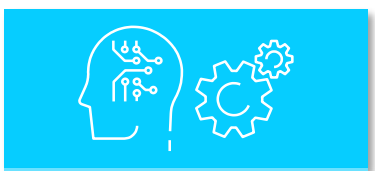
La brecha entre la demanda de expertos en ciberseguridad y la oferta disponible seguirá siendo un desafío en 2025. Esta situación impactará directamente en la capacidad de las organizaciones para implementar medidas de seguridad efectivas. Algunas estrategias clave para abordar esta problemática incluyen:

Invertir en programas de formación y certificación

especializados en ciberseguridad.

Fomentar alianzas público-privadas

para desarrollar talento local en mercados emergentes.



Incorporar inteligencia artificial y automatización

para cubrir parcialmente la falta de personal especializado.

La escasez de talento no solo afecta a la respuesta inmediata ante incidentes, sino también a la capacidad de innovación en ciberseguridad. Las empresas deberán considerar la formación interna de personal no técnico para cubrir ciertas funciones. Además, la diversidad y la inclusión en los programas de formación podrían ampliar la base de profesionales, atrayendo a talentos de distintas disciplinas para abordar los desafíos de manera creativa.

Regulaciones más estrictas y énfasis en la ciberresiliencia

La creciente presión de los gobiernos y organismos internacionales para fortalecer la ciberseguridad llevará a la adopción de regulaciones más estrictas. En particular, normativas como la Directiva NIS2 en Europa impulsarán un enfoque más riguroso en:

La gestión de riesgos cibernéticos

como parte esencial de la gobernanza corporativa.

La implementación de marcos de ciberresiliencia

que aseguren la continuidad operativa incluso en caso de ataques severos.

La transparencia en la notificación de incidentes

fomentando un enfoque más colaborativo entre sectores.

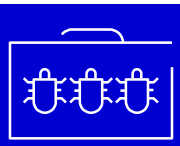
Estas normativas no solo establecen estándares mínimos de seguridad, sino que también obligan a las empresas a redefinir sus prioridades estratégicas en torno a la protección de datos. Además, el cumplimiento de estas regulaciones se está convirtiendo en un diferenciador competitivo, ya que los clientes y socios comerciales prefieren trabajar con organizaciones que demuestren un compromiso sólido con la ciberseguridad. Los costos asociados a la no conformidad, como multas y pérdida de reputación, subrayan aún más la importancia de integrar la ciberresiliencia en todos los niveles de la organización.

Automatización y profesionalización del cibercrimen

El cibercrimen está evolucionando hacia un modelo de negocio altamente organizado, con grupos especializados que ofrecen servicios en cada etapa del ciclo de ataque. Esta profesionalización incluye:

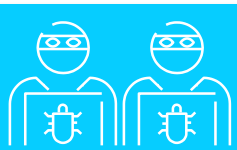
El uso de herramientas automatizadas

que aumentan la velocidad y la precisión de los ataques.



La venta de kits de explotación en mercados clandestinos

facilitando el acceso al cibercrimen para actores menos experimentados.



La colaboración entre grupos criminales

para maximizar la eficacia de sus operaciones.

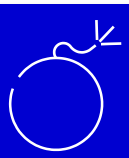
La automatización está permitiendo que los ciberdelincuentes reduzcan los costos operativos y aumenten la frecuencia de sus ataques. Por otro lado, la creación de redes clandestinas bien organizadas, que operan como auténticas empresas, está facilitando el desarrollo de amenazas personalizadas para objetivos específicos. Este modelo plantea retos adicionales para las organizaciones, que deben adaptar sus defensas para contrarrestar tanto a atacantes individuales como a operaciones criminales altamente estructuradas.

Integración de amenazas físicas y digitales

La convergencia entre las amenazas físicas y digitales será una realidad en 2025. Ejemplos de esto incluyen:

Ataques combinados

que interrumpen tanto sistemas informáticos como infraestructuras físicas.



El uso de tácticas de intimidación física

para extorsionar a empresas comprometidas digitalmente.

La necesidad de estrategias de defensa integradas

que aborden ambos tipos de amenazas.

La digitalización de infraestructuras críticas, como la energía y el transporte, las convierte en objetivos de alto valor. Los ataques híbridos, que combinan ciberataques con sabotajes físicos, pueden causar interrupciones masivas y prolongadas. Además, el espionaje industrial está aumentando, donde los adversarios combinan infiltración física y digital para extraer información sensible. En este contexto, la integración de estrategias de defensa física y cibernética será clave para garantizar la seguridad general.

Riesgos asociados al uso indebido de la IA

La rápida adopción de herramientas de IA en procesos empresariales conlleva riesgos, incluyendo:

La exposición accidental de datos sensibles

a través de plataformas mal configuradas.

La dependencia excesiva de soluciones automatizadas

que podrían ser manipuladas por atacantes.

La necesidad de marcos éticos y de gobernanza claros

para garantizar un uso seguro y responsable de estas tecnologías.

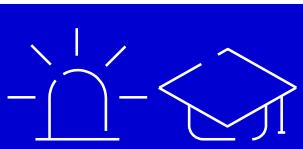
La falta de controles efectivos sobre la IA también plantea riesgos regulatorios y éticos, especialmente en sectores donde la toma de decisiones automatizada puede afectar a los consumidores. Por ejemplo, los errores en la IA utilizada para procesos financieros o de salud pueden generar consecuencias graves. Las empresas deben priorizar la implementación de auditorías de IA y establecer políticas claras para gestionar y supervisar estas tecnologías.

Prioridad en estrategias de seguridad proactivas

En lugar de limitarse a reaccionar ante incidentes, las organizaciones deberán adoptar enfoques proactivos, como:

Implementación de arquitecturas de confianza cero

para minimizar riesgos.



Inversiones en simulaciones de ciberataques y formación

para los empleados.

Uso de inteligencia de amenazas

para anticipar posibles vulnerabilidades.

Las estrategias proactivas no solo mejoran la capacidad de respuesta ante amenazas, sino que también reducen significativamente los costos asociados a los incidentes de seguridad. Además, las simulaciones avanzadas, como los ejercicios de red teaming, permiten a las empresas identificar debilidades internas antes de que los atacantes las exploten. La inversión en análisis predictivo y en colaboración con equipos especializados externos será fundamental para mantener una postura de seguridad sólida.

Ciberseguridad 2025:
Conclusión

El año 2025 se perfila como un periodo crucial para la ciberseguridad, donde las amenazas serán más sofisticadas y persistentes que nunca. La clave para superar estos desafíos será una combinación de innovación tecnológica, inversión en talento humano y colaboración entre sectores para construir un ecosistema digital más seguro.

Para garantizar su competitividad, las organizaciones deberán integrar la ciberseguridad en el núcleo de sus estrategias empresariales. Esto implica no solo implementar soluciones técnicas avanzadas, sino también fomentar una cultura de seguridad en todos los niveles de la organización. La capacitación continua de los profesionales, combinada con la sensibilización sobre las amenazas emergentes, será esencial para fortalecer los eslabones más débiles de la cadena de seguridad.

Además, la colaboración entre sectores público y privado jugará un papel fundamental en la detección y mitigación de amenazas. Las iniciativas conjuntas para compartir información sobre incidentes y mejores prácticas permitirán a las empresas adelantarse a los ataques. Paralelamente, los gobiernos deben adoptar un papel más activo, promoviendo regulaciones claras y fomentando la inversión en ciberdefensa.

En última instancia, la ciberresiliencia será el factor diferenciador entre las organizaciones que prosperen en el panorama digital de 2025 y aquellas que queden rezagadas. Más allá de prevenir ataques, las empresas deben ser capaces de recuperarse rápidamente, minimizando el impacto en sus operaciones y su reputación. Este enfoque holístico garantizará no solo la protección de los activos, sino también la confianza de los clientes y socios, consolidando su posición como líderes en un mundo cada vez más digital y conectado.

Nuestros servicios de Ciberseguridad 360º

INTEGRACIÓN DE SOLUCIONES DE CIBERSEGURIDAD IT/OT

CiD360

- Consultoría de adaptación e implantación
- Mejora la ciber resiliencia
- Servicios de Seguridad Gestionada (SOC)
- Protección a Sistemas de Control Industrial (ICS)
- Formación especializada a medida

SDLC-CIBERSEC (DESARROLLO SEGURO DEL SOFTWARE)

Autor

Álvaro Fraile
Global Cybersecurity Services Director

Fundada en 1966, Ayesa es una compañía global de servicios de tecnología e ingeniería, con 13.200 empleados y presencia directa en 23 países de Europa, América, África y Asia. Liderada por José Luis Manzanares, supera los 717 millones de euros de cifra de negocio, consolidándose como una de las principales empresas de consultoría y servicios TI en el mercado español.

Ofrece un amplio abanico de soluciones avanzadas de Transformación Digital (proyectos con tecnologías y soluciones disruptivas) y líneas de servicio core (servicios TI tradicionales) para mejorar la competitividad en todos los sectores de actividad mediante la aplicación de tecnología y conocimiento.

Industria 4.0, Analytics, Cloud, Hybrid IT, Ciberseguridad, Computación Cuántica, Blockchain, IoT, IA, RPA, Bimodal IT, Movilidad o Digital Experience son algunas de las tecnologías que pone a disposición de sus clientes para afrontar la nueva era digital.

También figura entre las ingenierías de referencia, trabajando por construir un mundo más eficiente y justo, aplicando la ingeniería y la tecnología de vanguardia de manera integrada. Ayuda a empresas, instituciones y organizaciones a convertirse en lo que quieren ser. Trabaja en el espacio que hay entre el ahora y el futuro, aplicando, con el mejor talento, la tecnología más puntera.