Predicciones 2026: Ciberseguridad

La evolución de la ciberdefensa: hacia la confianza dinámica

John Swanson, Director Global del Portfolio de Seguridad, Uvance, Fujitsu

Durante años, las organizaciones han luchado por seguir el ritmo del creciente nivel de complejidad de las amenazas cibernéticas, confiando en defensas reactivas basadas en perímetros que otorgaban acceso y luego asumían confianza. Sin embargo, estamos ante un cambio fundamental: los principios de la Confianza Dinámica se hacen posibles gracias a los avances en inteligencia artificial (IA), la gestión continua de la exposición y la evaluación del riesgo en tiempo real. Estas innovaciones están transformando la manera en que entendemos la ciberseguridad.

Hoy en día, muchas organizaciones presentan zonas ciegas en su seguridad, desplegando tecnologías sin marcos adecuados de gobernanza y con escasa visibilidad sobre dónde se almacena su información o cómo están expuestos sus sistemas. Para 2026, los avances en defensa impulsada por IA, la gestión proactiva del riesgo y la integración entre seguridad de la información (IT) y tecnología operacional (OT) convertirán la ciberseguridad en una prioridad estratégica, dejando de ser una función meramente técnica.

1. La gobernanza de la IA se convertirá en una prioridad a nivel de consejo

La promesa de la IA generativa y agente está superando la capacidad de las organizaciones para gobernarla de forma eficaz, creando una tormenta perfecta de vulnerabilidades. En 2026, esta brecha de gobernanza ya no será tolerable: reguladores, inversores y aseguradoras exigirán rendición de cuentas en el uso de la IA.

Surgirán soluciones de "IA Governance-as-a-Service" y plataformas integradas de cumplimiento normativo para aplicar políticas, supervisar el comportamiento de los modelos y mitigar riesgos como la filtración de datos, los ataques por inyección de *prompts* o los excesivos privilegios de acceso otorgados a sistemas autónomos. Estas plataformas ofrecerán visibilidad continua de los despliegues de IA, los flujos de datos y los procesos de toma de decisiones.

La prisa por implementar IA agente también abrirá la puerta a nuevos vectores de ataque. En 2026 veremos brechas significativas provocadas por inyecciones de *prompts* en fuentes inesperadas, como registros SIEM, DNS o datos de infraestructura que los agentes procesan automáticamente.

La seguridad de la IA dominará las conversaciones en los consejos de administración, impulsada por marcos regulatorios como la Ley de IA de la UE, que exigirán transparencia, trazabilidad y uso ético. Las organizaciones que establezcan marcos sólidos de gobernanza de IA ganarán ventaja competitiva; las rezagadas se enfrentarán a sanciones y daños reputacionales.

2. La soberanía del dato redefinirá la estrategia en la nube

Con el aumento de las tensiones geopolíticas, las organizaciones exigirán mayor transparencia sobre la ubicación y el control de sus datos. El temor a perder información crítica "de un plumazo" transformará la manera de pensar sobre la estrategia en la nube a lo largo de 2026.

Las recientes interrupciones han revelado una realidad preocupante: muchas empresas no saben realmente dónde se encuentran sus datos hasta que una auditoría revela verdades incómodas. Este desconocimiento supone un riesgo inaceptable en una era donde el acceso a la información puede restringirse por decisiones políticas sin margen técnico de respuesta.

Las compañías priorizarán proveedores que garanticen claridad jurisdiccional y resiliencia frente a interferencias políticas. Las estrategias de soberanía multicloud se acelerarán, distribuyendo los datos entre regiones de confianza para reducir riesgos geopolíticos. En los casos más sensibles, las empresas repatriarán cargas críticas a infraestructuras propias cuando las preocupaciones sobre la soberanía de los datos superen las ventajas del cloud.

En consecuencia, las decisiones de compra considerarán la ubicación del dato y la jurisdicción legal tanto como el coste o la capacidad técnica. Los proveedores incapaces de ofrecer respuestas claras sobre la residencia de los datos perderán terreno frente a competidores con garantías de soberanía.

3. La gestión continua de la exposición sustituirá las evaluaciones periódicas

A lo largo de 2026, el paradigma de seguridad pasará de evaluaciones puntuales de vulnerabilidades a una gestión continua de la exposición. Las organizaciones adoptarán plataformas que ofrezcan visibilidad en tiempo real del perímetro de ataque, identificando y priorizando riesgos según su explotabilidad, el contexto del negocio y la inteligencia de amenazas.

Estos sistemas integrarán datos de escáneres de vulnerabilidades, bases de configuración, *feeds* de inteligencia y análisis de impacto empresarial para crear índices de riesgo

dinámicos. A diferencia de las herramientas tradicionales, generarán una visión viva y evolutiva de los riesgos conforme cambian los sistemas, se aplican parches o surgen nuevas amenazas.

El impacto será claro: los equipos de seguridad podrán anticiparse a los ataques y pasar de un modo reactivo a una gestión estratégica del riesgo. Los responsables de ciberseguridad presentarán a los consejos métricas cuantificables sobre la exposición al riesgo, demostrando cómo las inversiones en seguridad protegen el valor empresarial y generan retorno.
Así, la ciberseguridad pasará de ser un centro de costes a un elemento de valor corporativo.

4. La convergencia entre IT y OT se acelerará

En 2026 se diluirá la frontera artificial entre la seguridad IT y la OT, ya que las amenazas no respetan estos límites. Los operadores de infraestructuras críticas alinearán sus controles OT con los estándares IT, implantando visibilidad y gobernanza unificada en ambos entornos.

Los ciberataques patrocinados por Estados y los *hackers* oportunistas seguirán apuntando a infraestructuras críticas, afectando también a objetivos secundarios fuera de zonas de conflicto. El riesgo de daños colaterales por herramientas cibernéticas militarizadas aumentará, como ya ocurrió con Stuxnet en la década de 2010.

Cada vez más organizaciones adoptarán plataformas integradas que ofrezcan una visión única de los riesgos de seguridad en activos IT y OT, aplicando políticas coherentes que respeten las prioridades de disponibilidad y seguridad de los entornos operativos.
Los marcos normativos evolucionarán para exigir esta integración, con estándares como NIS2 convirtiéndose en requisito básico. Las empresas que logren una convergencia madura IT/OT disfrutarán de mejores primas de seguro, ventajas regulatorias y mayor confianza de los clientes.

La transformación de la ciberseguridad en 2026 y más allá

La IA —incluida la generativa y la agente— no resolverá todos los desafíos de inmediato, pero impulsará una evolución decisiva. A partir de 2026, la combinación de defensa impulsada por IA, gobernanza sólida, soberanía del dato, gestión continua de la exposición e integración IT/OT sentará las bases de ecosistemas de ciberseguridad basados en la Confianza Dinámica más que en perímetros estáticos.

Pasaremos de una era en la que las organizaciones solo reaccionaban tras una brecha a otra donde la IA y la monitorización continua permitirán una prevención proactiva. La seguridad dejará de ser un asunto técnico para convertirse en un diferenciador estratégico, con la resiliencia cibernética como nuevo indicador clave del valor corporativo.

Las empresas que combinen capacidades avanzadas de IA con una gobernanza transparente y responsable estarán mejor preparadas para proteger sus activos y mantener la confianza de sus grupos de interés. Las que no lo hagan se enfrentarán a amenazas cada vez más sofisticadas, sanciones regulatorias y pérdida de competitividad.

El futuro de la ciberseguridad consiste en convertir la inteligencia sobre amenazas en estrategias defensivas accionables que protejan el valor del negocio. De cara a 2026, ese futuro nunca ha estado tan cerca.

John Swanson
Global Security Portfolio Lead, Uvance, at Fujitsu

John ha desempeñado diversos cargos de liderazgo en seguridad de la información en los sectores público y privado, incluyendo la dirección de programas y capacidades de seguridad, consultoría estratégica y operativa, Centros de Operaciones de Seguridad (SOC) y funciones de preventa técnica. Actualmente lidera el desarrollo de las **propuestas de ciberseguridad de Fujitsu**, que sustentan su oferta en **Aplicaciones, IT Híbrida, Espacios de Trabajo Digitales e Industria**. Su foco está en **ayudar a los clientes a reforzar la madurez estratégica y operativa** de sus capacidades de seguridad de la información

