LITORALPRESS

Fecha: 30-03-2026
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: El año de la resiliencia ¿Qué demandará de los CISOs el 2026?

Pág. : 38
Cm2: 390,3

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

El año de la resiliencia ¿Qué demandará de los CISOs el 2026?

En 2026, los CISOs eficaces serán aquellos que entiendan la IA no solo como una tecnología, sino como una fuerza que transforma el riesgo, la gobernanza y la continuidad. La resiliencia favorecerá a los líderes que se preparen para la disrupción impulsada por la IA, pongan a prueba sus suposiciones y garanticen que sus organizaciones puedan seguir operando cuando los sistemas automatizados fallen. Esa es la labor del CISO moderno.

Por **Carl Windsor,** Chief Information Security Officer (CISO) en Fortinet.

En "Las predicciones de los CISO para 2026", Fortinet señala las tendencias que están marcando el año que empieza, incluyendo la rápida adopción de la inteligencia artificial (IA) a través de toda la función del negocio, la creciente tensión geopolítica, la presión regulatoria y la continua industrialización del cibercrimen. La conclusión fue clara: la superficie de ataque se está expandiendo más rápido que lo que lo modelos tradicionales de seguridad se pueden adaptar.

Mientras que estas predicciones explican lo que viene, los CISOs tendrán que decidir cómo afrontar estos retos en un ambiente en donde la IA acelera ambos: innovación y riesgo. El límite entre riesgo de TI y riesgo de negocio ha colapsado, acelerado por la integración profunda de IA a las operaciones, toma de decisiones y fidelización del cliente. Los sistemas de IA ahora influencian cadenas de suministro, controles financieros, decisiones de contratación e interacciones con cliente, usualmente con mínima intervención humana.

Como resultado, los CISOs son hoy responsables de asegurar que los procesos de negocio impulsados por IA continúen confiables, disponibles y controlables bajo estrés. En la práctica, los CISOs han empezado a operar como directores de resiliencia.

¿Por qué el 2026 es diferente?

Las discusiones en el Foro Económico Mundial reflejan esta evolución. La IA ha dejado de ser un tema exclusivamente tecnológico para convertirse en un factor de riesgo sistémico, con implicancias en la estabilidad económica, la infraestructura crítica y la confianza institucional. La dependencia de modelos compartidos, la concentración de capacidades tecnológicas y los flujos globales de datos incrementan la exposición a fallas en cascada, obligando a repensar la gobernanza.

En paralelo, las organizaciones están ajustando sus estructuras de decisión. Los CISOs ganan mayor visibilidad en los directorios y participan activamente en la definición de estrategias de adopción de IA, gestión de datos y automatización. La resiliencia ya no es responsabilidad de un área aislada, sino una capacidad transversal que involucra a toda la organización.

A este escenario se suma una presión regulatoria creciente. Normativas asociadas a protección de datos, ciberseguridad e inteligencia artificial comienzan a exigir mayor trazabilidad, explicabilidad y control sobre los sistemas automatizados. Esto obliga a los CISOs a incorporar criterios legales y éticos en la gestión del riesgo, integrando cumplimiento y seguridad en un mismo marco operativo. La resiliencia, por tanto, también se mide en la capacidad de responder ante auditorías, incidentes regulatorios y exigencias de transparencia.

Cinco estrategias que los CISO deben adoptar de cara a 2026

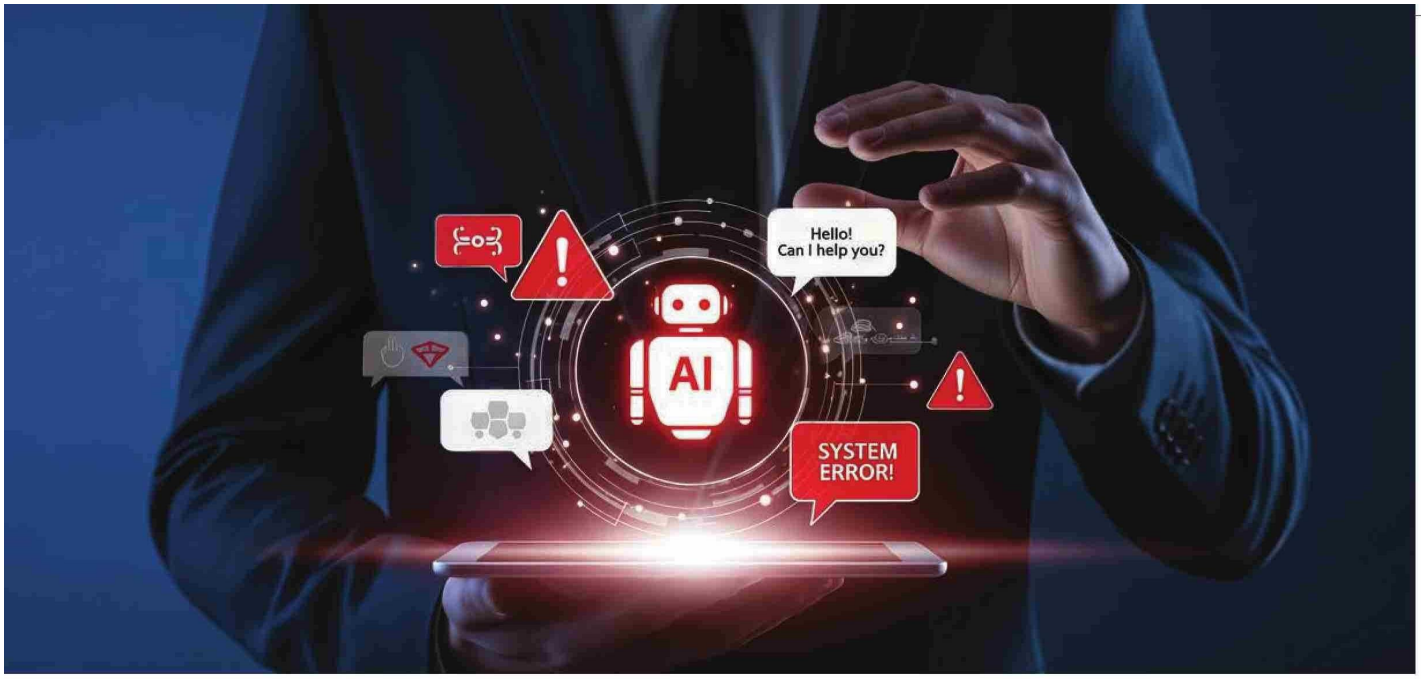
1. Construir para la continuidad de negocio en una empresa impulsada por IA

LITORALPRESS

Fecha: 30-03-2026
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: El año de la resiliencia ¿Qué demandará de los CISOs el 2026?

Pág. : 39
Cm2: 470,6

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida



La disrupción a gran escala no es hipotética. La IA incrementa tanto la posibilidad como el alcance de una falla. Por ello, la planeación de continuidad del negocio deberá evolucionar de acuerdo con ello. Para empezar, los CISO deberán redefinir el Mínimo Viable de Negocio de la organización, tomando en cuenta las dependencias a IA.

La resiliencia en 2026 significa comprender no sólo como los sistemas fallan, sino como la IA amplifica esas fallas. Los planes tradicionales de continuidad, rara vez toman en cuenta el comportamiento de la IA bajo estrés y eso debe cambiar.

2. Tratar a la IA como una capacidad de alto riesgo

La IA está siendo cada vez más integrada en toda la empresa, a menudo fuera de la visibilidad de seguridad tradicional. Los equipos de marketing utilizan herramientas generativas. Los desarrolladores integran modelos externos. Las unidades de negocio implementan la automatización para acelerar las decisiones. Cada uno de estos factores conlleva riesgos.

En 2026, los CISOs deberán tratar la IA como una capacidad de alto riesgo que exige una gobernanza explícita. Esto incluye definir la propiedad, aplicar controles de acceso, proteger los datos de entrenamiento e inferencia, y supervisar el comportamiento de la IA en producción. La IA debe estar sujeta al mismo escrutinio que cualquier sistema capaz de impactar significativamente el negocio.

3. Reforzar controles de identidad para humanos, máquinas y agentes de IA

La identidad se ha convertido en el plano de control de los entornos modernos y la IA está acelerando la complejidad de dichos entornos. No destacaron la identidad no humana como una fuente creciente de riesgo sistémico. Una sola identidad de máquina o agente comprometida puede propagarse por entornos en segundos. Hoy en día, las identidades no humanas ya superan en número a los usuarios humanos en muchas organizaciones. Los agentes de IA añaden una nueva capa al autenticar, consultar sistemas y tomar medidas a gran escala.

En una empresa impulsada por IA, la vulneración de la identidad no es solo un incidente de seguridad, es una falla de resiliencia. Los CISOs deben garantizar que los controles de identidad sean consistentes entre usuarios, máquinas, APIs y agentes de IA, con verificación continua y aplicación de privilegios mínimos. Al mismo tiempo, la gobernanza de la identidad también debe asumir la automatización, escalabilidad y velocidad.

4. Reforzar la colaboración al tiempo que la IA borra los límites tradicionales

La IA disuelve las fronteras organizacionales tradicionales. Las decisiones que antes tomaban las personas ahora se distribuyen entre sistemas, equipos y flujos de trabajo automatizados. Durante los incidentes, esta complejidad puede ralentizar la respuesta si las funciones y responsabilidades no están claras.

Ninguna organización puede desarrollar resiliencia ante la IA de forma aislada. En cambio, la resiliencia depende de la colaboración. Para lograrlo, los CISOs deben alinear los liderazgos de seguridad, TI, ciencia de datos, legal, riesgo y ejecutivo con supuestos compartidos sobre los riesgos y la respuesta ante la IA. Y externamente, la colaboración con colegas, socios y organizaciones del sector público se vuelve aún más crucial a medida que las amenazas impulsadas por la IA se expanden globalmente.

5. Asumir la disrupción acelerada por IA y mantenerse adaptativo

La IA acorta los plazos. Los atacantes se adaptan más rápido. Los errores se propagan con mayor rapidez. Las expectativas regulatorias evolucionan con mayor rapidez. En este entorno, la mentalidad adecuada prioriza las pruebas continuas, la reevaluación periódica de los casos de uso de la IA y la rápida retroalimentación entre los equipos de seguridad y de negocio. Las organizaciones resilientes consideran la adaptación como una disciplina continua, no como una revisión anual. ChN