

Número 119 | Octubre 2026



Radar

El magazine de
ciberseguridad

Anticiparse también es gobernar

Por Diego Javier Rocha Rodríguez

Durante años, la gestión del riesgo se ha apoyado en una lógica conocida: identificar, evaluar, establecer controles y revisar periódicamente. Ese modelo sigue siendo necesario, pero el entorno en el que operan hoy las organizaciones está cambiando a una velocidad que obliga a evolucionar también la forma en la que gobernamos.

La inteligencia artificial es quizá el ejemplo más evidente. Su incorporación a procesos, decisiones, datos y sistemas está generando nuevas oportunidades de transformación, pero también modifica continuamente la exposición de las organizaciones. El riesgo ya no cambia únicamente cuando ocurre un incidente o aparece una nueva regulación. Puede cambiar con una integración, un nuevo modelo, un proveedor, una decisión automatizada o un nivel diferente de autonomía.

En este contexto, gobernar de forma proactiva significa reducir la distancia entre el momento en que el riesgo cambia y el momento en que somos capaces de identificarlo y actuar.

Eso requiere evolucionar desde fotografías periódicas del riesgo hacia una visión más dinámica. Conectar información procedente de activos, datos, identidades, proveedores, vulnerabilidades e incidentes; detectar señales tempranas; entender dependencias y utilizar ese contexto para priorizar decisiones antes de que una exposición se convierta en impacto.

Pero disponer de más información y mayor capacidad de anticipación introduce otra cuestión fundamental: ¿podemos confiar en la inteligencia que utilizamos para decidir?

A medida que la IA pasa de recomendar a ejecutar acciones, la confianza deja de ser una declaración de principios. Debe poder diseñarse, supervisarse y demostrarse. Necesitamos comprender cómo se llega a una decisión, verificar la información que la sustenta, establecer límites claros y mantener mecanismos que permitan cuestionar, corregir o revertir una acción cuando sea necesario.

En esta edición de RADAR, dedicada a Proactive Governance & Risk Management, abordamos estas dos caras de una misma evolución. En “IA y riesgo corporativo: de la evaluación periódica a un radar continuo”, exploramos cómo observar el riesgo de forma más continua, correlacionar señales y anticipar cambios en la exposición. En “Intelligence we trust: la confianza como nueva frontera de la IA”, ponemos el foco en las condiciones necesarias para que esa inteligencia sea entendible, verificable, controlable y responsable.

Gestionar el riesgo de forma proactiva no consiste en predecir todo lo que puede ocurrir. Consiste en construir la capacidad para ver antes, comprender mejor y decidir a tiempo. Porque en un entorno donde la tecnología evoluciona continuamente, gobernar ya no puede significar únicamente revisar lo que ocurrió. También significa estar preparados para reconocer lo que está por venir.



**Diego Javier Rocha
Rodríguez**

Cybersecurity Expert Engineer

Las puertas de Nanao: gobernar el riesgo antes de que el castillo caiga

Cibercrónica por Juan Pablo Campo Téllez

Una organización no es segura simplemente porque tenga buenas murallas. También necesita saber quién puede abrir las puertas. La gestión del riesgo no debería comenzar cuando ocurre un incidente, sino mucho antes, cuando todavía es posible identificar las condiciones que podrían permitirlo.

En 1576, Uesugi Kenshin, uno de los señores de la guerra más temidos del Japón feudal, dirigió sus fuerzas contra el castillo de Nanao, en la provincia de Noto. Construido sobre el monte Sekidō y diseñado para resistir largos asedios, Nanao representaba exactamente lo que se esperaba de una fortaleza de su época: mantener al enemigo afuera.

Kenshin lo intentó y fracasó. Cuando regresó en 1577, comenzó un nuevo asedio que se prolongaría durante meses. Sin embargo, la batalla más importante ya no estaba ocurriendo frente a sus defensas, sino dentro de ellas. Una epidemia debilitó a sus defensores, aumentaron las tensiones políticas y las disputas internas terminaron fragmentando la estructura que sostenía la fortaleza.

Según los registros históricos recopilados por la ciudad de Nanao, el 15 de septiembre de 1577 Yusa Tsugumitsu y sus aliados se rebelaron y finalmente abrieron las puertas a las fuerzas de Uesugi Kenshin. Después de meses intentando entrar, el enemigo ya no tuvo que conquistar las murallas.

Nanao no cayó porque sus piedras fueran demasiado débiles. La fortaleza cayó cuando las condiciones que garantizaban su seguridad dejaron de ser gobernadas.

Más de cuatro siglos después, las organizaciones continúan construyendo castillos: los muros ahora son firewalls; los puestos de vigilancia, centros de operaciones de seguridad; los fosos, mecanismos de segmentación; y las puertas están protegidas mediante MFA, sistemas de gestión de identidades, SIEM, EDR y plataformas de monitoreo.

Las empresas invierten millones en fortalecer esas defensas, pero una organización no es segura simplemente porque tenga buenas murallas. También necesita saber quién puede abrir las puertas.

Ese es uno de los principios fundamentales del manejo proactivo del riesgo. La gestión del riesgo no debería comenzar cuando ocurre un incidente, sino mucho antes, cuando todavía es posible identificar las condiciones que podrían permitirlo.

Una cuenta administrativa que conserva privilegios innecesarios, un proveedor con acceso permanente a un entorno crítico, una excepción de seguridad temporal que nunca vuelve a revisarse o un sistema legado que permanece operativo pueden parecer, individualmente, decisiones justificables. Sin embargo, cuando estas decisiones se acumulan y dejan de ser supervisadas, pueden convertirse en las puertas de Nanao.

El problema es que el riesgo no permanece estático. Mientras la organización evoluciona, aparecen nuevos proveedores, aplicaciones, vulnerabilidades e identidades; cambian las funciones, las arquitecturas y los permisos. Una decisión aceptable meses atrás puede convertirse posteriormente en una exposición crítica. Por eso, gobernar el riesgo exige revisar continuamente las condiciones que pueden modificarlo.

Un ejemplo demuestra hasta dónde puede llegar este problema. En febrero de 2024, Change Healthcare, una de las principales plataformas de procesamiento de transacciones del sistema de salud estadounidense, sufrió un ciberataque que produjo importantes interrupciones en servicios relacionados con prescripciones, reclamaciones médicas y pagos.

Los atacantes utilizaron credenciales comprometidas para ingresar remotamente a un portal Citrix que no tenía autenticación multifactor habilitada. Una vez dentro, consiguieron desplazarse lateralmente por el entorno, extraer información y posteriormente desplegar ransomware.

El caso resulta especialmente relevante porque el punto de entrada no fue una sofisticada vulnerabilidad desconocida. La puerta existía, era utilizada legítimamente para acceso remoto y simplemente no contaba con una protección que hoy se considera fundamental.

Precisamente allí aparece la diferencia entre gestionar vulnerabilidades y gobernar el riesgo. No se trata únicamente de preguntar qué vulnerabilidades existen, sino qué decisiones, excepciones y condiciones están creando la exposición del futuro.

¿Por qué un sistema crítico continúa sin MFA? ¿Quién aceptó ese riesgo? ¿Durante cuánto tiempo debía permanecer aceptado? ¿Qué mecanismo debía verificar que esa condición fuera corregida?

El manejo proactivo del riesgo convierte estas preguntas en un proceso continuo y obliga a la organización a revisar sus decisiones conforme cambia el negocio.

Esta perspectiva adquirió todavía mayor relevancia cuando, en febrero de 2024, NIST publicó la versión 2.0 de su Cybersecurity Framework e incorporó GOVERN como una sexta función junto con Identify, Protect, Detect, Respond y Recover.

Con ello, NIST hizo explícito que la gestión de la ciberseguridad también requiere establecer estrategias de riesgo, responsabilidades, políticas, mecanismos de supervisión y gestión del riesgo asociado con terceros y cadenas de suministro. La ciberseguridad deja entonces de ser exclusivamente responsabilidad de quienes administran herramientas técnicas y pasa a formar parte de la gestión del riesgo empresarial y de las decisiones de liderazgo.

Un firewall puede bloquear una conexión, pero no puede decidir cuánto riesgo está dispuesta a aceptar una organización. Un EDR puede identificar una actividad sospechosa, pero no puede determinar quién debe asumir la responsabilidad sobre un sistema crítico. Una solución de IAM puede restringir permisos, pero no puede decidir por qué un proveedor necesita determinado nivel de acceso ni durante cuánto tiempo debería conservarlo.

Esas son decisiones de gobernanza. En otras palabras, alguien debe conocer dónde están las puertas, quién posee las llaves y bajo qué circunstancias puede utilizarlas.

Gestionar los riesgos de manera proactiva implica evitar que las decisiones se acumulen silenciosamente. Requiere propietarios reales para los riesgos, fechas de vencimiento para las excepciones, revisiones periódicas de accesos privilegiados, seguimiento a terceros y mecanismos que permitan detectar cuándo ha cambiado la exposición de la organización.

También requiere una cultura donde identificar un riesgo no sea interpretado como un fracaso. Una gobernanza madura no busca organizaciones donde nadie encuentre problemas; busca organizaciones capaces de encontrarlos antes que sus adversarios.

Los defensores de Nanao pudieron observar durante meses al ejército enemigo al otro lado de sus fortificaciones. Sabían dónde estaba la amenaza y habían construido defensas capaces de mantenerla lejos. Lo que no consiguieron controlar fue el deterioro que estaba ocurriendo detrás de sus propias murallas.

Ese sigue siendo uno de los grandes retos de la gobernanza moderna.

Una organización verdaderamente resiliente no es aquella que confía en que sus murallas son inexpugnables, sino aquella que evalúa continuamente qué podría debilitarlas, quién puede abrir sus puertas y qué decisiones podrían transformar una fortaleza en una falsa sensación de seguridad.

Porque el manejo efectivo del riesgo no comienza cuando el ejército aparece frente al castillo. Comienza mucho antes, cuando todavía estamos a tiempo de decidir quién tiene las llaves.



Juan Pablo Campo Téllez
Cybersecurity Engineer

IA y riesgo corporativo: de la evaluación periódica a un radar continuo

Artículo por Ángel Fernando Andrango Mejía

La inteligencia artificial evoluciona más rápido de lo que las organizaciones pueden anticipar sus riesgos. En este contexto, la ventaja competitiva ya no estará únicamente en adoptar IA, sino en desarrollar capacidades para identificar, comprender y gobernar sus riesgos de forma continua.

Cuando la velocidad de la IA supera la velocidad del riesgo

Las matrices de riesgo siguen siendo herramientas valiosas para priorizar y apoyar la toma de decisiones. Sin embargo, cuando la IA modifica rápidamente el nivel de exposición de una organización, estas herramientas necesitan alimentarse con información actualizada sobre las tecnologías utilizadas, los datos procesados, los accesos concedidos, las integraciones habilitadas, las vulnerabilidades detectadas, los incidentes y las dependencias operativas.

El objetivo no es sustituir la matriz de riesgos, sino complementarla con una capacidad de observación continua que permita comprender cómo cambia la exposición de la organización y apoyar decisiones más oportunas.

De esta forma, la gestión del riesgo evoluciona desde una fotografía revisada periódicamente hacia una visión más dinámica, capaz de identificar cambios y anticipar escenarios antes de que generen impactos relevantes para el negocio.

La nueva generación de modelos: ¿qué cambia?

La atención del mercado suele centrarse en cada nuevo modelo de IA que aparece. Sin embargo, el verdadero desafío no radica en una tecnología específica, sino en una tendencia más profunda: la capacidad de estas soluciones para ampliar continuamente lo que personas y organizaciones pueden hacer.

La IA no solo introduce nuevas formas de exposición; también modifica la velocidad, escala e interdependencia de los riesgos existentes. Una misma solución puede procesar información sensible, conectarse a sistemas críticos, automatizar decisiones y depender simultáneamente de proveedores externos.

Estas capacidades ofrecen importantes oportunidades de productividad y transformación, pero también pueden ampliar la exposición con la misma rapidez con la que se adopta la tecnología.

El riesgo aparece cuando estas capacidades operan sin suficiente visibilidad, supervisión o gobierno. Por ello, resulta fundamental comprender dónde pueden materializarse las principales exposiciones y cómo pueden afectar a la organización.

Riesgos estratégicos para una gestión empresarial anticipada

La IA incrementa la complejidad del riesgo porque combina datos, sistemas, decisiones automatizadas y dependencias externas dentro de una misma solución.

Por ello, una gestión anticipada debería observar al menos cinco dimensiones:

Datos y privacidad

Uso indebido de información sensible, nuevos flujos de datos y accesos no previstos.

Ciberseguridad

Suplantación, explotación de vulnerabilidades e integraciones con modelos y agentes.

Operación

Dependencias tecnológicas, fallos, cambios de proveedores y adopción de IA en procesos críticos.

Cumplimiento y ética

Falta de trazabilidad, responsables definidos o criterios regulatorios claros.

Reputación y negocio

Errores o incidentes con impacto en clientes, confianza, decisiones o marca.

La IA, por tanto, no constituye una categoría aislada de riesgo. Su impacto atraviesa simultáneamente la ciberseguridad, la privacidad, la continuidad operativa, el cumplimiento y la reputación.

Del listado de riesgos al radar inteligente

La diferencia entre una matriz tradicional y un radar inteligente está principalmente en la capacidad de observar la evolución del riesgo.

Matriz de riesgos

Identifica → Evalúa → Registra → Revisa

Radar inteligente

Descubre → Correlaciona → Prioriza → Responde → Aprende

Ambos enfoques son complementarios. Mientras la matriz permite estructurar y evaluar riesgos conocidos, el radar incorpora una lógica de observación continua que conecta señales procedentes de distintas fuentes para comprender cómo está cambiando la exposición.

Este enfoque permite:

1. Descubrir herramientas, modelos, agentes e integraciones.
2. Correlacionar señales procedentes de datos, usuarios, sistemas y proveedores.
3. Priorizar los riesgos de mayor impacto y criticidad.
4. Responder mediante controles y acciones de mitigación.
5. Aprender de incidentes y nuevos patrones para mejorar continuamente la capacidad de monitoreo.

En síntesis, la matriz muestra dónde está el riesgo; el radar ayuda a comprender hacia dónde se está desplazando.

Los indicadores que anticipan el riesgo

Una capacidad de observación continua necesita indicadores que permitan identificar señales tempranas antes de que se conviertan en incidentes o afectaciones relevantes para el negocio.

Entre los indicadores que pueden resultar especialmente útiles se encuentran:

- Herramientas de IA sin gobernanza definida.
- Casos de uso de IA sin un responsable de negocio asignado.
- Integraciones de IA conectadas a sistemas críticos.
- Vulnerabilidades asociadas a modelos, proveedores o conectores.
- Tiempos de detección y respuesta ante eventos relacionados con IA.

La medición continua de estas señales ayuda a identificar tendencias emergentes y a evolucionar desde una gestión principalmente reactiva hacia una capacidad preventiva y anticipativa.

Innovar con velocidad, gobernar con anticipación

Durante los próximos años, el factor diferenciador no será únicamente quién adopte más inteligencia artificial, sino quién consiga comprenderla, supervisarla y gobernarla mejor.

Las organizaciones que desarrollen capacidades de observación continua estarán mejor preparadas para aprovechar los beneficios de la IA mientras gestionan de forma proactiva sus impactos sobre la información, la seguridad, la operación y la confianza.

Porque en un entorno donde los modelos evolucionan constantemente, el riesgo ya no puede gestionarse mirando únicamente el pasado. Debe gestionarse observando el horizonte.



**Ángel Fernando Andrango
Mejía**
Cybersecurity Lead Analyst

Intelligence we trust: la confianza como nueva frontera de la IA

Artículo por María Pilar Torres Bruna

La inteligencia artificial ya es capaz de sorprendernos. El próximo desafío es más profundo: lograr que sus decisiones sean entendibles, verificables y seguras a medida que gana autonomía.

Hoy la Inteligencia Artificial ya redacta, analiza, predice, recomienda, automatiza procesos y asiste en decisiones que antes dependían exclusivamente de las personas. Su capacidad es extraordinaria, pero en este momento, la IA dejó atrás la etapa en la que debía demostrar su potencial. Estamos pasando a la siguiente etapa en la adopción de esta tecnología, y es plantearnos para qué procesos o decisiones podemos confiar en ella.

A medida que dependemos de la IA para responder consultas complejas e incluso ejecutar acciones —por ejemplo, priorizar una alerta, aprobar una operación, interactuar con un cliente o recomendar una decisión crítica— aparece la confianza como una condición esencial para seguir ahondando en su uso y adoptarla con paso firme. La IA ya nos está ayudando a hacer sistemas más capaces, más impresionantes. Pero ahora el foco está en hacerlos confiables.

Y eso nos cambia la conversación y la arquitectura que acompaña la IA en una organización. La confianza es mucho más que una declaración de principios o una política de seguridad y debe traducirse en una capacidad operativa: algo que las organizaciones puedan diseñar, poner en práctica, monitorear y demostrar.

De la fascinación a la confianza

Durante los últimos años, ya hemos explorado qué puede crear la IA, cuánto puede ayudar a una organización a acelerar su negocio y qué tareas puede transformar.

Sin embargo, a medida que la tecnología comienza a operar con mayor autonomía, necesitamos conocer cómo llegó a una conclusión, con qué información trabajó, qué límites tiene y quién puede intervenir si algo no sale como debería. Demandamos transparencia y trazabilidad en los procesos de esta tecnología.

La IA puede crear inteligencia; los agentes pueden convertir esa inteligencia en acción; pero la confianza es lo que vuelve esa acción aceptable, segura y escalable.

Una organización puede incorporar IA en múltiples procesos, pero tiene que ser capaz de explicar, controlar y auditar sus decisiones. Si no adquiere esta capacidad, será difícil escalar el uso de la IA, será difícil transmitir confianza a los empleados y clientes de esta organización. La confianza es lo que permite pasar de una prueba de concepto atractiva a una adopción real.

Tres preguntas para construir confianza

Una manera sencilla de abordar este desafío es partir de tres preguntas fundamentales.

1. ¿Podemos entenderla?

Si un sistema recomienda una acción, las personas responsables deben poder comprender, al menos en un nivel adecuado al contexto, por qué lo hizo.

La transparencia y la trazabilidad permiten explicar, a partir de la información introducida, los resultados planteados, entender la recomendación y explicarla cuando sea necesario.

Esto es especialmente relevante en decisiones de alto impacto, que afectan a la vida de las personas, como su carrera profesional, o que incluso pueden salvar una vida. Si una IA sugiere bloquear una transacción, descartar una candidatura, priorizar un caso médico o asignar un recurso, la decisión tiene que ser explicable.

2. ¿Podemos verificarla?

La calidad de una respuesta de IA es proporcional a la calidad de la información que la alimenta. Los datos deben estar completos, actualizados y debemos asegurar que no han sido manipulados.

La confianza comienza en el origen de los datos. Las organizaciones necesitan saber de dónde proviene la información, quién la modifica, cuándo se ha modificado y si ha habido alguna otra alteración.

El proceso de cambios debe ser trazable, ya que la trazabilidad es cada vez más relevante en un entorno donde circulan contenidos sintéticos, datos de múltiples fuentes y decisiones automatizadas.

Verificar también implica validar la autenticidad del contenido y de las identidades que intervienen. La fuente, sea organización, persona o incluso agente, debe ser confiable.

En la era de la IA, conocer el origen y la integridad de la información deja de ser un requisito técnico para convertirse en una condición de confianza.

3. ¿Podemos cuestionarla?

La última parte de la confianza la forman los mecanismos habilitados para supervisar, desafiar, corregir o revertir las decisiones que toma la IA cuando el contexto lo requiera.

Una IA confiable y los agentes definidos con IA deben tener límites claros. Deben saber qué pueden hacer, a qué información pueden acceder y cuándo deben escalar una decisión a una persona. También debe ser posible intervenir si detectamos un comportamiento inesperado, una desviación respecto de las reglas establecidas o una señal de manipulación.

Aquí, la colaboración entre IA y ciberseguridad adquiere una nueva dimensión.

El enfoque de Zero Trust, tradicionalmente aplicado a usuarios, dispositivos y conexiones, también es relevante y útil para los sistemas inteligentes. La regla es simple: confianza cero. Cada agente, modelo o componente debe operar con permisos definidos, acceso mínimo necesario y validación continua.

Seguridad activa para sistemas que evolucionan

Los riesgos asociados a la IA van más allá de la infraestructura y los datos. Los modelos asociados para la toma de decisiones representan una nueva superficie de ataque. Un atacante puede intentar manipular las fuentes de información, alterar los permisos de un agente o influir sobre el comportamiento de un modelo. Por eso, la seguridad tiene que pasar de reactiva a activa y predictiva.

La ciberdefensa activa y la seguridad predictiva permiten detectar patrones, correlacionar grandes volúmenes de alertas y responder ante determinadas amenazas con mayor velocidad.

Una autonomía madura es una autonomía supervisada: capaz de actuar, pero también de rendir cuentas.

Gobernar la IA es gobernar sus decisiones

Cuando un sistema inteligente participa en procesos relevantes, la gobernanza no puede llegar al final. Debe estar integrada desde el diseño.

Esto implica definir responsables, derechos de decisión, circuitos de escalamiento y criterios claros para intervenir. También requiere generar evidencia: registros que permitan revisar qué ocurrió, qué datos se utilizaron, qué reglas se aplicaron y por qué el sistema tomó determinada acción.

Los audit trails explicables —o trazas de auditoría— son fundamentales para transformar la IA en una capacidad supervisada. Nos ayudan a responder ante un error y permiten aprender, mejorar controles y fortalecer la confianza de clientes, colaboradores, reguladores y socios.

La confianza no es lo que una organización dice sobre su IA. Es lo que puede probar, monitorear y gobernar.

La dimensión humana de la confianza

Por último, existe una dimensión que ninguna tecnología puede resolver por sí sola: la humana.

Las personas no evaluamos la confianza únicamente a partir de métricas de precisión. Consideramos si el sistema es justo, si respeta la privacidad, si responde en tiempos razonables y si mantenemos espacios de decisión humana, sobre todo en decisiones sensibles.

Porque para las personas, lo que resulta aceptable en un contexto puede no serlo en otro. Las expectativas cambian según la cultura, el sector, el tipo de decisión y el impacto que esta tiene sobre las personas.

Construir confianza en IA exige escuchar y esto supone comprender cómo los usuarios perciben los riesgos, qué nivel de autonomía están dispuestos a aceptar y en qué condiciones consideran legítimo que una máquina participe en una decisión que los afecta.

Hacer operativa la confianza

Convertir la confianza en una capacidad operativa implica avanzar en tres frentes de manera simultánea:

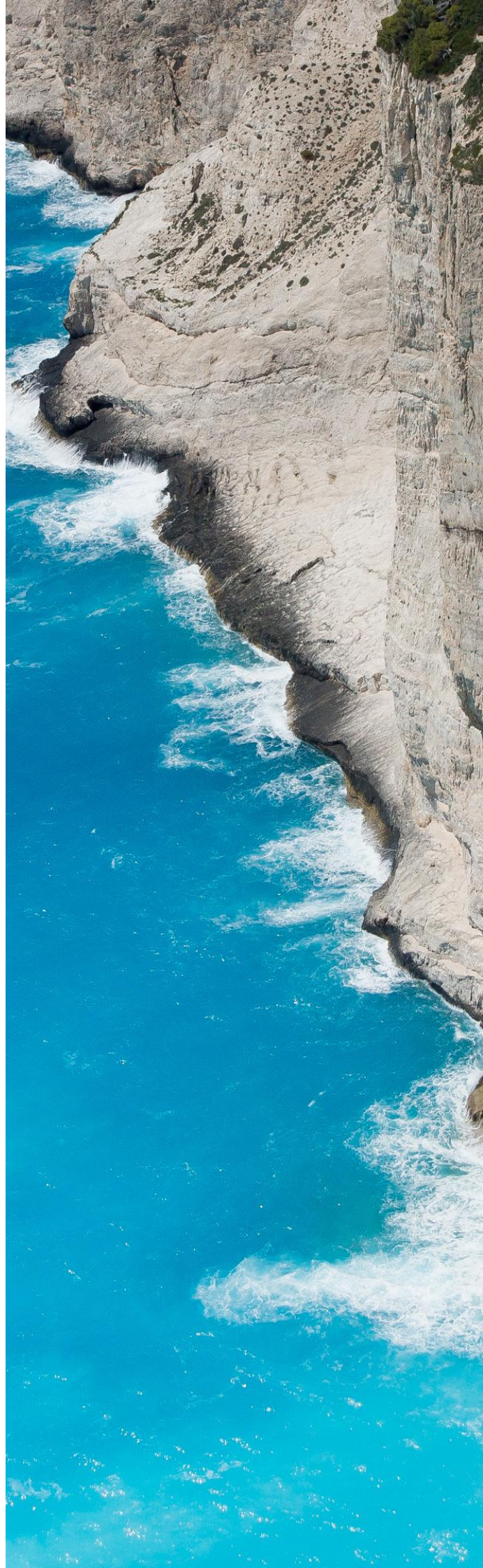
- Hacer la IA entendible: explicar decisiones y verificar contenido, fuentes y procedencia de los datos.
- Hacer la IA controlable: establecer límites, gestionar permisos, supervisar agentes y detectar manipulaciones o desvíos.
- Hacer la IA responsable: crear evidencia, trazabilidad y mecanismos de auditoría que permitan intervenir y corregir.

La inteligencia artificial seguirá avanzando. Será más potente, más integrada y más autónoma. Pero su verdadero valor dependerá de la confianza que sea capaz de generar.

Porque en la próxima etapa de la IA dejaremos de preguntar “¿puede hacerlo?” para preguntar “¿podemos confiar en lo que haga?”.



María Pilar Torres Bruna
Head of Cybersecurity IBIOL



Vulnerabilidades

Vulnerabilidad Crítica en Cisco Nexus 9000 – Ejecución remota de código

Fecha: 02 de septiembre de 2026
CVE: CVE-2026-20212



CVSS: 9.8

CRÍTICA

Descripción

Cisco ha publicado una vulnerabilidad que afecta a determinados switches Nexus 9000 Series equipados con tecnología Silicon One, alcanzando una puntuación CVSS 3.1 de 9,8.

Donde un atacante remoto y no autenticado podría llegar a ejecutar código con privilegios de *root* sobre dichos dispositivos. El problema se encuentra en la exposición de los puertos TCP 43210 y 43211 dentro de la VRF de capa 3 utilizada por defecto.

Este equipamiento de red se sitúa habitualmente en infraestructuras críticas de centros de datos, donde puede significar un alto impacto, lo que justifica una revisión prioritaria de los dispositivos afectados.

Solución

Cisco recomienda los siguientes puntos:

- Utilizar listas de control de acceso a la infraestructura (iACL) para permitir únicamente el tráfico necesario del dispositivo afectado.
- Implementar el parche para Cisco NX-OS Software:
 - Live Protect Shield Software - 10.6(3)

Productos afectados

Los siguientes identificadores de Cisco Nexus 9000 están afectados:

- N9324C-SE1U y N9348Y2C6D-SE1U
- N9364E-SG2-O/Q
- N9396T12C-SE1 y N9348Y12C-SE1
- N9336C-SE1
- N9K-C9804 y N9K-C9808

Referencias

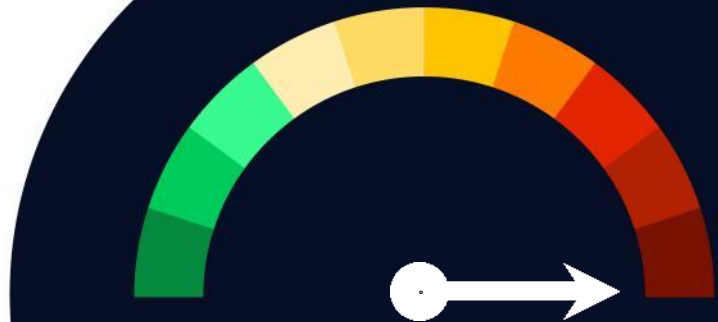
- nvd.nist.gov
- rapid7.com

Vulnerabilidades

Vulnerabilidades críticas en SonicWall SMA1000 con explotación activa

Fecha: 01 de septiembre de 2026

CVE: CVE-2026-83548 y 1 más



CVSS: 10

CRÍTICA

Descripción

SonicWall publicó 2 vulnerabilidades que afectan a los dispositivos SonicWall SMA1000:

- CVE-2026-83548: Vulnerabilidad SSRF *pre-authentication* que permite a un atacante remoto no autenticado realizar peticiones hacia recursos internos.
- CVE-2026-83549: Vulnerabilidad *post-authentication OS command injection* que permite a un atacante, con privilegios administrativos, ejecutar comandos arbitrarios en el sistema operativo del *appliance*.

Estas dos vulnerabilidades han sido explotadas activamente según ha confirmado el equipo de respuesta ante incidentes de SonicWall.

Solución

El fabricante recomienda a todas las organizaciones con dispositivos afectados las siguientes acciones:

- Actualizar a la última versión disponible en la página oficial.
- Revisar los sistemas en busca de indicadores de compromiso con el soporte del servicio de asistencia técnica de SonicWall.
- En caso de identificarse IOCs en alguno de los sistemas, las acciones recomendadas son:
 - Reinstalar el sistema operativo o los dispositivos virtuales.
 - Resetear todas las contraseñas de usuario y administrador.
 - Restablecer los tokens TOTP

Productos afectados

Los productos afectados por estas dos vulnerabilidades son los modelos 6210, 7210 y 8200v de la serie SonicWall SMA 1000 en las siguientes versiones:

- 12.4.3-03453 y versiones anteriores
- 12.5.0-02835 y versiones anteriores

Referencias

- sonicwall.com
- rapid7.com
- securityweek.com

Parches

Parche de seguridad de Microsoft para vulnerabilidades críticas en SQL Server 2022

Fecha: 8 de septiembre de 2026

CVE: CVE-2026-67378 y más

Alta

Descripción

Microsoft ha publicado varias nuevas actualizaciones de seguridad destinadas a corregir vulnerabilidades que afectan tanto a instalaciones Windows como Linux. Dentro de la rama GDR.

Estos parches corrigen diferentes vulnerabilidades como: ejecución remota de código, escalada de privilegios, divulgación de información, denegación de servicio y mecanismos de evasión de funciones de seguridad.

Entre ellas, las vulnerabilidades más destacadas son CVE-2026-67378, una vulnerabilidad de ejecución remota con CVSS 8,5, además de CVE-2026-67380, CVE-2026-67384 y CVE-2026-67385, que alcanzan CVSS 8,8.

Productos afectados

Los productos afectados son:

- SQL Server 2022 RTM GDR.

Solución

Instalar los siguientes parches de seguridad:

- KB5122771
- KB5122768

Referencias

- support.microsoft.com
- catalog.update.microsoft.com

Parches

Parche de seguridad de Adobe Commerce

Fecha: 07 de Septiembre de 2026

CVE: CVE-2026-75650

Crítica

Descripción

Adobe ha publicado un parche de seguridad de carácter urgente para corregir una vulnerabilidad crítica (CVSS 10.0) que afecta a Adobe Commerce/Magento y que está siendo explotada activamente en ataques reales.

La vulnerabilidad CVE-2026-75650, también denominada *StyleSmuggler*, afecta al sistema de plantillas de Adobe Commerce/Magento, permitiendo a un atacante remoto y no autenticado el envío de una petición especialmente manipulada para conseguir la ejecución de código PHP en el servidor.

En ataques reales recientes se ha observado el aprovechamiento de este fallo para desplegar un *backdoor* desarrollado en Rust, así como para instalar una *PHP web shell* dentro del directorio de imágenes de Magento.

Productos afectados

Los productos afectados por esta vulnerabilidad crítica son:

- Adobe Commerce versiones 2.4.4-2026-aug hasta 2.4.9-2026-aug y anteriores dentro de esas ramas.
- Adobe Commerce B2B versiones 1.3.3-2026-aug, 1.3.4-2026-aug, 1.4.2-2026-aug, 1.5.2-2026-aug y 1.5.3-2026-aug y anteriores.
- Magento Open Source versiones 2.4.6-2026-aug hasta 2.4.9-2026-aug y anteriores.

Solución

El fabricante recomienda aplicar de inmediato el parche VULN-39341 y rotar las claves de cifrado y las credenciales potencialmente expuestas, incluidas las de administrador, servidor, base de datos, APIs e integraciones. Adicionalmente, se recomienda revisar los IoCs identificados en los ataques observados.

Referencias

- helpx.adobe.com
- experienceleague.adobe.com
- sansec.io
- thehackernews.com

Eventos

ISACA 2026 Europe Conference

7 de octubre – 9 de octubre

ISACA Europe Conference reunirá en Múnich y en formato virtual a profesionales y líderes de tecnología, ciberseguridad, auditoría, gobierno y gestión del riesgo. Por su enfoque en gobierno, riesgo y toma de decisiones, resulta especialmente relevante para organizaciones que buscan anticiparse a un entorno tecnológico cada vez más dinámico.

[Enlace](#)

Cyber Security & Cloud Expo Europe 2026

19 de octubre – 20 de octubre

Cyber Security & Cloud Expo Europe reunirá en Ámsterdam a responsables de ciberseguridad, tecnología y transformación digital. La agenda contempla liderazgo en ciberseguridad y riesgo empresarial, seguridad cloud, inteligencia artificial, identidad, Zero Trust y cumplimiento.

[Enlace](#)

ISC2 Security Congress 2026

24 de octubre – 28 de octubre

ISC2 Security Congress reunirá en Denver y en formato virtual a profesionales de la comunidad global de ciberseguridad. La edición 2026 incluye sesiones sobre liderazgo, gestión del riesgo, seguridad de la inteligencia artificial y retos de supervisión ante la innovación.

[Enlace](#)

Recursos

➤ **The new rules of trust: Governance, risk and compliance in the AI era**

Publicación de NTT DATA que analiza cómo la inteligencia artificial, cloud, los ecosistemas digitales y la evolución regulatoria están transformando los modelos tradicionales de gobierno, riesgo y cumplimiento. Plantea la evolución hacia un GRC más integrado y proactivo.

[Enlace](#)

➤ **Global Cybersecurity Outlook 2026**

Informe del World Economic Forum, en colaboración con Accenture, que analiza los principales factores que transforman el panorama global de ciberseguridad: inteligencia artificial, fragmentación geopolítica, cadenas de suministro y brechas de capacidades.

[Enlace](#)

➤ **NIST CSF 2.0: Cybersecurity, Enterprise Risk Management and Workforce Management Quick-Start Guide**

Guía de NIST publicada en marzo de 2026 que conecta la gestión del ciberriesgo con el riesgo empresarial y las capacidades necesarias para responder a un entorno tecnológico en evolución.

[Enlace](#)



Suscríbete a RADAR
up.nttdata.com/suscribetearadar

**Powered by the
cybersecurity
NTT DATA team**

es.nttdata.com