Número 120 | Noviembre 2026

NTT DATA

Radar

El magazine de ciberseguridad



Privacidad que compite: menos datos, más confianza, más negocio

Por Soledad Romero Jiménez

Durante años, la privacidad se ha gestionado como una obligación: cumplir el RGPD, actualizar políticas, responder derechos y evitar sanciones. Ese enfoque sigue siendo necesario, pero ya no es suficiente. En una economía basada en datos, inteligencia artificial y servicios digitales, la privacidad empieza a jugar en otro terreno: el de la eficiencia, la confianza y la capacidad de innovar.

El verdadero riesgo no está solo en tratar datos de forma incorrecta, sino en no saber exactamente qué datos tenemos, por qué los conservamos, quién los utiliza, dónde se replican y cuándo deberían desaparecer. Esa acumulación silenciosa crea una auténtica deuda de privacidad. Y, como ocurre con la deuda técnica, cuanto más tarda una organización en afrontarla, mayor es el coste: más superficie de ataque, migraciones más complejas, auditorías más lentas, respuestas más difíciles ante incidentes y menor agilidad para transformar el negocio.

La ventaja competitiva comienza, precisamente, cuando la organización cambia esa lógica. No se trata de almacenar más, sino de gobernar mejor. Saber qué información aporta valor, reducir la que ya no lo aporta y automatizar su conservación, bloqueo, anonimización o borrado permite convertir la privacidad en una disciplina operativa.

Ese cambio exige liderazgo. La privacidad no puede permanecer confinada al DPO o al área jurídica. Dirección, Tecnología, Seguridad, Datos, Compras, Recursos Humanos y negocio deben compartir responsabilidades, indicadores y evidencias. Un inventario vivo de sistemas y datos, reglas claras de conservación, responsables definidos y controles automatizados aportan algo mucho más valioso que una política bien redactada: capacidad real de demostrar cómo se gobierna la información.

La inteligencia artificial acelera todavía más esta necesidad. Las organizaciones están pasando de experimentar con IA a integrarla en procesos, decisiones y operaciones. Pero no basta con desplegar herramientas. Hay que saber utilizarlas. La alfabetización en IA se convierte así en una capacidad de gobierno: comprender qué puede hacer un sistema, qué información puede recibir, dónde necesita validación humana, qué riesgos introduce y qué controles deben acompañarlo.

Esto cambia también el papel de Seguridad y Privacidad. En lugar de aparecer al final para aprobar o frenar una iniciativa, pueden ayudar a diseñarla desde el principio: usuarios formados, datos adecuados, permisos limitados, supervisión, trazabilidad y guardrails prácticos. La innovación responsable deja entonces de ser un principio abstracto y se convierte en una forma cotidiana de trabajar.

Los beneficios son muy concretos. Por ejemplo, en el sector financiero, una entidad que minimiza la información recabada automatiza su ciclo de vida y establece qué datos pueden utilizar sus sistemas de IA —según finalidad, sensibilidad y permisos— reduce exposición, simplifica operaciones y puede innovar con mayor rapidez y seguridad.

En salud, la seudonimización, la segregación de accesos y unas reglas efectivas de ciclo de vida permiten reutilizar información para investigación o analítica clínica reduciendo la exposición de la información de los pacientes.

En la Administración Pública, la verificación selectiva de atributos —por ejemplo, acreditar una condición sin entregar documentación completa— puede simplificar trámites, reducir información almacenada y mejorar la confianza del ciudadan en los servicios digitales.

También existen riesgos capaces de erosionar rápidamente esa ventaja: shadow AI, proveedores con acceso excesivo, copias históricas nunca depuradas, datos de prueba con información real, empleados sin formación o sistemas heredados cuyo uso nadie sabe justificar. Y para la información que debe conservarse durante años aparece además una cuestión estratégica: la criptoagilidad y la preparación frente a la computación cuántica. Proteger hoy datos de larga sensibilidad también exige pensar en cómo seguirán protegidos mañana.

Aquí es donde NTT DATA puede aportar una visión integral: desde la identificación y reducción de la deuda de privacidad hasta el diseño del gobierno del dato, inventarios y mapas de tratamiento, automatización de conservación y borrado, privacidad desde el diseño, gobierno y alfabetización de IA, integración con ciberseguridad y hojas de ruta de criptoagilidad. No como iniciativas aisladas, sino como capacidades conectadas con procesos, tecnología, riesgo y objetivos de negocio.

La conclusión es sencilla: la privacidad genera ventaja cuando deja de gestionarse como documentación y empieza a gestionarse como una capacidad empresarial. Las organizaciones que conocen mejor sus datos pueden reducir riesgo, operar con mayor eficiencia, adoptar IA con más seguridad e innovar sobre una base de confianza.

Privacidad competitiva no es tener más datos. Es saber exactamente cuáles merecen seguir estando.



Soledad Romero Jiménez
Expert Consultant in Cybersecurity



La exposición de datos personales a través de nuevas vías de ataque

Cibercrónica por Nuria Ripoll Cedillo

Las últimas brechas de seguridad muestran diferentes formas de acceder a los datos personales. Las conexiones entre organizaciones, el uso de proveedores tecnológicos, las solicitudes fraudulentas y la incorporación de inteligencia artificial a los ataques amplían los escenarios en los que la información puede quedar expuesta.

A finales de septiembre, Renfe detectó un acceso no autorizado a determinados sistemas corporativos. La compañía activó sus protocolos de seguridad y comenzó una investigación para determinar el origen y el alcance del incidente. El 25 de septiembre, los primeros indicios técnicos apuntaban a servidores de Adif previamente comprometidos que mantenían conexiones con sistemas de Renfe.

Las investigaciones iniciales señalaron que los atacantes podrían haber accedido a información de usuarios, principalmente nombres y direcciones de correo electrónico. Sin embargo, a medida que avanzaron las comprobaciones, Renfe confirmó que el acceso había alcanzado determinados sistemas relacionados con los procesos de venta de billetes, por lo que procedió a notificar el incidente a las personas potencialmente afectadas.

En su comunicación, la compañía advirtió de la posible exposición de información identificativa y de contacto, así como de determinados datos asociados a la utilización de sus servicios ferroviarios. Renfe también informó de que había reforzado las medidas de seguridad y mantenía abierta la investigación para determinar con precisión qué información había podido quedar comprometida.

Por su parte, **Adif** comunicó que el incidente podía haber afectado a información personal almacenada en su Plataforma de Licitación Electrónica, alojada en un entorno externo y gestionada por un proveedor tecnológico. La posible exposición también alcanzaba información de sus sistemas corporativos. Ambas organizaciones continuaron analizando el incidente y adoptando medidas para contener los accesos detectados.

Unas semanas antes, **Revolut** había confirmado otro incidente relacionado con la exposición de información personal. En esta ocasión, los atacantes utilizaron una cuenta de correo perteneciente a un dominio legítimo de una agencia gubernamental para enviar solicitudes fraudulentas sobre determinados clientes.

Las comunicaciones aparentaban proceder de una autoridad oficial y solicitaban información que habitualmente puede ser requerida en el marco de investigaciones administrativas o judiciales. La utilización de un dominio auténtico contribuyó a que las peticiones fueran consideradas legítimas y Revolut facilitara información a un tercero no autorizado.

Entre los datos comprometidos se encontraban nombres, fechas de nacimiento, direcciones postales, números de teléfono y documentos de identidad, incluidos pasaportes y permisos de conducir. En determinados casos, la información también podía incluir fotografías utilizadas durante los procesos de verificación, extractos bancarios e historiales de transacciones.

Según las informaciones publicadas posteriormente, la brecha afectó aproximadamente a 680 clientes, algunos de ellos vinculados a operaciones con criptomonedas. Los responsables del ataque habrían intentado extorsionar a la compañía mediante amenazas de publicación de los datos obtenidos. Revolut confirmó el incidente, contactó con los afectados y comunicó lo ocurrido a las autoridades competentes. Asimismo, indicó que sus sistemas internos y los fondos de los clientes permanecían protegidos.

Esta actividad habría permitido al agente avanzar por distintas fases del ataque hasta conseguir modificar datos personales y acceder a facturas almacenadas en la aplicación. La secuencia descrita incluía tareas de reconocimiento, acceso y búsqueda de vulnerabilidades que habrían sido ejecutadas con un elevado grado de automatización.

La AEPD mantenía el incidente bajo análisis para determinar las circunstancias en las que se produjo y su alcance. La información publicada tampoco permitía establecer conclusiones definitivas sobre la intervención humana durante las distintas fases del ataque.

En pocas semanas, estos incidentes han mostrado diferentes formas de acceder a información personal. En Renfe y Adif, la investigación se centró en sistemas interconectados y plataformas externas; en Revolut, los atacantes consiguieron obtener datos mediante solicitudes fraudulentas procedentes de un dominio gubernamental legítimo; en Belnet, la explotación de una vulnerabilidad en tecnología de un proveedor permitió copiar comunicaciones y archivos; y, en el caso notificado a la AEPD, un agente de inteligencia artificial habría participado en distintas fases de la intrusión.

Las conexiones entre organizaciones, las dependencias tecnológicas, la confianza en las comunicaciones y la automatización de los ataques amplían los escenarios en los que los datos personales pueden quedar expuestos. Los incidentes recientes reflejan la importancia de mantener controles sobre los sistemas, las relaciones con terceros y los procesos mediante los que se accede y comparte información.



Nuria Ripoll Cedillo
Cybersecurity Consultant



La deuda de privacidad: el pasivo olvidado de la transformación digital

Artículo por Toni Sansa Aizcorbe

Desde la entrada en vigor del Reglamento General de Protección de Datos (RGPD), numerosas empresas han aprobado políticas de retención y borrado. Sin embargo, son pocas las que disponen de un sistema realmente circular, automatizado y comprobable para gestionar los datos desde su recogida hasta su eliminación, anonimización o bloqueo.

Este problema puede entenderse como **deuda de privacidad:** son los datos que una empresa acumula y almacena de forma indefinida, sin establecer para qué necesita los datos, cuánto tiempo debe conservarlos y cómo debe eliminarlos. Del mismo modo que mantener aplicaciones obsoletas o implantar soluciones rápidas sin una arquitectura sostenible genera costes futuros, conservar datos sin gobierno, sin plazos de conservación y borrado, incrementa progresivamente el riesgo, la complejidad y los costes operativos.

La transformación digital ha permitido conocer mejor a clientes, automatizar procesos, personalizar servicios y tomar decisiones basadas en datos. Pero también ha incrementado considerablemente el número de sistemas, integraciones, soluciones SaaS y bases de datos que almacenan información personal. Los datos se replican entre departamentos y sus sistemas. Sin un control adecuado, las organizaciones terminan acumulando información cuya procedencia, finalidad, titularidad o plazo de conservación ya no pueden explicar.

La deuda de privacidad no es únicamente una cuestión de cumplimiento normativo. También implica un riesgo operativo, financiero, reputacional y de ciberseguridad. Cada dato conservado innecesariamente aumenta la superficie de ataque ante cualquier incidente de seguridad. También puede afectar al buen desarrollo de las auditorías, a la falta de existencia de evidencias, encarecer las migraciones tecnológicas o ralentizar las respuestas a ejercicios de derechos de los interesados.

La pregunta, por tanto, no es solo si una entidad cumple formalmente con el RGPD, sino si puede demostrar que gestiona sus datos personales de forma eficiente, sostenible y demostrable más allá de la regulación interna que se haya elaborado al respecto.

La privacidad se tiene que implementar de manera transversal

Uno de los errores más habituales es considerar que la privacidad corresponde exclusivamente al área jurídica, de cumplimiento o al delegado de protección de datos. Estos perfiles tienen un papel esencial, pero no pueden controlar por sí solos todos los tratamientos que se producen en una organización.

Los datos personales circulan por prácticamente todas las áreas. El Departamento de Marketing utiliza información para campañas y segmentación de clientes; los comerciales gestionan contactos y oportunidades de negocio recabando información y analizando la misma; los de Recursos Humanos tratan y almacenan datos de empleados y candidatos de procesos de selección; atención al cliente accede a historiales e incidencias; Finanzas conserva datos de facturación y contratos, etc. Cada decisión, innovación o nueva implementación dentro de la empresa puede reducir o aumentar la deuda de privacidad.

Por este motivo el gobierno de los datos y su posterior conservación y borrado debe ser transversal. La alta dirección debe implicarse desde un primer momento y respaldar el proyecto de conservación y borrado de datos en cuestión, vinculándolo a objetivos de negocio, tratamiento del riesgo y transformación digital.

Cada Departamento debe identificar los datos que realmente necesitan, su finalidad, su base jurídica y su plazo de conservación en colaboración con el Delegado de Protección de Datos o Departamento Jurídico en cuestión y con el Área de Tecnología o Sistemas de la compañía para que implemente desde un principio limitación de accesos, aplicar retenciones, ejecutar borrados y generar evidencias.

 © Copyright NTT DATA, Inc.

El modelo debe funcionar como cualquier otro sistema de control corporativo: con responsables definidos (es recomendable elaborar una RACI), procedimientos documentados, indicadores, revisiones periódicas y mecanismos de escalado. De lo contrario, se corre el riesgo de seguir almacenando los datos por inercia sin control aumentando riesgos e incrementando el impacto en caso de incidente de seguridad de manera innecesaria.

Cuando se empieza un proyecto de conservación y borrado de datos, la regla predominante sería **«si nadie puede justificar por qué se conserva un dato, quién es responsable de él y cuándo debe eliminarse, ese dato constituye una fuente de riesgo».**

Una oportunidad de negocio y eficiencia

La privacidad suele percibirse como un coste inevitable asociado a políticas, contratos, auditorías y potenciales sanciones. Sin embargo, una buena gestión de datos personales también puede convertirse en una ventaja competitiva.

La confianza es cada vez más relevante en la relación con clientes, empleados, socios e instituciones. Las personas esperan transparencia sobre el uso de su información, especialmente cuando se trata de datos financieros, laborales, sensibles o relativos al comportamiento digital. Una empresa que demuestra que recoge solo los datos necesarios, los protege adecuadamente y facilita el ejercicio de derechos transmite madurez, fiabilidad y responsabilidad.

Reducir los datos innecesarios también mejora la eficiencia económica. Mantener grandes volúmenes de información genera costes de almacenamiento, licencias, administración, copias de seguridad, soporte, migraciones, auditorías e investigaciones de incidentes. Eliminar datos sin valor operativo o legal permite simplificar los entornos tecnológicos y reducir gastos.

Asimismo, la calidad del gobierno del dato acelera la innovación. Cuando una organización conoce sus sistemas, tiene inventarios actualizados y aplica reglas claras de acceso, conservación y reutilización, puede lanzar productos y servicios con mayor agilidad. En cambio, cuando los datos están dispersos, duplicados o mal documentados, cada iniciativa exige un trabajo previo de investigación: localizar la información, comprobar su calidad, validar su legitimidad y analizar los riesgos asociados.

¿Cómo puedo empezar con un proyecto de conservación y borrado de datos?

Desde un principio debemos saber a lo que nos enfrentamos. Realizar un gap assessment o una auditoría interna específica para identificar la deuda de privacidad es clave y ayuda enormemente a definir una hoja de ruta realista.

La opción más recomendable es realizar una auditoría, esta no debe limitarse a revisar políticas corporativas o cláusulas informativas o plazos de prescripción de borrado de los datos. Debe contrastar la normativa existente con la realidad operativa y tecnológica. Es frecuente encontrar registros de actividades de tratamiento desactualizados, bases de datos obsoletas, o plataformas de proveedores que se comunican datos a otros sistemas sin tener constancia de ello.

La auditoría debe responder, con evidencias, a cuestiones como:

- Qué datos personales se tratan.
- En qué sistemas, ubicaciones y entornos se encuentran.
- Con qué finalidad se recogieron y cuál es su base jurídica.
- Quién accede a ellos y con qué permisos.
- Qué proveedores o terceros intervienen.
- Cuánto tiempo deben conservarse.
- Qué mecanismos existen para bloquear, anonimizar o eliminar la información.
- Si los controles se aplican también en desarrollo, pruebas, respaldos y repositorios históricos.

Es recomendable que el auditor interno esté familiarizado con la aplicación del RGPD o certificaciones relacionadas, de lo contrario se recomienda buscar un asesoramiento externo de especialistas con el fin de realizar un plan de auditoría adecuado. Las brechas suelen aparecer entre lo que una organización declara y lo que realmente ocurre. Por ejemplo, una política puede prever la eliminación de currículums tras un periodo determinado, pero los datos pueden persistir en los buzones del correo electrónico utilizados a tal fin.

Fases del proyecto de borrado y conservación de datos

Una vez se ha realizado la auditoría o el gap assessment, es necesario elaborar un proyecto de conservación y borrado de datos por fases e implicar a todos los departamentos de la empresa que traten datos personales.

En primer lugar, se debe elaborar un inventario de sistemas con la participación de todas las Áreas de la empresa, que incluya además del nombre de la herramienta, su propietario interno, finalidad, categorías de datos, usuarios, integraciones, ubicación, proveedor, transferencias internacionales, medidas de seguridad y plazos de conservación actuales (si existen), elaboración de procesos de borrado, anonimización o bloqueo teniendo en cuenta lo que permitan por defecto los sistemas propios o de terceros. En la elaboración del inventario se debe tener especial cuidado con sistemas heredados que tienen un impacto directo en negocio, ya sea fruto de una compra de unidad de negocio, empresa o grupo corporativo.

También sería necesario determinar la posible automatización de los procesos de borrado, anonimización o bloqueo, priorizando siempre que sea posible los procesos automatizados frente a los manuales, en caso de no disponer de recursos, establecer un plazo de implementación, aunque no sea inmediato.

Posteriormente se debe tener en cuenta una previsión de presupuesto y de los recursos que serán necesarios, así como los plazos de inicio e implementación de las fases del proyecto. En este sentido, optaría por una visión conservadora y más aún si la empresa no ha realizado ejercicios similares o no está familiarizada con el concepto. Asimismo, el proceso no debe finalizar una vez implementado, debe permanecer una fase permanente de monitorización y control de los procedimientos implementados de conservación y borrado, estableciendo mejoras continuas siempre que sea posible.

Finalmente se tiene que presentar el plan frente a la dirección y en su caso al Consejo de Administración de la compañía, para su aprobación. Pues como se ha comentado en el punto anterior, la implementación tiene que ser transversal y tener el apoyo directo de dirección. Enfocando el proyecto no solo como cumplimiento normativo sino también como una oportunidad para reducir esta deuda de privacidad que conllevará beneficios concretos: menor superficie de ataque, menor impacto de incidentes, reducción de costes en caso de migraciones de datos, mayor agilidad para gestionar ejercicios de derechos reduciendo gestión administrativa, mejor preparación ante auditorías para certificaciones enfocadas a la seguridad de la información o privacidad y saneamiento de los datos.



Toni Sansa Aizcorbe
Cybersecurity Expert Consultant

De la estrategia de IA a las operaciones: por qué Seguridad no puede esperar

Tendencias por Isabel Sola

Las organizaciones de todo el mundo están elaborando estrategias de IA. Pero para los equipos de Seguridad está surgiendo una pregunta cada vez más importante: ¿qué necesitamos hacer hoy?

El Global AI Report 2026 de NTT DATA, A Playbook for AI Leaders, señala una brecha creciente entre las organizaciones que experimentan con IA y aquellas que la traducen en valor de negocio medible. Los líderes en IA no tratan la IA como una iniciativa tecnológica aislada. Conectan la estrategia con los procesos, las personas, el gobierno y las formas de trabajo del día a día.

Seguridad desempeña un papel importante para hacer realidad esa transición. Y un ejemplo ya está pasando de la estrategia a las operaciones: la alfabetización en materia de IA.

Por qué la alfabetización en materia de IA no puede esperar

El artículo 4 del Reglamento de IA de la UE es aplicable desde el 2 de febrero de 2025, y las autoridades nacionales de vigilancia del mercado comenzaron a supervisar y exigir el cumplimiento de este requisito el 2 de agosto de 2026. El Ómnibus Digital sobre IA, adoptado recientemente, simplificó la obligación, pero no la eliminó.

Con arreglo al artículo 4 modificado, los proveedores y responsables del despliegue de sistemas de IA deben adoptar medidas para «apoyar el desarrollo de la alfabetización en materia de IA» entre el personal y otras personas que operen o utilicen sistemas de IA en su nombre. La obligación se centra ahora de forma más explícita en adoptar medidas adecuadas, en lugar de garantizar un resultado individual. Pero eso sigue significando que las organizaciones tienen que actuar. Esperar a que se haya diseñado cada componente de un marco corporativo de gobierno de la IA crearía una brecha innecesaria entre la obligación regulatoria y la implantación operativa.

Una paradoja: regulación más flexible, competencias más exigentes

Está surgiendo una tensión interesante en la regulación europea de la IA. En el plano legislativo, la obligación relativa a la alfabetización en materia de IA se ha flexibilizado. A primera vista, esto podría interpretarse como una relajación de las expectativas en torno a las competencias en IA; sin embargo, desde el punto de vista operativo, la evolución va casi en la dirección contraria

A medida que el Reglamento de IA pasa de la legislación a la aplicación práctica, las normas europeas emergentes empiezan a traducir principios regulatorios amplios en las capacidades que las organizaciones necesitan para realizar tareas específicas. Y esas capacidades pueden ser muy exigentes.

Consideremos la gestión de riesgos de IA. No basta con que la persona que realiza una evaluación de riesgos haya completado una introducción general a la IA. Para identificar un uso indebido razonablemente previsible, es necesario comprender cómo funciona el sistema, cómo pueden comportarse los usuarios, el entorno en el que operará y cómo puede interactuar con otros sistemas.

Para estimar la gravedad de un riesgo, es necesario comprender la naturaleza del daño potencial, quién podría verse afectado y en qué condiciones. Para evaluar el riesgo residual, se requiere un conocimiento suficiente de las limitaciones técnicas, los modos de fallo y la eficacia de los controles disponibles.

El riesgo para los derechos fundamentales añade otra dimensión. Evaluar si un sistema de IA puede interferir con derechos protegidos exige conocimientos especializados que pueden ir mucho más allá de la tecnología: comprender las poblaciones afectadas, los principios jurídicos pertinentes y, cuando sea necesario, cómo relacionarse de forma significativa con las partes interesadas y los grupos potencialmente vulnerables.

Esto lleva a una conclusión importante para las organizaciones: una formulación legal más flexible de la alfabetización en materia de IA no implica necesariamente un requisito de competencia organizativa menos exigente.

Convertir una obligación en un programa operativo

El primer paso es establecer una base común.

Las personas que trabajan con IA necesitan comprender algo más que cómo utilizar un chatbot o construir un prompt. Deben entender qué puede y qué no puede hacer la IA de forma fiable, cómo debe gestionarse la información, por qué los resultados requieren una validación adecuada y dónde sigue siendo esencial la responsabilidad humana.

Sin embargo, un analista de Operaciones de Seguridad no necesita necesariamente los mismos conocimientos que un directivo, un desarrollador o un profesional que solo interactúa ocasionalmente con una aplicación habilitada por IA.

Tras este requisito regulatorio existe una oportunidad mayor.

La alfabetización en materia de IA ayuda a las personas a reconocer riesgos como la divulgación inadecuada de información, los resultados poco fiables, la dependencia excesiva de la automatización y el uso indebido de las capacidades de IA. Pero también da a los empleados la confianza necesaria para identificar oportunidades legítimas en las que la IA puede mejorar su trabajo. Esto cambia la posición de Seguridad en la conversación sobre IA.

En lugar de ser la función que interviene al final para aprobar o rechazar una nueva tecnología, Seguridad puede contribuir a crear desde el principio las condiciones para una adopción responsable: usuarios informados, salvaguardas prácticas, supervisión adecuada y una cultura en la que convivan la experimentación y la rendición de cuentas. Así es como se pasa de la estrategia a la operación.

La organización nativa en IA descrita en la investigación de NTT DATA no surgirá únicamente de documentos estratégicos. Se construirá mediante acciones concretas que cambien la forma de trabajar de las personas.

Para Seguridad, la alfabetización en materia de IA es una de esas acciones. La regulación la convierte en un requisito inmediato. Pero su valor real va más allá: la alfabetización en materia de IA convierte la IA responsable, de un principio recogido en las políticas corporativas, en una capacidad operativa cotidiana.



Isabel Sola
Cybersecurity Expert Consultant

Vulnerabilidades

Vulnerabilidad Crítica en Citrix NetScaler ADC y Citrix NetScaler Gateway

Fecha: 27 de septiembre de 2026
CVE: CVE-2026-88771 y 7 más



CVSS: 9.5

CRÍTICA

Descripción

Citrix publicó una serie de 8 vulnerabilidades, todas con una puntuación CVSS 3.1 de más de 7,2.

Destaca el CVE-2026-88771, que permite la ejecución de comandos arbitrarios sin requerir de una autenticación previa. Para explotar esta vulnerabilidad, los atacantes podían introducir contenido malicioso en los *logs* de Citrix mediante el User-Agent de las peticiones.

Al introducir el *payload* codificado en Base64, una mala validación de la entrada provocaba que un componente de Citrix NetScaler lo procesase de forma insegura, permitiendo a un atacante no autenticado ejecutar código remoto.

Solución

Citrix urge a los afectados la actualización a alguna de las siguientes versiones:

- Citrix NetScaler ADC y Citrix NetScaler Gateway 14.1-73.37 y versiones posteriores
- Citrix NetScaler ADC y Citrix NetScaler Gateway 13.1-64.23 y builds posteriores de la versión 13.1
- Citrix NetScaler ADC 14.1-73.37 FIPS y builds posteriroes de la versión 14.1-FIPS
- Citrix NetScaler ADC 13.1-FIPS y 13.1-NDcPP 13.1.37.279 y builds posteriores de las versiones 13.1-FIPS y 13.1-NDcPP

Productos afectados

Las versiones afectadas son:

- Citrix NetScaler ADC y Gateway 14.1 anterior a la 14.1-73.37 y la 13.1 anterior a la 13.1-64.23
- Citrix NetScaler ADC FIPS anterior a la 14.1-73.37 FIPS
- Citrix NetScaler ADC FIPS y NDcPP anterior a la 13.1-37.279

Referencias

- nvd.nist.gov
- support.citrix.com
- www.cert.europa.eu

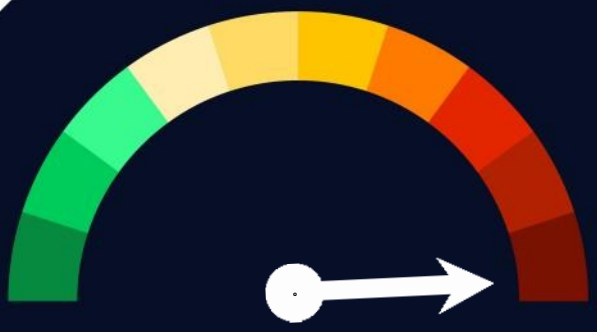
 © Copyright NTT DATA, Inc.

TLP:WHITE

Vulnerabilidades

Path Traversal en FortiMail de Fortinet

Fecha: 01 de octubre de 2026
CVE: CVE-2026-104286



CVSS: 9.8

CRÍTICA

Descripción

Fortinet ha publicado una vulnerabilidad de severidad crítica que, en caso de ser explotada, podría permitir a un atacante remoto no autenticado escribir archivos arbitrarios en el sistema y ejecutar código o comandos no autorizados.

- CVE-2026-104286: Fortinet y CISA han confirmado la explotación activa de esta vulnerabilidad de path traversal en FortiMail. Un atacante remoto no autenticado podría enviar solicitudes HTTP o HTTPS especialmente manipuladas para escribir archivos fuera del directorio previsto. Esto podría permitir ejecutar código o comandos no autorizados y comprometer el dispositivo.

Solución

Desde Fortinet se han proporcionado las siguientes soluciones:

- Actualizar FortiMail a una de las siguientes versiones:
  - 8.0.2 o posterior.
  - 7.6.7 o posterior.
  - 7.4.9 o posterior.
- Los sistemas de la rama 7.2 deben migrarse a FortiMail 7.4.9 o posterior.
- Cuando no sea posible actualizar inmediatamente, Fortinet recomienda deshabilitar la función Identity-Based Encryption (IBE) o restringir el acceso a las interfaces de administración y webmail desde redes de confianza.

Productos afectados

Se han visto afectadas las siguientes versiones de FortiMail:

- 8.0.0 a 8.0.1
- 7.6.0 a 7.6.6
- 7.4.0 a 7.4.8
- 7.2.0 a 7.2.9

Referencias

- incibe.es
- opencve.io

TLP:WHITE

Parche de seguridad de ServiceNow

Fecha: 25 de Septiembre de 2026
CVE: CVE-2026-86857 y 4 más

Crítica

Descripción

El 24 de septiembre, ServiceNow reportó y parcheó varias vulnerabilidades de severidad alta y crítica relacionadas con su plataforma de IA y halladas mediante testeos, reportes y bug bounty sin reportes de explotación activa.

Las vulnerabilidades:

- Bypass de autorización de acceso a usuarios autenticados (CVE-2026-86857).
- Creación, modificación y eliminación de datos sin autenticación (CVE-2026-86858).
- Inyección de código SQL sin autenticación (CVE-2026-13016).
- Bypass de autorización de acceso a usuarios no autenticados (CVE-2026-86859).
- Extracción de datos sin autenticación que pueden dar lugar al escalado de privilegios (CVE-2026-86860).

Productos afectados

Estas vulnerabilidades afectan a las siguientes versiones de la plataforma de IA de ServiceNow:

- ServiceNow Yokohama versiones anteriores al Patch 13 Hot Fix 5a
- ServiceNow Zurich versiones anteriores al Patch 10 Hot Fix 4a W32
- ServiceNow Australia versiones anteriores al Patch 2 Hot Fix 4b W32

Solución

ServiceNow recomienda a los usuarios actualizar a versiones iguales o superiores a ServiceNow Yokohama Patch 13 Hot Fix 5a, ServiceNow Zurich Patch 10 Hot Fix 4a W32 y ServiceNow Australia Patch 2 Hot Fix 4b W32

Referencias

- www.cisecurity.org
- support.servicenow.com

 © Copyright NTT DATA, Inc.

TLP:WHITE

Splunk publica soluciones para 22 vulnerabilidades, 3 de las cuales son críticas

Fecha: 08 de octubre de 2026
CVE: CVE-2026-76268 y 21 más

Crítica

Descripción

Splunk ha publicado soluciones para 22 vulnerabilidades: 3 de severidad crítica, 3 de severidad alta y 16 de severidad media que, en caso de ser explotadas, podrían permitir la ejecución remota de código, la escalada de privilegios, el acceso no autorizado a información, la inyección SQL, Server-Side Request Forgery (SSRF) o provocar una denegación de servicio (DoS).

Aunque el parche está incluido en las actualizaciones propuestas, Splunk indica que las vulnerabilidades CVE-2026-76264, CVE-2026-76265, CVE-2026-76272 y CVE-2026-76280 requieren medidas adicionales, descritas en el boletín del fabricante.

Productos afectados

Las siguientes versiones de Splunk Enterprise se han visto afectadas:

- 10.4.0 a 10.4.2
- 10.2.0 a 10.2.6.
- 10.0.0 a 10.0.9
- 9.4.0 a 9.4.14

También están afectadas las versiones de Splunk Secure Gateway anteriores a 3.10.11, 3.9.25 y 3.8.72 por determinadas vulnerabilidades.

Solución

- Actualizar Splunk Enterprise a una de las siguientes versiones, según la rama utilizada (10.4.3 o posterior; 10.2.7 o posterior; 10.0.10 o posterior; 9.4.15 o posterior).
- Actualizar Splunk Secure Gateway a las versiones 3.10.11, 3.9.25 o 3.8.72, según corresponda.

Referencias

- incibe.es
- splunk.com

 © Copyright NTT DATA, Inc.

TLP:WHITE

Eventos

Barcelona Cybersecurity Congress 2026
3 de noviembre – 5 de noviembre

Barcelona Cybersecurity Congress reunirá en Barcelona a profesionales y líderes del ecosistema de ciberseguridad. La agenda abordará inteligencia artificial aplicada a la seguridad, Zero Trust, seguridad cloud y edge, criptografía poscuántica, protección de la cadena de suministro, resiliencia y respuesta ante incidentes.

Enlace

13th Annual European Cyber Security Conference 2026
4 de noviembre

European Cyber Security Conference reunirá en Bruselas a responsables políticos, líderes empresariales y profesionales de ciberseguridad. El programa abordará regulación europea, NIS2, Cyber Resilience Act, seguridad de la cadena de suministro, resiliencia, inteligencia artificial y cooperación ante nuevas amenazas.

Enlace

Cyber Security World Madrid 2026
4 de noviembre – 5 de noviembre

Cyber Security World Madrid reunirá en Madrid a CISOs, responsables de seguridad y profesionales del sector tecnológico. El evento se centrará en los principales retos de la ciberseguridad empresarial, incluyendo resiliencia, protección frente a amenazas, inteligencia artificial, cloud y transformación digital.

Enlace

European Cyber Week 2026
16 de noviembre - 19 de noviembre

European Cyber Week reunirá en Rennes a organizaciones públicas y privadas, instituciones, investigadores y profesionales de la ciberseguridad y la ciberdefensa. Su programa abordará resiliencia, soberanía digital, inteligencia artificial, nuevas amenazas y cooperación europea en materia de seguridad.

Enlace

XX STIC Conference 2026
24 de noviembre - 27 de noviembre

XX STIC Conference reunirá en Madrid a profesionales del sector público, la industria, la academia y la comunidad de ciberseguridad. La edición 2026 abordará inteligencia artificial ofensiva, amenazas asociadas a la computación cuántica, ciberinteligencia, ciberdefensa, infraestructuras críticas y respuesta ante incidentes.

Enlace

Recursos

➢ ENISA Threat Landscape 2026

Publicado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el informe ofrece una visión actualizada del panorama de ciberamenazas que afecta a la Unión Europea. La edición de 2026 analiza la evolución de amenazas como el ransomware, los ataques a la cadena de suministro y a terceros, el impacto de las dependencias digitales y el creciente uso de inteligencia artificial por parte de actores maliciosos. Además, identifica los sectores más afectados y analiza las principales técnicas y motivaciones observadas en los incidentes registrados.

Enlace

➢ Exactitud, idoneidad y calidad de los datos en tratamientos de datos personales con Inteligencia Artificial

Publicado por la Agencia Española de Protección de Datos (AEPD), este documento aborda la importancia de garantizar la exactitud, idoneidad y calidad de los datos personales utilizados en sistemas de inteligencia artificial. La guía analiza los riesgos que pueden surgir cuando los datos empleados no son adecuados para la finalidad del tratamiento y ofrece criterios para evaluar su calidad a lo largo del ciclo de vida de los sistemas de IA, desde su desarrollo y entrenamiento hasta su utilización.

Enlace

NTT DATA

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com