Número 120 | Novembro 2026

NTT DATA

Radar

A revista de cibersegurança



Privacidade como vantagem competitiva: menos dados, mais confiança, mais negócios

Por Soledad Romero Jiménez

Durante anos, a privacidade foi tratada como uma obrigação: cumprir o Regulamento Geral sobre a Proteção de Dados (RGPD), atualizar políticas, atender aos direitos dos titulares e evitar sanções. Essa abordagem continua necessária, mas já não é suficiente. Em uma economia baseada em dados, inteligência artificial e serviços digitais, a privacidade passa a ter um novo papel, ligado à eficiência, à confiança e à capacidade de inovar.

O verdadeiro risco não está apenas no tratamento inadequado dos dados, mas também em não saber exatamente quais dados temos, por que os mantemos, quem os utiliza, onde são replicados e quando devem ser eliminados. Esse acúmulo silencioso cria uma verdadeira dívida de privacidade. E, assim como acontece com a dívida técnica, quanto mais uma organização demora a enfrentá-la, maiores são os custos e os riscos. A superfície de ataque se amplia, as migrações e auditorias se tornam mais complexas e demoradas, a resposta a incidentes fica mais difícil e a transformação do negócio perde agilidade.

A vantagem competitiva começa justamente quando a organização muda essa lógica. Não se trata de armazenar mais, mas de governar melhor. Saber quais informações geram valor, reduzir aquelas que já não são úteis e automatizar sua retenção, seu bloqueio, sua anonimização ou eliminação permite transformar a privacidade em uma disciplina operacional.

Essa mudança exige liderança. A privacidade não pode ficar restrita ao responsável de proteção de dados (DPO) ou à área jurídica. Direção, Tecnologia, Segurança, Dados, Compras, Recursos Humanos e áreas de negócio devem compartilhar responsabilidades, indicadores e evidências. Um inventário atualizado de sistemas e dados, regras claras de retenção, responsáveis definidos e controles automatizados proporcionam algo muito mais valioso do que uma política bem redigida: a capacidade real de demonstrar como as informações são governadas.

A inteligência artificial torna essa necessidade ainda mais urgente. As organizações estão passando da experimentação com IA para a integração da tecnologia a processos, decisões e operações. Mas não basta implementar ferramentas. É preciso saber utilizá-las. O letramento em IA torna-se, assim, uma capacidade de governança, que envolve compreender o que um sistema pode fazer, quais informações pode receber, em que situações precisa de validação humana, quais riscos apresenta e quais controles devem ser aplicados.

Isso também muda o papel das áreas de Segurança e Privacidade. Em vez de atuarem apenas na etapa final para aprovar ou interromper uma iniciativa, essas áreas podem ajudar a estruturá-la desde o início, com usuários capacitados, dados adequados, permissões limitadas, supervisão, rastreabilidade e limites de segurança práticos. A inovação responsável deixa, então, de ser um princípio abstrato e se torna uma prática cotidiana.

Os benefícios são concretos. No setor financeiro, por exemplo, uma instituição que reduz ao mínimo as informações coletadas, automatiza seu ciclo de vida e estabelece quais dados seus sistemas de IA podem utilizar — de acordo com a finalidade, a sensibilidade e as permissões — reduz a exposição, simplifica as operações e pode inovar com mais rapidez e segurança.

Na área da saúde, a pseudonimização, a segregação de acessos e regras eficazes para o ciclo de vida dos dados permitem reutilizar informações em pesquisas ou análises clínicas, reduzindo a exposição dos dados dos pacientes.

Na administração pública, a verificação seletiva de atributos — por exemplo, a comprovação de uma condição sem a entrega de toda a documentação — pode simplificar trâmites, reduzir o volume de informações armazenadas e aumentar a confiança dos cidadãos nos serviços digitais.

Também existem riscos capazes de comprometer rapidamente essa vantagem: Shadow AI, fornecedores com acesso excessivo, cópias históricas que nunca foram depuradas, dados de teste com informações reais, profissionais sem capacitação ou sistemas legados cujo uso ninguém sabe justificar. E, para as informações que precisam ser mantidas durante anos, surge ainda uma questão estratégica: a criptoagilidade e a preparação para a computação quântica. Proteger dados que permanecerão sensíveis por muitos anos também exige planejar como mantê-los seguros no futuro.

É nesse contexto que a NTT DATA pode oferecer uma visão mais abrangente: desde a identificação e redução da dívida de privacidade até o projeto da governança de dados, inventários e mapeamentos de tratamento, automação da retenção e eliminação, privacidade desde a concepção, governança e letramento em IA, integração com a cibersegurança e planejamento estratégico de criptoagilidade. Não como iniciativas isoladas, mas como capacidades conectadas aos processos, à tecnologia, aos riscos e aos objetivos de negócio.

A conclusão é simples: a privacidade gera vantagem quando deixa de ser tratada como uma questão documental e passa a ser gerida como uma capacidade empresarial. As organizações que conhecem melhor seus dados podem reduzir riscos, operar com mais eficiência, adotar IA com mais segurança e inovar sobre uma base de confiança.

Ter uma privacidade que gera vantagem competitiva não significa acumular mais dados. Significa saber exatamente quais dados devem ser mantidos.



Soledad Romero Jiménez
Consultora especialista em Cibersegurança



A exposição de dados pessoais por meio de novas vias de ataque

Cibercrônica por Nuria Ripoll Cedillo

As recentes violações de segurança mostram diferentes formas de acesso a dados pessoais. As conexões entre organizações, o uso de fornecedores de tecnologia, as solicitações fraudulentas e a incorporação de inteligência artificial aos ataques ampliam as situações em que as informações podem ser expostas.

No fim de setembro, a Renfe (operadora ferroviária pública da Espanha) detectou um acesso não autorizado a determinados sistemas corporativos. A empresa acionou seus protocolos de segurança e iniciou uma investigação para determinar a origem e a extensão do incidente. Em 25 de setembro, os primeiros indícios técnicos apontavam para servidores da Adif (Administrador de Infraestruturas Ferroviárias da Espanha) que haviam sido comprometidos anteriormente e mantinham conexões com sistemas da Renfe.

As investigações iniciais indicaram que os cibercriminosos poderiam ter acessado informações de usuários, principalmente nomes e endereços de e-mail. No entanto, à medida que as verificações avançaram, a Renfe confirmou que o acesso havia atingido determinados sistemas relacionados à venda de passagens e, por isso, notificou as pessoas potencialmente afetadas pelo incidente.

Em seu comunicado, a empresa alertou para a possível exposição de informações de identificação e contato, assim como de determinados dados associados ao uso de seus serviços ferroviários. A Renfe também informou que havia reforçado as medidas de segurança e mantinha a investigação aberta para determinar com precisão quais informações poderiam ter sido comprometidas.

Por sua vez, a **Adif** comunicou que o incidente poderia ter afetado informações pessoais armazenadas em sua plataforma de licitação eletrônica, hospedada em um ambiente externo e gerenciada por um fornecedor de tecnologia. A possível exposição também abrangia informações de seus sistemas corporativos. Ambas as organizações continuaram analisando o incidente e adotando medidas para conter os acessos detectados.

Algumas semanas antes, a **Revolut** (fintech global) havia confirmado outro incidente relacionado à exposição de informações pessoais. Nessa ocasião, os cibercriminosos usaram uma conta de e-mail vinculada ao domínio legítimo de uma agência governamental para enviar solicitações fraudulentas sobre determinados clientes.

As comunicações pareciam vir de uma autoridade oficial e solicitavam informações que normalmente podem ser exigidas no âmbito de investigações administrativas ou judiciais. O uso de um domínio autêntico contribuiu para que as solicitações fossem consideradas legítimas e a Revolut fornecesse informações a terceiros não autorizados.

Entre os dados comprometidos estavam nomes, datas de nascimento, endereços, números de telefone e documentos de identidade, incluindo passaportes e carteiras de habilitação. Em determinados casos, as informações também poderiam incluir fotografias usadas nos processos de verificação, extratos bancários e históricos de transações.

Segundo informações divulgadas posteriormente, a violação afetou aproximadamente 680 clientes, alguns deles envolvidos em operações com criptomoedas. Os responsáveis pelo ataque teriam tentado extorquir a empresa, ameaçando divulgar os dados obtidos. A Revolut confirmou o incidente, entrou em contato com as pessoas afetadas e comunicou o ocorrido às autoridades competentes. A empresa também informou que seus sistemas internos e os recursos financeiros dos clientes permaneciam protegidos.

Essa atividade teria permitido que o agente avançasse por diferentes fases do ataque até conseguir modificar dados pessoais e acessar faturas armazenadas na aplicação. A sequência descrita incluía atividades de reconhecimento, acesso e busca por vulnerabilidades que teriam sido executadas com alto grau de automação.

A AEPD (Agencia Española de Protección de Datos) mantinha o incidente sob análise para determinar as circunstâncias em que ocorreu e sua extensão. As informações divulgadas também não permitiam chegar a conclusões definitivas sobre a intervenção humana durante as diferentes fases do ataque.

Em poucas semanas, esses incidentes mostraram diferentes formas de acesso a informações pessoais. Nos casos da Renfe e da Adif, a investigação se concentrou em sistemas interconectados e plataformas externas; na Revolut, os cibercriminosos conseguiram obter dados por meio de solicitações fraudulentas enviadas de um domínio governamental legítimo; na Belnet, a exploração de uma vulnerabilidade na tecnologia de um fornecedor permitiu copiar comunicações e arquivos; e, no caso notificado à AEPD, um agente de inteligência artificial teria participado de diferentes fases da invasão.

As conexões entre organizações, as dependências tecnológicas, a confiança nas comunicações e a automação dos ataques ampliam as situações em que os dados pessoais podem ser expostos. Os incidentes recentes refletem a importância de manter controles sobre os sistemas, as relações com terceiros e os processos de acesso e compartilhamento de informações.



Nuria Ripoll Cedillo
Consultora em Cibersegurança



Dívida de privacidade: o passivo esquecido da transformação digital

Artigo por Toni Sansa Aizcorbe

Desde a entrada em vigor do Regulamento Geral sobre a Proteção de Dados (RGPD), muitas empresas aprovaram políticas de retenção e eliminação. No entanto, poucas contam com um sistema que permita gerenciar todo o ciclo de vida dos dados de forma automatizada e verificável, desde a coleta até a eliminação, anonimização ou bloqueio.

Esse problema pode ser entendido como uma **dívida de privacidade**, que surge quando uma empresa acumula e armazena dados por tempo indeterminado, sem definir para que precisa dessas informações, por quanto tempo deve mantê-las e como deve eliminá-las. Assim como a manutenção de aplicações obsoletas ou a implementação de soluções rápidas sem uma arquitetura sustentável geram custos futuros, a retenção de dados sem governança e sem prazos para armazenamento e eliminação aumenta progressivamente os riscos, a complexidade e os custos operacionais.

A transformação digital permitiu conhecer melhor os clientes, automatizar processos, personalizar serviços e tomar decisões baseadas em dados. Mas também aumentou consideravelmente o número de sistemas, integrações, soluções SaaS e bancos de dados que armazenam informações pessoais. Os dados são replicados entre departamentos e seus respectivos sistemas. Sem o controle adequado, as organizações acabam acumulando informações cuja origem, finalidade, titularidade ou prazo de retenção já não conseguem explicar.

A dívida de privacidade não é apenas uma questão de conformidade com as normas. Também representa riscos operacionais, financeiros, reputacionais e de cibersegurança. Cada dado armazenado sem necessidade amplia a superfície de ataque em caso de incidente de segurança. Também pode dificultar a realização de auditorias, resultar na falta de evidências, aumentar os custos das migrações tecnológicas ou tornar mais lentas as respostas às solicitações dos titulares de dados.

Portanto, a questão não é apenas saber se uma organização cumpre formalmente o RGPD (Regulamento Geral sobre a Proteção de Dados), mas se consegue demonstrar que gerencia os dados pessoais de forma eficiente e sustentável, além de comprovar essa gestão para além das normas internas elaboradas sobre o tema.

A privacidade precisa estar presente em toda a organização

Um dos erros mais comuns é considerar que a privacidade é responsabilidade exclusiva da área jurídica, da área de conformidade ou do encarregado de proteção de dados. Esses profissionais desempenham um papel essencial, mas não conseguem controlar, sem o apoio de outras áreas, todas as atividades de tratamento de dados realizadas em uma organização.

Os dados pessoais circulam por praticamente todas as áreas. O departamento de Marketing utiliza informações em campanhas e na segmentação de clientes; os profissionais de vendas gerenciam contatos e oportunidades de negócio, coletando e analisando informações; a área de Recursos Humanos trata e armazena dados de funcionários e candidatos; o atendimento ao cliente acessa históricos e registros de ocorrências; e a área financeira mantém dados de faturamento e contratos, entre outros exemplos. Cada decisão, inovação ou nova implementação na empresa pode reduzir ou aumentar a dívida de privacidade.

Por esse motivo, a governança dos dados e sua posterior retenção e eliminação devem envolver toda a organização. A alta direção deve se envolver desde o início e apoiar o projeto de retenção e eliminação de dados, associando-o aos objetivos de negócio, à gestão de riscos e à transformação digital.

Cada departamento deve identificar os dados de que realmente precisa, sua finalidade, sua base legal e seu prazo de retenção. Esse trabalho deve ser realizado em conjunto com o encarregado de proteção de dados ou com o departamento jurídico e com a área de Tecnologia ou Sistemas da empresa, responsável por limitar acessos, aplicar os prazos de retenção, eliminar os dados e gerar evidências desde o início.

O modelo deve funcionar como qualquer outro sistema de controle corporativo, com responsáveis definidos — para isso, recomenda-se elaborar uma matriz RACI de papéis e responsabilidades —, procedimentos documentados, indicadores, revisões periódicas e mecanismos de escalonamento. Caso contrário, a organização pode continuar armazenando dados por inércia e sem controle, o que aumenta os riscos e amplia sem necessidade o impacto de um eventual incidente de segurança.

Ao iniciar um projeto de retenção e eliminação de dados, a regra principal deve ser: **"Se ninguém consegue justificar por que um dado é mantido, quem é responsável por ele e quando deve ser eliminado, esse dado representa uma fonte de risco".**

A privacidade precisa estar presente em toda a organização

Um dos erros mais comuns é considerar que a privacidade é responsabilidade exclusiva da área jurídica, da área de conformidade ou do encarregado de proteção de dados. Esses profissionais desempenham um papel essencial, mas não conseguem controlar, sem o apoio de outras áreas, todas as atividades de tratamento de dados realizadas em uma organização.

Os dados pessoais circulam por praticamente todas as áreas. O departamento de Marketing utiliza informações em campanhas e na segmentação de clientes; os profissionais de vendas gerenciam contatos e oportunidades de negócio, coletando e analisando informações; a área de Recursos Humanos trata e armazena dados de colaboradores e candidatos; o atendimento ao cliente acessa históricos e registros de ocorrências; e a área financeira mantém dados de faturamento e contratos, entre outros exemplos. Cada decisão, inovação ou nova implementação na empresa pode reduzir ou aumentar a dívida de privacidade.

Por esse motivo, a governança dos dados e sua posterior retenção e eliminação devem envolver toda a organização. A alta direção deve se envolver desde o início e apoiar o projeto de retenção e eliminação de dados, associando-o aos objetivos de negócio, à gestão de riscos e à transformação digital. Cada departamento deve identificar os dados de que realmente precisa, sua finalidade, sua base legal e seu prazo de retenção. Esse trabalho deve ser realizado em conjunto com o encarregado de proteção de dados ou com o departamento jurídico e com a área de Tecnologia ou Sistemas da empresa, responsável por limitar acessos, aplicar os prazos de retenção, eliminar os dados e gerar evidências desde o início.

Uma oportunidade para os negócios e a eficiência

A privacidade costuma ser vista como um custo inevitável associado a políticas, contratos, auditorias e possíveis sanções. No entanto, uma boa gestão de dados pessoais também pode se tornar uma vantagem competitiva.

A confiança é cada vez mais relevante no relacionamento com clientes, colaboradores, parceiros e instituições. As pessoas esperam transparência sobre o uso de suas informações, especialmente quando se trata de dados financeiros, profissionais, sensíveis ou relacionados ao comportamento digital. Uma empresa que demonstra coletar apenas os dados necessários, protegê-los adequadamente e facilitar o exercício dos direitos dos titulares transmite maturidade, confiabilidade e responsabilidade.

Reduzir os dados desnecessários também melhora a eficiência econômica. Manter grandes volumes de informações gera custos de armazenamento, licenças, administração, backups, suporte, migrações, auditorias e investigação de incidentes. Eliminar dados sem utilidade operacional ou necessidade legal de retenção permite simplificar os ambientes tecnológicos e reduzir custos.

A qualidade da governança de dados também acelera a inovação. Quando uma organização conhece seus sistemas, mantém inventários atualizados e aplica regras claras de acesso, retenção e reutilização, pode lançar produtos e serviços com mais agilidade. Por outro lado, quando os dados estão dispersos, duplicados ou mal documentados, cada iniciativa exige um trabalho prévio de investigação para localizar as informações, verificar sua qualidade, validar a legitimidade de seu uso e analisar os riscos associados.

Como começar um projeto de retenção e eliminação de dados?

Desde o início, é preciso entender a dimensão do desafio. Realizar uma avaliação de lacunas ou uma auditoria interna específica para identificar a dívida de privacidade é essencial e ajuda a definir um plano de ação realista.

A opção mais recomendada é realizar uma auditoria, que não deve se limitar à revisão de políticas corporativas, cláusulas informativas ou prazos de prescrição para a eliminação dos dados. A auditoria deve confrontar as normas existentes com a realidade operacional e tecnológica. É comum encontrar registros de atividades de tratamento desatualizados, bancos de dados obsoletos ou plataformas de fornecedores que compartilham dados com outros sistemas sem que a organização tenha conhecimento disso.

A auditoria deve responder, com base em evidências, a questões como:

- Quais dados pessoais são tratados.
- Em quais sistemas, locais e ambientes estão armazenados.
- Para qual finalidade foram coletados e qual é sua base legal.
- Quem tem acesso a esses dados e com quais permissões.
- Quais fornecedores ou terceiros estão envolvidos.
- Por quanto tempo os dados devem ser mantidos.
- Quais mecanismos existem para bloquear, anonimizar ou eliminar as informações.
- Em quais ambientes os controles são aplicados, incluindo desenvolvimento, testes, backups e repositórios históricos.

É recomendável que o auditor interno esteja familiarizado com a aplicação do RGPD ou com certificações relacionadas. Caso contrário, recomenda-se buscar assessoria externa especializada para elaborar um plano de auditoria adequado. As lacunas costumam surgir entre o que uma organização declara e o que realmente acontece. Por exemplo, uma política pode prever a eliminação de currículos após determinado período, mas os dados podem permanecer nas caixas de e-mail utilizadas para essa finalidade.

Etapas do projeto de retenção e eliminação de dados

Após a auditoria ou avaliação de lacunas, é necessário estruturar um projeto de retenção e eliminação de dados em etapas e envolver todos os departamentos da empresa que tratam dados pessoais.

Em primeiro lugar, deve-se elaborar um inventário de sistemas com a participação de todas as áreas da empresa. Além do nome de cada ferramenta, o inventário deve incluir seu responsável interno, finalidade, categorias de dados, usuários, integrações, localização, fornecedor, transferências internacionais, medidas de segurança e prazos atuais de retenção, se existirem. Também devem ser definidos processos de eliminação, anonimização ou bloqueio, considerando os recursos disponíveis por padrão nos sistemas próprios ou de terceiros. Na elaboração do inventário, é preciso ter especial atenção aos sistemas legados que têm impacto direto no negócio, inclusive os provenientes da aquisição de uma unidade de negócio, empresa ou grupo corporativo.

Também é necessário avaliar a possibilidade de automatizar os processos de eliminação, anonimização ou bloqueio, priorizando, sempre que possível, os processos automatizados em relação aos manuais e, caso não haja recursos disponíveis, estabelecendo um prazo para sua implementação, mesmo que não seja imediata.

Em seguida, é preciso prever o orçamento e os recursos necessários, além de definir os prazos de início e implementação das etapas do projeto. Nesse sentido, eu adotaria uma estimativa conservadora, sobretudo se a empresa ainda não tiver realizado iniciativas semelhantes ou não estiver familiarizada com o conceito. Além disso, o processo não deve terminar após a implementação: é preciso manter uma etapa permanente de monitoramento e controle dos procedimentos de retenção e eliminação implementados, promovendo melhorias contínuas sempre que possível.

Por fim, o plano deve ser apresentado à direção e, quando necessário, ao conselho de administração da empresa para aprovação. Afinal, como mencionado no tópico anterior, a implementação deve envolver toda a organização e contar com o apoio direto da direção. O projeto deve ser visto não apenas como uma questão de conformidade normativa, mas também como uma oportunidade de reduzir a dívida de privacidade e obter benefícios concretos: uma menor superfície de ataque, menos impacto em caso de incidentes, redução dos custos de migração de dados, mais agilidade para atender às solicitações dos titulares, com menos trabalho administrativo, melhor preparação para auditorias de certificação voltadas à segurança da informação ou à privacidade e saneamento dos dados.



Toni Sansa Aizcorbe
Consultor especialista em Cibersegurança

Da estratégia de IA às operações: por que a área de Segurança não pode esperar

Tendências por Isabel Sola

Organizações em todo o mundo estão elaborando estratégias de IA. Mas uma pergunta se torna cada vez mais importante para as equipes da área de Segurança: o que precisamos fazer hoje?

O Reporte Global de IA 2026 da NTT DATA: o playbook para quem lidera com IA aponta uma lacuna crescente entre as organizações que experimentam a IA e aquelas que a transformam em valor mensurável para o negócio. Os líderes em IA não tratam a tecnologia como uma iniciativa isolada. Eles conectam a estratégia aos processos, às pessoas, à governança e às práticas de trabalho do dia a dia.

A área de Segurança desempenha um papel importante para concretizar essa transição. E um exemplo já está passando da estratégia para as operações: o letramento em IA.

Por que o letramento em IA não pode esperar

O artigo 4º do Regulamento de IA da União Europeia é aplicável desde 2 de fevereiro de 2025, e as autoridades nacionais de fiscalização do mercado começaram a supervisionar e exigir o cumprimento desse requisito em 2 de agosto de 2026. O Pacote Digital sobre IA, adotado recentemente, simplificou a obrigação, mas não a eliminou.

De acordo com o artigo 4º alterado, os fornecedores e responsáveis pela implantação de sistemas de IA devem adotar medidas para "apoiar o desenvolvimento do letramento em IA" entre os profissionais e outras pessoas que operem ou utilizem sistemas de IA em seu nome. A obrigação agora se concentra de forma mais explícita na adoção de medidas adequadas, em vez de garantir um resultado individual. Isso significa que as organizações ainda precisam agir. Esperar até que todos os componentes de um framework corporativo de governança de IA estejam definidos criaria uma lacuna desnecessária entre a obrigação regulatória e sua implementação nas operações.

Um paradoxo: regulamentação mais flexível, competências mais exigentes

Um debate interessante começa a surgir na regulamentação europeia de IA. No âmbito legislativo, a obrigação relativa ao letramento em IA foi flexibilizada. À primeira vista, isso poderia ser interpretado como uma redução das expectativas em relação às competências em IA. Na prática, porém, a evolução segue uma direção quase oposta.

À medida que o Regulamento de IA começa a ser aplicado na prática, as normas europeias em desenvolvimento passam a definir as capacidades necessárias para que as organizações cumpram tarefas específicas, com base nos princípios gerais da regulamentação. E o desenvolvimento dessas capacidades pode ser bastante exigente.

Vejamos a gestão de riscos de IA. Não basta que a pessoa responsável por uma avaliação de riscos tenha concluído uma introdução geral à IA. Para identificar usos indevidos razoavelmente previsíveis, é necessário compreender como o sistema funciona, como os usuários podem se comportar, o ambiente em que ele operará e como poderá interagir com outros sistemas.

Para estimar a gravidade de um risco, é necessário compreender a natureza do possível dano, quem pode ser afetado e em quais condições. Para avaliar o risco residual, é preciso conhecer suficientemente as limitações técnicas, os modos de falha e a eficácia dos controles disponíveis.

O risco aos direitos fundamentais acrescenta outra dimensão. Avaliar se um sistema de IA pode interferir em direitos protegidos exige conhecimentos especializados que podem ir muito além da tecnologia: compreender as populações afetadas, os princípios jurídicos pertinentes e, quando necessário, como estabelecer um diálogo efetivo com os stakeholders e os grupos potencialmente vulneráveis.

Isso leva a uma conclusão importante para as organizações, uma formulação legal mais flexível sobre o letramento em IA não implica necessariamente requisitos menos exigentes para as competências da organização.

Como transformar uma obrigação em um programa operacional

O primeiro passo é estabelecer uma base comum.

As pessoas que trabalham com IA precisam compreender mais do que o uso de um chatbot ou a elaboração de um prompt. Elas devem entender o que a IA pode e não pode fazer de maneira confiável, como as informações devem ser gerenciadas, por que os resultados precisam de validação adequada e em quais situações a responsabilidade humana continua sendo essencial.

No entanto, um analista de Operações de Segurança não precisa necessariamente dos mesmos conhecimentos que um executivo, um desenvolvedor ou um profissional que interage apenas ocasionalmente com uma aplicação que utiliza IA.

Por trás desse requisito regulatório existe uma oportunidade ainda maior.

O letramento em IA ajuda as pessoas a reconhecer riscos como a divulgação inadequada de informações, resultados não confiáveis, dependência excessiva da automação e uso indevido dos recursos de IA. Mas também dá aos profissionais a confiança necessária para identificar oportunidades legítimas de usar a IA para melhorar seu trabalho. Isso muda a posição da área de Segurança na discussão sobre IA.

Em vez de atuar apenas na etapa final para aprovar ou rejeitar uma nova tecnologia, a área de Segurança pode contribuir desde o início para criar as condições necessárias a uma adoção responsável: usuários bem informados, medidas de proteção práticas, supervisão adequada e uma cultura que combine experimentação e responsabilidade. É assim que a estratégia se transforma em ação nas operações.

A organização AI-native descrita na pesquisa da NTT DATA não surgirá apenas de documentos estratégicos. Será construída por meio de ações concretas que mudem a forma de trabalhar das pessoas.

Para a área de Segurança, o letramento em IA é uma dessas ações. A regulamentação torna essa ação uma exigência imediata. Mas seu valor vai além. O letramento em IA transforma a IA responsável, que deixa de ser apenas um princípio das políticas corporativas e passa a fazer parte das operações cotidianas.



Isabel Sola
Consultora especialista em Cibersegurança

Vulnerabilidades

Vulnerabilidade crítica no Citrix NetScaler ADC e no Citrix NetScaler Gateway

Data: 27 de setembro de 2026
CVE: CVE-2026-88771 e mais 7



CVSS: 9.5

CRÍTICA

Descrição

A Citrix divulgou uma série de 8 vulnerabilidades, todas com pontuação CVSS 3.1 superior a 7,2.

Destaca-se a CVE-2026-88771, que permite a execução de comandos arbitrários sem necessidade de autenticação prévia. Para explorar essa vulnerabilidade, os atacantes podiam inserir conteúdo malicioso nos logs da Citrix por meio do campo User-Agent das requisições.

Quando o *payload* codificado em Base64 era inserido, uma validação inadequada da entrada fazia com que um componente do Citrix NetScaler o processasse de forma insegura, permitindo que um atacante não autenticado executasse código remotamente.

Solução

A Citrix recomenda que os usuários afetados atualizem para uma das seguintes versões:

- Citrix NetScaler ADC e Citrix NetScaler Gateway 14.1-73.37 e versões posteriores
- Citrix NetScaler ADC e Citrix NetScaler Gateway 13.1-64.23 e builds posteriores da versão 13.1
- Citrix NetScaler ADC 14.1-73.37 FIPS e builds posteriores da versão 14.1-FIPS
- Citrix NetScaler ADC 13.1-FIPS e 13.1-NDcPP 13.1.37.279 e builds posteriores das versões 13.1-FIPS e 13.1-NDcPP

Produtos afetados

As versões afetadas são:

- Citrix NetScaler ADC e Gateway 14.1 anterior à 14.1-73.37 e 13.1 anterior à 13.1-64.23
- Citrix NetScaler ADC FIPS anterior à 14.1-73.37 FIPS
- Citrix NetScaler ADC FIPS e NDcPP anterior à 13.1-37.279

Referências

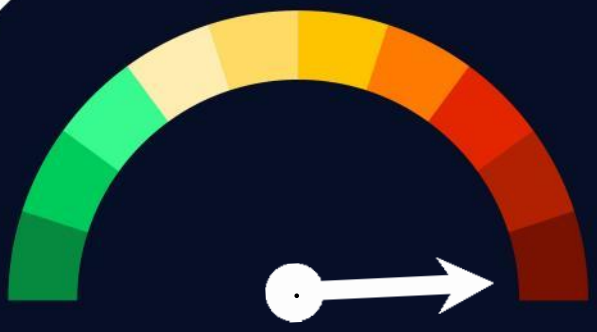
- nvd.nist.gov
- support.citrix.com
- www.cert.europa.eu

 © Copyright NTT DATA, Inc.

Vulnerabilidades

Vulnerabilidade de acesso indevido a diretórios (path transversal) no FortiMail da Fortinet

Data: 1º de outubro de 2026
CVE: CVE-2026-104286



CVSS: 9.8

CRÍTICA

Descrição

A Fortinet divulgou uma vulnerabilidade de gravidade crítica que, se explorada, poderia permitir que um atacante remoto não autenticado gravasse arquivos arbitrários no sistema e executasse códigos ou comandos não autorizados.

- CVE-2026-104286: a Fortinet e a CISA confirmaram a exploração ativa dessa vulnerabilidade de path traversal no FortiMail. Um atacante remoto não autenticado poderia enviar requisições HTTP ou HTTPS especialmente manipuladas para gravar arquivos fora do diretório previsto. Isso poderia permitir a execução de códigos ou comandos não autorizados e comprometer o dispositivo.

Solução

A Fortinet forneceu as seguintes soluções:

- Atualizar o FortiMail para uma das seguintes versões:
  - 8.0.2 ou posterior.
  - 7.6.7 ou posterior.
  - 7.4.9 ou posterior.
- Os sistemas da linha 7.2 devem ser migrados para o FortiMail 7.4.9 ou posterior.
- Quando não for possível atualizar imediatamente, a Fortinet recomenda desabilitar a função Identity-Based Encryption (IBE) ou restringir o acesso às interfaces de administração e webmail a redes confiáveis.

Produtos afetados

As seguintes versões do FortiMail foram afetadas:

- 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

Referências

- incibe.es
- opencve.io

TLP:WHITE

Correção de segurança da ServiceNow

Data: 25 de setembro de 2026
CVE: CVE-2026-86857 e mais 4

Crítica

Descrição

Em 24 de setembro, a ServiceNow comunicou e corrigiu várias vulnerabilidades de gravidade alta e crítica relacionadas à sua plataforma de IA, identificadas por meio de testes, relatos e programas de bug bounty, sem registros de exploração ativa.

As vulnerabilidades:

- Contorno da autorização de acesso por usuários autenticados (CVE-2026-86857).
- Criação, modificação e eliminação de dados sem autenticação (CVE-2026-86858).
- Injeção de código SQL sem autenticação (CVE-2026-13016).
- Contorno da autorização de acesso por usuários não autenticados (CVE-2026-86859).
- Extração de dados sem autenticação que pode levar ao escalonamento de privilégios (CVE-2026-86860).

Produtos afetados

Essas vulnerabilidades afetam as seguintes versões da plataforma de IA da ServiceNow:

- ServiceNow Yokohama em versões anteriores ao Patch 13 Hot Fix 5a
- ServiceNow Zurich em versões anteriores ao Patch 10 Hot Fix 4a W32
- ServiceNow Australia em versões anteriores ao Patch 2 Hot Fix 4b W32

Solução

A ServiceNow recomenda que os usuários atualizem para as versões ServiceNow Yokohama Patch 13 Hot Fix 5a, ServiceNow Zurich Patch 10 Hot Fix 4a W32 e ServiceNow Australia Patch 2 Hot Fix 4b W32 ou posteriores.

Referências

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

 © Copyright NTT DATA, Inc.

TLP:WHITE

Splunk publica correções para 22 vulnerabilidades – 3 críticas

Data: 8 de outubro de 2026
CVE: CVE-2026-76268 e mais 21

Crítica

Descrição

A Splunk publicou correções para 22 vulnerabilidades: 3 de gravidade crítica, 3 de gravidade alta e 16 de gravidade média que, se exploradas, poderiam permitir a execução remota de código, o escalonamento de privilégios, o acesso não autorizado a informações, a injeção de SQL, o Server-Side Request Forgery (SSRF) ou provocar uma negação de serviço (DoS).

Embora a correção esteja incluída nas atualizações propostas, a Splunk informa que as vulnerabilidades CVE-2026-76264, CVE-2026-76265, CVE-2026-76272 e CVE-2026-76280 exigem medidas adicionais, descritas no boletim do fabricante.

Produtos afetados

As seguintes versões do Splunk Enterprise foram afetadas:

- 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

As versões do Splunk Secure Gateway anteriores à 3.10.11, 3.9.25 e 3.8.72 também são afetadas por determinadas vulnerabilidades.

Solução

- Atualizar o Splunk Enterprise para uma das seguintes versões, de acordo com a linha utilizada: 10.4.3 ou posterior; 10.2.7 ou posterior; 10.0.10 ou posterior; 9.4.15 ou posterior.
- Atualizar o Splunk Secure Gateway para as versões 3.10.11, 3.9.25 ou 3.8.72, conforme aplicável.

Referências

- incibe.es
- splunk.com

 © Copyright NTT DATA, Inc.

TLP:WHITE

Eventos

Barcelona Cybersecurity Congress 2026
3 a 5 de novembro

O Barcelona Cybersecurity Congress reunirá em Barcelona profissionais e líderes do ecossistema de cibersegurança. A programação abordará inteligência artificial aplicada à segurança, Zero Trust, segurança em cloud e edge, criptografia pós-quântica, proteção da cadeia de suprimentos, resiliência e resposta a incidentes.

Link

13th Annual European Cyber Security Conference 2026
4 de novembro

A European Cyber Security Conference reunirá em Bruxelas formuladores de políticas públicas, líderes empresariais e profissionais de cibersegurança. O programa abordará a regulamentação europeia, a NIS2, o Cyber Resilience Act, a segurança da cadeia de suprimentos, a resiliência, a inteligência artificial e a cooperação diante de novas ameaças.

Link

Cyber Security World Madrid 2026
4 a 5 de novembro

O Cyber Security World Madrid reunirá em Madri CISOs, responsáveis pela segurança e profissionais do setor de tecnologia. O evento será dedicado aos principais desafios da cibersegurança empresarial, incluindo resiliência, proteção contra ameaças, inteligência artificial, cloud e transformação digital.

Link

European Cyber Week 2026
16 a 19 de novembro

A European Cyber Week reunirá em Rennes organizações públicas e privadas, instituições, pesquisadores e profissionais de cibersegurança e ciberdefesa. A programação abordará resiliência, soberania digital, inteligência artificial, novas ameaças e cooperação europeia em segurança.

Link

XX STIC Conference 2026
24 a 27 de novembro

A XX STIC Conference reunirá em Madri profissionais do setor público, do setor industrial, da academia e da comunidade de cibersegurança. A edição de 2026 abordará inteligência artificial ofensiva, ameaças associadas à computação quântica, ciberinteligência, ciberdefesa, infraestruturas críticas e resposta a incidentes.

Link

Recursos

➢ ENISA Threat Landscape 2026

Publicado pela Agência da União Europeia para a Cibersegurança (ENISA), o relatório oferece uma visão atualizada do cenário de ciberameaças que afeta a União Europeia. A edição de 2026 analisa a evolução de ameaças como ransomware e ataques à cadeia de suprimentos e a terceiros, o impacto das dependências digitais e o uso crescente de inteligência artificial por agentes maliciosos. Além disso, identifica os setores mais afetados e analisa as principais técnicas e motivações observadas nos incidentes registrados.

Link

➢ Exatidão, adequação e qualidade dos dados no tratamento de dados pessoais com inteligência artificial

Publicado pela Agência Espanhola de Proteção de Dados (AEPD), o documento aborda a importância de garantir a exatidão, a adequação e a qualidade dos dados pessoais utilizados em sistemas de inteligência artificial. O guia analisa os riscos que podem surgir quando os dados utilizados não são adequados à finalidade do tratamento e oferece critérios para avaliar sua qualidade ao longo do ciclo de vida dos sistemas de IA, desde o desenvolvimento e o treinamento até a utilização.

Link

NTT DATA

CLIQUE AQUI E SIGA A RADAR

Powered by the cibersegurança NTT DATA team

br.nttdata.com