

Ministério da Justiça e Segurança Pública regulamenta sistema nacional de notificação de violações contra crianças e adolescentes no ambiente digital

05.10.2026 12 minutos de leitura

Profissionais relacionados

Felipe Palhares
Fernanda Villela

Áreas relacionadas

Proteção de Dados e
Cybersecurity

Assuntos

Proteção de Dados e
Cybersecurity ECA Digital

Em resumo

A Portaria MJSP nº 1.312/2026, publicada em 28 de setembro de 2026, regulamenta o Centro Nacional de Proteção à Criança e ao Adolescente (CNCA), da Polícia Federal, e detalha como fornecedores de tecnologia devem notificar, pelo Sistema NIDUS, indícios de violações contra crianças e adolescentes no ambiente digital. Os prazos de envio são de 12 horas, 72 horas ou sete dias, conforme o risco, e o conteúdo deve ser removido de imediato e preservado até a validação pelo CNCA. As obrigações ligadas ao NIDUS serão implementadas em duas etapas, mas os deveres de remoção e preservação já são exigíveis.

Em 28 de setembro de 2026, foi publicada a Portaria do Ministério da Justiça e Segurança Pública nº 1.312/2026 ("Portaria"), que regulamenta o funcionamento do Centro Nacional de Proteção à Criança e ao Adolescente (CNCA). Integrado à Diretoria de Combate a Crimes Cibernéticos da Polícia Federal, o CNCA será responsável pelo recebimento centralizado, validação, triagem e encaminhamento de notificações relacionadas a violações contra crianças e adolescentes no ambiente digital.

A Portaria complementa o regime estabelecido pela Lei nº 15.211/2025, conhecida como ECA Digital, e pelo Decreto nº 12.880/2026, que a regulamenta. Além de estruturar o fluxo de comunicação com as autoridades brasileiras, a norma detalha as obrigações operacionais impostas aos fornecedores de produtos ou serviços de tecnologia da informação que identifiquem indícios de infrações penais e atos infracionais envolvendo exploração, abuso sexual, sequestro, aliciamento, cárcere privado, recrutamento ou cooptação de crianças e adolescentes.

Sistema centralizado de recebimento e tratamento de notificações

As notificações deverão ser encaminhadas por meio do Sistema NIDUS, mantido pela Polícia Federal. O Sistema NIDUS admitirá integração programática por interface de aplicação, acesso por portal web autenticado ou, excepcionalmente, outros meios técnicos autorizados pelo CNCA. Para utilizar o sistema, os fornecedores deverão realizar cadastro prévio, indicando,

entre outras informações, os produtos e serviços disponibilizados no Brasil, os domínios, aplicações ou plataformas abrangidos, o representante legal ou procurador, o ponto de contato técnico e o ponto de contato institucional com as autoridades policiais.

O fornecedor deverá manter suas informações cadastrais atualizadas e comunicar imediatamente eventual comprometimento, uso indevido ou suspeita de uso indevido das credenciais de acesso. A indicação das pessoas naturais responsáveis pela interlocução com a Polícia Federal não implica, por si só, responsabilidade pessoal pelas obrigações do fornecedor, ressalvadas as consequências decorrentes dos atos praticados pelo próprio indicado.

A norma também admite o cumprimento da obrigação por intermédio de central de triagem situada no exterior, desde que a comunicação se refira aos mesmos fatos e as informações correspondentes estejam acessíveis às autoridades brasileiras. Nessa hipótese, os relatórios estrangeiros estarão sujeitos a procedimentos de validação quanto à autenticidade, completude, consistência interna e correspondência com as hipóteses de comunicação obrigatória previstas na regulamentação brasileira.

Prazos diferenciados conforme o risco

A Portaria estabelece três prazos diferentes para o envio das notificações, a partir da confirmação da detecção do conteúdo ou da conduta pelo fornecedor. A comunicação deverá ocorrer em até **12 horas** nas situações que indiquem risco crível, iminente ou em curso. O prazo passa a ser de **72 horas** quando forem identificados indícios de material de violência sexual contra crianças e adolescentes produzidos recentemente, ainda não previamente identificados, ou gerados por meio de ferramenta de captura oferecida pelo próprio fornecedor. Para as demais hipóteses sujeitas à norma, a notificação poderá ser realizada em até **sete dias**.

Os prazos serão contados de forma corrida, incluindo sábados, domingos e feriados. A confirmação da detecção ocorrerá quando o fornecedor, mediante mecanismo automatizado ou revisão humana, constatar indícios de enquadramento nas hipóteses previstas na Portaria. Embora a revisão humana seja admitida, a atividade deverá ser concluída sem demora injustificada e não poderá ser utilizada para postergar o envio da notificação.

Caso surjam novos elementos após a comunicação inicial, o fornecedor poderá apresentar relatório complementar para corrigir informações, acrescentar dados ou solicitar a reclassificação do caso. A complementação deverá estar vinculada ao número de protocolo da notificação original.

Conteúdo dos relatórios de notificação

Os relatórios de notificação de conteúdo deverão reunir as informações disponíveis na arquitetura tecnológica do fornecedor que sejam úteis à compreensão e à apuração do conteúdo ou da conduta reportada. A relação prevista na Portaria inclui, entre outros elementos, tipo, data e hora do incidente, identificação do produto ou serviço afetado, identificadores e dados cadastrais dos usuários envolvidos, endereços IP, portas lógicas, URLs, identificadores de dispositivos, geolocalização, mídias e metadados, histórico

de interações, hashes de arquivos e dados de pagamento ou operações financeiras relacionados à conduta.

Via de regra, a indisponibilidade de uma dessas informações não impedirá necessariamente o envio ou a validação da notificação, desde que o fornecedor não disponha do dado e não possa obtê-lo pelos meios ordinariamente disponíveis em sua arquitetura tecnológica. Contudo, a indicação do tipo do incidente, da data e hora, com o respectivo fuso horário, e dos dados de contato da pessoa ou unidade responsável pelo envio constitui requisito mínimo para a apresentação e a validação da notificação.

A notificação poderá ainda indicar a fonte de detecção, eventual discrepância na idade declarada pelo usuário e as providências já adotadas, como remoção ou preservação do conteúdo, suspensão ou bloqueio de conta e comunicação a central estrangeira. O fornecedor deverá assinalar expressamente a existência de urgência ou de elementos que recomendem tratamento imediato, acompanhada de descrição objetiva dos fatos.

Remoção, preservação e cadeia de custódia

A Portaria reafirma que o fornecedor que identificar conteúdo abrangido pelo dever legal de comunicação deverá promover sua imediata remoção dos ambientes acessíveis aos usuários. Paralelamente, deverá preservar o conteúdo notificado e os registros, dados e demais elementos necessários à apuração dos fatos e à manutenção da cadeia de custódia até a validação do relatório pelo CNCA.

Após a validação, o conteúdo relacionado à exploração ou ao abuso sexual de criança ou adolescente deverá ser definitivamente excluído dos servidores do fornecedor. Permanecerão preservados, contudo, os registros de conexão e de acesso a aplicações, os dados da conta, as informações do usuário, os metadados associados e os demais elementos cuja retenção seja exigida pela legislação aplicável. A autoridade competente poderá solicitar a preservação por prazo superior, desde que especifique a finalidade e o período correspondente.

Esse regime exigirá que os fornecedores conciliem, em seus procedimentos internos, respostas rápidas de remoção com mecanismos tecnicamente seguros de preservação de evidências, controle de acesso, rastreabilidade e documentação das decisões adotadas.

Canais institucionais de notificação

Os fornecedores que disponibilizem funcionalidades de redes sociais ou serviços de mensageria instantânea com canais públicos e abertos deverão manter canal ou interface específica para o recebimento de notificações apresentadas por órgãos legalmente legitimados, incluindo Ministério Público, Defensorias Públicas, autoridades policiais e entidades da sociedade civil habilitadas pela Agência Nacional de Proteção de Dados (ANPD).

A notificação que evidencie violação a direitos de crianças e adolescentes deverá receber tratamento prioritário e, quando cabível, resultar na retirada

imediatamente do conteúdo, independentemente de ordem judicial. Se o caso também estiver compreendido nas hipóteses de comunicação ao Poder Público, o fornecedor deverá encaminhar o respectivo relatório ao CNCA dentro dos prazos previstos na Portaria. Notificações apresentadas pela própria vítima ou por seu representante no canal destinado aos usuários também deverão receber tratamento prioritário.

Proteção de dados e limites da atuação estatal

A Portaria estabelece que sua aplicação não autoriza o monitoramento geral, permanente ou indiscriminado de usuários, conteúdos, comunicações ou serviços digitais, nem amplia as hipóteses legais de acesso estatal a informações protegidas por sigilo, privacidade ou pela legislação de proteção de dados pessoais.

O tratamento dos relatórios deverá observar finalidade, necessidade, proporcionalidade, minimização, segurança da informação, rastreabilidade das operações e preservação da cadeia de custódia. O acesso será restrito aos agentes públicos diretamente envolvidos, mediante controle individualizado e registro auditável. Também é vedada a divulgação de dados pessoais de crianças ou adolescentes identificados nos relatórios, ressalvadas as hipóteses estritamente necessárias à investigação, ao encaminhamento protetivo ou à adoção de medidas de proteção.

A norma proíbe ainda o envio, aos órgãos do Sistema de Garantia dos Direitos da Criança e do Adolescente, de conteúdo que retrate violência sexual. Quando indispensável para a avaliação do risco ou a adoção de medidas protetivas, admite-se apenas sua descrição sumária.

Fiscalização e responsabilização

O descumprimento das obrigações de comunicação, inclusive em relação à forma, ao conteúdo e aos prazos estabelecidos pela Portaria, poderá sujeitar o fornecedor às penalidades previstas no ECA Digital, assegurado o devido processo legal. Falhas isoladas ou residuais, inerentes ao estado da técnica e à natureza da operação, não serão caracterizadas como descumprimento.

Por outro lado, ocorrências que indiquem falhas recorrentes ou sistêmicas nos mecanismos de moderação poderão ser comunicadas às autoridades competentes, inclusive à ANPD, acompanhadas dos registros de rastreabilidade do Sistema NIDUS. A disciplina reforça, portanto, a importância de mecanismos de governança capazes de demonstrar não apenas a existência de controles, mas também sua efetividade e operação contínua.

Implementação escalonada

Embora a Portaria tenha entrado em vigor na data de sua publicação, as obrigações relacionadas ao Sistema NIDUS serão implementadas em duas etapas. Na primeira, será disponibilizado o sistema para cadastro e credenciamento dos fornecedores. O ato inaugural deverá ser publicado em

até 30 dias da data de publicação da Portaria no Diário Oficial da União, e os fornecedores terão até 60 dias, contados da publicação do ato, para concluir o cadastro.

Na segunda etapa, a Polícia Federal disponibilizará as funcionalidades destinadas ao recebimento dos relatórios. O ato correspondente deverá ser publicado em até 90 dias após o encerramento do prazo de cadastro, e os fornecedores terão até 120 dias, contados da publicação desse segundo ato, para cumprir as obrigações relativas aos prazos, ao conteúdo e ao envio dos relatórios.

A implementação escalonada, contudo, não suspende nem posterga as obrigações de remoção e preservação de conteúdo, que permanecem exigíveis nos termos do ECA Digital e da legislação aplicável. A Polícia Federal também deverá publicar guias de cadastro e integração e regulamento técnico com os requisitos operacionais, padrões de integração e especificações do Sistema NIDUS.

Pontos principais

O que é o CNCA e qual o seu papel segundo a Portaria MJSP nº 1.312/2026?

Em 28 de setembro de 2026, foi publicada a Portaria do Ministério da Justiça e Segurança Pública nº 1.312/2026 ("Portaria"), que regulamenta o funcionamento do Centro Nacional de Proteção à Criança e ao Adolescente (CNCA). Integrado à Diretoria de Combate a Crimes Cibernéticos da Polícia Federal, o CNCA será responsável pelo recebimento centralizado, validação, triagem e encaminhamento de notificações relacionadas a violações contra crianças e adolescentes no ambiente digital.

Quais fornecedores de tecnologia estão sujeitos às obrigações de notificação da Portaria?

Além de estruturar o fluxo de comunicação com as autoridades brasileiras, a norma detalha as obrigações operacionais impostas aos fornecedores de produtos ou serviços de tecnologia da informação que identifiquem indícios de infrações penais e atos infracionais envolvendo exploração, abuso sexual, sequestro, aliciamento, cárcere privado, recrutamento ou cooptação de crianças e adolescentes.

Qual é o prazo para notificar violações contra crianças e adolescentes ao CNCA?

A Portaria estabelece três prazos diferentes para o envio das notificações, a partir da confirmação da detecção do conteúdo ou da conduta pelo fornecedor. A comunicação deverá ocorrer em até 12 horas nas situações que indiquem risco crível, iminente ou em curso. O prazo passa a ser de 72 horas quando forem identificados indícios de material de violência sexual contra crianças e adolescentes produzidos recentemente, ainda não previamente identificados, ou gerados por meio de ferramenta de captura oferecida pelo próprio fornecedor. Para as demais hipóteses sujeitas à norma, a notificação poderá ser realizada em até sete dias. Os prazos serão contados de forma corrida, incluindo sábados, domingos e feriados.

Quais informações são obrigatórias no relatório de notificação enviado ao CNCA?

A relação prevista na Portaria inclui, entre outros elementos, tipo, data e hora do incidente, identificação do produto ou serviço afetado, identificadores e dados cadastrais dos usuários envolvidos, endereços IP, portas lógicas, URLs, identificadores de dispositivos, geolocalização, mídias e metadados, histórico de interações, hashes de arquivos e dados de pagamento ou operações financeiras relacionados à conduta. Via de regra, a indisponibilidade de uma dessas informações não impedirá necessariamente o envio ou a validação da notificação, desde que o fornecedor não disponha do dado e não possa obtê-lo pelos meios ordinariamente disponíveis em sua arquitetura tecnológica. Contudo, a indicação do tipo do incidente, da data e hora, com o respectivo fuso horário, e dos dados de contato da pessoa ou unidade responsável pelo envio constitui requisito mínimo para a apresentação e a validação da notificação.

Como devem ser feitas a remoção e a preservação do conteúdo notificado?

A Portaria reafirma que o fornecedor que identificar conteúdo abrangido pelo dever legal de comunicação deverá promover sua imediata remoção dos ambientes acessíveis aos usuários. Paralelamente, deverá preservar o conteúdo notificado e os registros, dados e demais elementos necessários à apuração dos fatos e à manutenção da cadeia de custódia até a validação do relatório pelo CNCA. Após a validação, o conteúdo relacionado à exploração ou ao abuso sexual de criança ou adolescente deverá ser definitivamente excluído dos servidores do fornecedor. Permanecerão preservados, contudo, os registros de conexão e de acesso a aplicações, os dados da conta, as informações do usuário, os metadados associados e os demais elementos cuja retenção seja exigida pela legislação aplicável.

A Portaria autoriza o monitoramento geral de usuários ou amplia o acesso estatal a dados protegidos?

A Portaria estabelece que sua aplicação não autoriza o monitoramento geral, permanente ou indiscriminado de usuários, conteúdos, comunicações ou serviços digitais, nem amplia as hipóteses legais de acesso estatal a informações protegidas por sigilo, privacidade ou pela legislação de proteção de dados pessoais.

O que acontece se o fornecedor descumprir as obrigações de comunicação da Portaria?

O descumprimento das obrigações de comunicação, inclusive em relação à forma, ao conteúdo e aos prazos estabelecidos pela Portaria, poderá sujeitar o fornecedor às penalidades previstas no ECA Digital, assegurado o devido processo legal. Falhas isoladas ou residuais, inerentes ao estado da técnica e à natureza da operação, não serão caracterizadas como descumprimento.

Quando as obrigações do Sistema NIDUS passam a ser exigidas dos fornecedores?

Embora a Portaria tenha entrado em vigor na data de sua publicação, as obrigações relacionadas ao Sistema NIDUS serão implementadas em duas etapas. Na primeira, será disponibilizado o sistema para cadastro e

credenciamento dos fornecedores. O ato inaugural deverá ser publicado em até 30 dias da data de publicação da Portaria no Diário Oficial da União, e os fornecedores terão até 60 dias, contados da publicação do ato, para concluir o cadastro. Na segunda etapa, a Polícia Federal disponibilizará as funcionalidades destinadas ao recebimento dos relatórios. O ato correspondente deverá ser publicado em até 90 dias após o encerramento do prazo de cadastro, e os fornecedores terão até 120 dias, contados da publicação desse segundo ato, para cumprir as obrigações relativas aos prazos, ao conteúdo e ao envio dos relatórios. A implementação escalonada, contudo, não suspende nem posterga as obrigações de remoção e preservação de conteúdo, que permanecem exigíveis nos termos do ECA Digital e da legislação aplicável.

Profissionais que aliam visão jurídica e visão de mercado



Felipe Palhares



Fernanda Villela