

Plano de resposta a incidentes

Hineh Tecnologia Ltda · CNPJ 69.280.849/0001-62

Versão 1.1 · 8 de outubro de 2026

Aprovação e última revisão: 10/10/2026 · Direção da Hineh

Próxima revisão: até 10/10/2027 ou antes, em caso de mudança relevante.

Edição pública: 10/10/2026

[Consultar a versão no site da Hineh](#)

Este plano estabelece como a Hineh identifica, registra, contém, investiga e encerra incidentes de segurança da informação, e como comunica os incidentes que envolvam dados pessoais.

Aplica-se aos produtos e serviços da Hineh, incluindo projetos de transcrição de áudio, processamento de imagens e integração com serviços externos, abrangendo equipamentos, contas, infraestrutura, software e fornecedores, assim como os sócios, profissionais e terceiros que tenham acesso a essas informações.

Incidente de segurança é qualquer evento confirmado ou com indícios razoáveis que comprometa a confidencialidade, a integridade ou a disponibilidade de informações ou sistemas sob responsabilidade da Hineh. Incidente com dados pessoais é aquele que afeta dados pessoais tratados pela Hineh como controladora ou como operadora. A suspeita deve seguir este plano desde o primeiro sinal, sem aguardar a confirmação.

1 Papéis e acionamento

Funções

O responsável por incidentes coordena a resposta, decide as medidas de contenção e conduz a investigação técnica. A função de privacidade avalia os dados pessoais e os titulares envolvidos e prepara as comunicações exigíveis. O responsável pelo relacionamento com cada cliente mantém a comunicação com seus contatos designados. A direção decide sobre recursos, comunicações externas e, quando a Hineh for controladora, sobre as notificações à autoridade e aos titulares.

Essas funções podem ser exercidas pela mesma pessoa em uma equipe pequena. Cada função deve ter um substituto designado, e a indisponibilidade de uma pessoa transfere suas atribuições ao substituto, sem interromper a contagem dos prazos. A designação nominal, os contatos de cada função e os contatos de incidente de cada cliente e fornecedor devem constar de registro interno atualizado, com ao menos um meio de contato que não dependa do e-mail corporativo.

Como relatar

Sócios, profissionais e prestadores devem relatar qualquer suspeita imediatamente ao responsável por incidentes e ao seu substituto, pelo canal interno já utilizado pela equipe. Clientes, usuários, fornecedores e outras pessoas podem relatar incidentes ou vulnerabilidades pelo endereço privacidade@hineh.com.br. Se houver suspeita de comprometimento do e-mail ou da conta utilizada, o relato deve seguir pelo contato alternativo previsto no registro interno.

A Hineh não mantém equipe de monitoramento em regime contínuo. Alertas automáticos de segurança devem ser direcionados aos responsáveis por um meio que permita ação imediata em

eventos críticos. Os prazos deste plano contam a partir da ciência, isto é, do momento em que um sócio ou profissional da Hineh toma conhecimento do relato ou do alerta.

2 Registro e triagem

O primeiro relato deve abrir um registro com identificador, data e hora da ciência com fuso horário, origem do relato, serviços e ativos envolvidos, sintomas observados, classificação inicial, responsável e evidências disponíveis. O registro deve ser atualizado durante toda a resposta e mantido em local de acesso restrito.

A triagem deve ocorrer em até quatro horas da ciência. Ela confirma se há um incidente, define a classificação, identifica os serviços afetados e determina se a Hineh atua como controladora ou como operadora dos dados envolvidos, o que define o fluxo de comunicação da seção 5. Eventos críticos exigem contenção imediata, mesmo antes da conclusão da triagem.

Os incidentes são classificados conforme o impacto conhecido:

Crítico: vazamento de dados em curso, comprometimento de acesso administrativo, ransomware ou indisponibilidade ampla de um serviço.

Alto: acesso indevido confirmado a dados ou sistemas, ou indisponibilidade relevante de um serviço.

Moderado: suspeita delimitada, sem dano confirmado, que exija investigação.

Baixo: evento bloqueado pelos controles existentes, sem indício de comprometimento.

A classificação deve ser revista sempre que surgirem novos fatos. Eventos que não configurem incidente devem ser encerrados com o registro da justificativa.

3 Contenção e preservação de evidências

A contenção deve adotar a menor medida eficaz para interromper o dano: revogar tokens e chaves, encerrar sessões, suspender contas, desconectar integrações, bloquear exportações, interromper processamentos ou isolar equipamentos. Credenciais possivelmente expostas devem ser revogadas, e não apenas monitoradas. Mudanças emergenciais devem seguir o procedimento autorizado, com as aprovações, validações e registros aplicáveis. A urgência não autoriza contornar as proteções operacionais.

Antes de alterações que possam apagá-las, devem ser preservadas as evidências necessárias à investigação: logs, configurações, alertas e a cronologia dos fatos. Registros sujeitos a retenção curta devem ser copiados para área restrita assim que o incidente for aberto, como exceção registrada às regras de retenção da Hineh, limitada à necessidade da investigação. O registro deve indicar quem coletou e acessou cada evidência, quando e com qual verificação de integridade.

Evidências devem ser armazenadas em ambiente corporativo aprovado, com acesso restrito. Não devem ser enviadas por canais abertos nem copiadas para equipamentos não autorizados ou serviços pessoais. O acesso por equipamento próprio autorizado para uso profissional deve respeitar os controles de segurança e as restrições de cópia e download aplicáveis ao serviço. O acionamento do suporte de fornecedores deve utilizar identificadores técnicos e o mínimo de

dados pessoais necessário. Não se deve restaurar sistemas sobre a única cópia disponível de uma evidência.

4 Avaliação de dados pessoais

Quando houver possibilidade de envolvimento de dados pessoais, a função de privacidade deve avaliar, com o responsável por incidentes:

1. Os serviços, as categorias de dados e os titulares afetados, incluindo pessoas que apareçam de forma incidental em imagens ou gravações.
2. O volume estimado de registros e de titulares.
3. A presença de dados sensíveis, dados de crianças, adolescentes ou idosos, dados financeiros, dados de autenticação, dados protegidos por sigilo ou tratamento em larga escala.
4. A possibilidade de dano material, moral, discriminatório ou reputacional, de fraude ou de uso indevido de identidade.
5. As proteções que reduzam o risco, como criptografia ou pseudonimização eficazes, e a efetividade da contenção.

A avaliação deve registrar sua conclusão e a justificativa, inclusive quando concluir pela ausência de risco ou dano relevante. As incertezas devem ser registradas e reavaliadas à medida que a investigação avançar. A conclusão da perícia técnica não deve ser aguardada para iniciar essa avaliação.

5 Comunicação

Quando a Hineh atua como operadora

A Hineh deve comunicar ao cliente controlador, sem demora injustificada, o incidente que envolva ou possa afetar dados tratados em seu nome. O aviso deve ocorrer no prazo contratado ou, na ausência de prazo específico, em até 24 horas da ciência. A informação inicial pode ser parcial; a Hineh não deve aguardar a certeza sobre toda a extensão do incidente para comunicá-lo.

O aviso deve ser enviado aos contatos designados pelo cliente e conter os elementos da seção 8. Enquanto houver impacto relevante, a Hineh deve atualizar o cliente ao menos diariamente ou na periodicidade acordada. Deve também preservar os registros e prestar as informações necessárias para que o controlador avalie e realize suas próprias comunicações.

A comunicação à Autoridade Nacional de Proteção de Dados e aos titulares é atribuição do controlador. A Hineh não contata titulares nem divulga o incidente por iniciativa própria, salvo instrução do cliente ou obrigação legal.

Quando a Hineh atua como controladora

Se a avaliação concluir que o incidente pode acarretar risco ou dano relevante aos titulares, a Hineh deve comunicá-lo à Autoridade Nacional de Proteção de Dados e aos titulares afetados em até três dias úteis da ciência de que o incidente afetou dados pessoais. A comunicação pode ser preliminar e complementada de forma fundamentada nos prazos regulamentares.

A comunicação aos titulares deve usar linguagem simples e ser feita de forma direta e individual sempre que possível, informando o ocorrido, os dados envolvidos, os riscos, as medidas adotadas, as providências recomendadas e o canal de contato. A decisão de comunicar ou de não comunicar deve ser tomada pela direção com base na avaliação da seção 4 e registrada com sua justificativa.

Fornecedores e comunicações públicas

Incidentes ocorridos em fornecedores seguem o mesmo fluxo. A ciência conta a partir do momento em que a Hineh recebe o aviso do fornecedor ou identifica o incidente por outro meio. A Hineh deve solicitar ao fornecedor as informações necessárias à avaliação e à comunicação aos clientes.

Comunicações públicas sobre incidentes dependem de decisão da direção e, quando envolverem dados de cliente, de coordenação prévia com o controlador. Informações sobre o incidente não devem ser compartilhadas além das pessoas e organizações que precisem delas para a resposta.

6 Erradicação, recuperação e encerramento

A resposta deve eliminar a causa do incidente: corrigir a vulnerabilidade explorada, substituir segredos e credenciais e revisar as permissões envolvidas. A restauração deve partir de uma cópia íntegra, em ambiente isolado quando possível, e reaplicar as exclusões de dados pendentes antes da liberação. O serviço só deve ser reaberto após verificação de integridade e segurança e autorização do responsável por incidentes.

Após a recuperação, os sistemas afetados devem ser monitorados para identificar a reincidência. Impactos residuais devem ser informados aos clientes e titulares que tenham recebido comunicação sobre o incidente.

O incidente é encerrado quando a contenção estiver concluída, a causa tiver sido corrigida ou o risco remanescente estiver aceito com registro, as comunicações devidas tiverem sido realizadas e o registro estiver completo. Para incidentes críticos e altos, a Hineh deve produzir em até cinco dias úteis após a estabilização uma análise inicial com a cronologia, a causa identificada ou as hipóteses em apuração, os controles envolvidos e as ações corretivas, com responsáveis e prazos. Informações ainda pendentes, inclusive de fornecedores, devem ter responsável e previsão de atualização registrados. A análise deve ser complementada à medida que a investigação avançar, sem adiar as comunicações devidas. Para incidentes moderados e baixos, o próprio registro deve conter a causa e as medidas adotadas.

7 Registros e guarda

O registro de cada incidente deve permitir identificar o que ocorreu, quando a Hineh tomou ciência, quem decidiu cada medida, quais dados e titulares foram afetados, quais comunicações foram realizadas ou dispensadas e com qual justificativa, e quais correções foram adotadas.

Registros de incidentes que envolvam dados pessoais devem ser mantidos por no mínimo cinco anos a partir de sua criação, inclusive quando não houver comunicação à autoridade ou aos titulares. Os demais registros de incidentes seguem os prazos de guarda dos registros de governança da Hineh.

O registro deve conter o mínimo de dados pessoais necessário à sua finalidade. Cópias de evidências que contenham dados pessoais ou conteúdo de clientes devem ser eliminadas quando deixarem de ser necessárias à investigação, à cooperação com o controlador ou ao exercício regular de direitos, permanecendo no registro apenas sua descrição e verificação de integridade.

8 Aviso inicial ao cliente

O aviso inicial ao cliente deve conter, conforme as informações disponíveis:

1. Identificador do incidente, data e hora da ciência.
2. Serviços e sistemas afetados.
3. Fatos confirmados e pontos ainda sob investigação.
4. Natureza dos dados e categorias de titulares potencialmente envolvidos, com a dimensão estimada.
5. Medidas de contenção já adotadas e próximas etapas.
6. Recomendações imediatas ao cliente, quando houver.
7. Responsável pelo contato e horário previsto da próxima atualização.

O aviso não deve afirmar a ausência de risco antes da conclusão da avaliação. Conteúdo sensível deve ser transmitido por canal seguro acordado com o cliente.

9 Preparação e revisão

O registro interno de contatos deve ser revisado sempre que houver mudança na equipe, nos clientes ou nos fornecedores, e ao menos a cada seis meses. A Hineh deve realizar um exercício de resposta a incidentes ao menos anualmente e sempre que houver mudança relevante nos serviços ou nos papéis, ou quando previsto em contrato. O exercício deve usar cenário fictício, sem dados reais, e registrar participantes, tempos, decisões, falhas e ações corretivas.

A direção deve revisar este plano ao menos anualmente, após incidentes críticos ou altos e quando houver mudança relevante nos serviços, nos riscos ou nas obrigações aplicáveis. Alterações devem receber versão e data e ser comunicadas às pessoas responsáveis por sua execução.

Este plano observa a Lei nº 13.709/2018, especialmente as regras de segurança e de comunicação de incidentes, e a Resolução CD/ANPD nº 15/2024, que aprova o Regulamento de Comunicação de Incidente de Segurança.