

# Política de segurança da informação

Hineh Tecnologia Ltda · CNPJ 69.280.849/0001-62

Versão 1.1 · 9 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](#)

Esta política estabelece as regras e as responsabilidades da Hineh para proteger as informações da empresa e de seus clientes e descreve as práticas de segurança adotadas em sua operação. Aplica-se aos produtos e serviços da Hineh, incluindo projetos de transcrição de áudio, processamento de imagens e integração com serviços externos, abrangendo informações, contas, equipamentos, infraestrutura, software e fornecedores.

O cumprimento desta política é obrigatório para sócios, colaboradores, prestadores de serviço e terceiros que tenham acesso a informações ou sistemas da Hineh. Neste documento, profissionais são os sócios, colaboradores e prestadores de serviço. Terceiros ficam sujeitos a estas regras ou a requisitos equivalentes previstos em contrato.

Esta política é complementada pelos Procedimentos de proteção de dados e terceiros, pelo Plano de resposta a incidentes, pelo Manual de operação e desenvolvimento seguro e pelo Plano de backup, continuidade e recuperação.

## 1 Governança e responsabilidades

A direção aprova esta política, assegura os recursos necessários à sua aplicação e decide sobre exceções e riscos residuais. O responsável pela segurança da informação coordena a aplicação desta política e a execução dos controles. O responsável por cada serviço aplica estas regras ao serviço sob sua gestão e mantém os registros correspondentes.

Essas funções podem ser exercidas pela mesma pessoa em uma equipe pequena. Cada função deve ter um substituto designado, e a designação nominal deve constar de registro interno atualizado.

Cada profissional deve conhecer e cumprir esta política, proteger suas credenciais e equipamentos, utilizar as informações somente para as finalidades autorizadas e relatar imediatamente qualquer suspeita de incidente. A política deve ser apresentada a cada profissional antes da liberação de acesso, com registro de sua ciência, e as novas versões devem ser comunicadas às pessoas responsáveis por sua execução.

O descumprimento desta política será apurado de forma proporcional e pode resultar na suspensão ou revogação de acessos e nas medidas contratuais e legais cabíveis.

## 2 Classificação e uso das informações

As informações são classificadas como públicas, internas, confidenciais ou restritas. Informações de clientes são confidenciais. Credenciais, chaves, dados pessoais sensíveis e arquivos de incidentes são restritos. O proprietário da informação define sua finalidade, seus destinatários e sua retenção.

O compartilhamento de informações deve usar repositório corporativo autorizado, com acesso nominal e prazo, quando aplicável. O armazenamento em nuvem deve manter o bloqueio de acesso público, e os arquivos de aplicações web são servidos por rede de distribuição com acesso restrito à origem.

É proibido copiar conteúdo de clientes para e-mail pessoal, nuvem pessoal, aplicativo de mensagens não aprovado, repositório público, ferramenta de inteligência artificial de consumo ou mídia removível sem autorização formal e proteção equivalente.

Conteúdo de clientes, tokens, senhas e dados pessoais desnecessários não devem ser incluídos em tickets, logs, testes, documentação ou capturas de tela.

## 3 Gestão de acessos

O acesso a sistemas e informações segue o princípio do menor privilégio: todo acesso humano deve ser nominal, justificado, aprovado e limitado às permissões necessárias à atividade, pelo prazo necessário. O perfil concedido para um cliente não deve permitir a consulta de dados de outros clientes.

A concessão de acesso segue as etapas abaixo:

1. Solicitação com identificação da pessoa ou do serviço, do sistema, do perfil, da justificativa e do prazo, quando temporário.
2. Aprovação pelo responsável pelo serviço ou pela informação.
3. Concessão do perfil mínimo, por conta nominal e com autenticação conforme a seção 4.
4. Registro no inventário de acessos.

Contas compartilhadas são proibidas. O acesso administrativo exige justificativa distinta do acesso operacional. Acesso emergencial é temporário, registrado e revisado no dia útil seguinte.

Os serviços usam papéis de execução ou credenciais específicas de serviço, com responsável e escopo definidos. As credenciais de serviço ficam no cofre de segredos do provedor de nuvem.

O responsável pela segurança da informação deve revisar os acessos ao menos trimestralmente e sempre que houver mudança de função, remover as permissões desnecessárias e registrar o resultado.

No desligamento ou no término da atuação de um profissional em um serviço, os acessos devem ser revogados imediatamente após a comunicação, com bloqueio das contas, encerramento das sessões, remoção de grupos, revogação de tokens e avaliação da rotação dos segredos conhecidos pela pessoa. A revogação deve ser registrada com data e hora e não depende da conclusão da devolução de equipamentos ou informações.

## 4 Autenticação e MFA

O acesso humano a sistemas da Hineh deve usar conta individual e autenticação multifator (MFA). O MFA é obrigatório no e-mail corporativo, no provedor de nuvem, no banco de dados gerenciado, na organização de repositórios de código e nas interfaces administrativas. Solicitações de MFA inesperadas não devem ser aprovadas.

O acesso ao provedor de nuvem deve ocorrer por login único corporativo (SSO), com MFA e sessões temporárias, sem chaves de acesso permanentes pessoais. Cada pessoa deve usar sua própria credencial de banco de dados. Logins pessoais, senhas e arquivos de configuração com credenciais não podem ser compartilhados.

A suspeita de exposição de uma credencial exige troca imediata e relato conforme a seção 11. Identidades de serviço não usam MFA humano e seguem os controles da seção 3.

## 5 Equipamentos e dispositivos pessoais

O uso de equipamento pessoal (BYOD) em atividades profissionais é permitido somente após cadastro, aceite de uso profissional e cumprimento dos requisitos desta seção. Sistemas sem suporte, dispositivos de terceiros e dispositivos com integridade comprometida são proibidos.

Antes de acessar sistemas ou informações da Hineh e de seus clientes, o equipamento deve ser registrado no inventário e atender aos requisitos abaixo, que devem ser mantidos durante todo o uso:

1. Sistema operacional com suporte vigente e atualizações de segurança do sistema e do navegador aplicadas.
2. Antivírus ou EDR ativo.
3. Firewall do sistema operacional habilitado.
4. Criptografia do disco.
5. Bloqueio automático da tela após, no máximo, cinco minutos de inatividade.
6. Conta de usuário individual, sem compartilhamento da sessão profissional com outras pessoas.

O cumprimento dos requisitos deve ser verificado no registro do equipamento e nas conferências periódicas previstas no Manual de operação e desenvolvimento seguro.

Dados de clientes não podem ser sincronizados com armazenamento pessoal. Ao término da atuação, as cópias autorizadas devem ser excluídas de forma verificável e os acessos revogados.

Equipamentos perdidos, infectados ou fora dos requisitos devem ser desconectados dos acessos corporativos até a regularização, sem que dados pessoais do proprietário sejam apagados sem autorização e fundamento. A perda ou a suspeita de comprometimento deve ser relatada imediatamente como incidente.

## 6 Acesso remoto e rede

O acesso remoto a sistemas da Hineh e de clientes deve ocorrer por canais criptografados, como HTTPS com TLS ou VPN, com autenticação individual e MFA conforme a seção 4. Redes Wi-Fi abertas não dispensam o canal protegido.

Os serviços de backend em produção são executados em sub-redes privadas, sem IP público, e recebem requisições da internet somente pelo balanceador HTTPS.

O acesso a redes e sistemas privados de clientes deve ocorrer somente pelo canal explicitamente autorizado pelo cliente, como VPN ou identidade de serviço. Integrações entre sistemas devem usar API autenticada por HTTPS, com credencial dedicada.

## 7 Criptografia e gestão de segredos

Informações confidenciais e restritas devem ser protegidas por criptografia em trânsito e em repouso:

1. Em trânsito: os pontos de entrada públicos usam HTTPS com TLS 1.2 ou superior, e as conexões com o banco de dados usam TLS.
2. Em repouso: o armazenamento de objetos, o banco de dados gerenciado, as cópias de segurança e o cofre de segredos são criptografados pelo provedor. Os registros de acesso às aplicações usam chave gerenciada no serviço de chaves do provedor de nuvem.
3. Em equipamentos: os discos devem ser criptografados, conforme a seção 5.

O acesso às chaves de criptografia deve ser controlado e restrito às identidades que delas precisam.

Segredos, como senhas de serviço, tokens e chaves de API, ficam no cofre de segredos do provedor de nuvem ou na configuração protegida do pipeline de integração contínua e não podem constar do código-fonte ou do repositório, nem de tickets, logs, testes ou documentação. Um segredo exposto deve ser revogado e substituído imediatamente, e o evento deve ser tratado como incidente.

## 8 Desenvolvimento e operação

Mudanças em software e infraestrutura devem ser versionadas e chegar à branch principal por pull request. Nos repositórios de serviços em produção, o merge deve depender da aprovação das verificações automatizadas definidas para o serviço, como testes, verificação de segredos e auditoria de dependências. A publicação dos serviços web e de backend usa os mecanismos de release aprovados, que conferem a origem dos commits. Os serviços de backend são publicados como imagens imutáveis, verificadas quanto a vulnerabilidades ao serem enviadas ao registro; os achados seguem o processo de gestão de vulnerabilidades do Manual de operação e desenvolvimento seguro. Falhas de implantação desses serviços acionam a reversão automática para a versão anterior.

O ambiente de produção usa credenciais, bases e permissões próprias. Os testes automatizados e o desenvolvimento dos serviços de backend devem usar bases locais ou temporárias, separadas da produção. Quando o desenvolvimento local de uma interface precisar consultar um serviço em

produção, deve usar conta de teste, sem dados de clientes, e conferir o destino antes de operações que alterem dados. Um ambiente de homologação, quando existir, também deve ter identidade, credenciais e bases próprias. Dados reais não devem alimentar o desenvolvimento; exceções precisam de minimização, justificativa e autorização.

Vulnerabilidades em código, dependências, imagens e equipamentos devem ser identificadas por ferramentas de verificação e alertas dos provedores, classificadas por severidade e corrigidas nos prazos do Manual de operação e desenvolvimento seguro. Exploração ativa ou exposição pública exige contenção prioritária.

## 9 Registros, monitoramento e prevenção de vazamento

Os registros das aplicações são centralizados no serviço de logs do provedor de nuvem. Os registros de acesso das aplicações que os mantêm são guardados por 180 dias, e os logs técnicos, por 14 dias. Esses prazos não podem ultrapassar os limites de cada categoria de serviço previstos nos Procedimentos de proteção de dados e terceiros, e prazos mais curtos previstos no aviso de privacidade ou no contrato de um serviço prevalecem. Os registros devem identificar data e hora, usuário ou serviço, ação e resultado e não devem conter senhas, tokens, imagens ou o conteúdo integral de informações de clientes. A leitura dos registros é restrita às pessoas autorizadas.

Alarmes automáticos acompanham a execução dos serviços, os erros, o uso de recursos e as falhas na coleta dos registros de acesso. Os alarmes que exigem ação devem notificar os responsáveis. Alertas e eventos suspeitos devem ser analisados pelos responsáveis e, quando indicarem incidente, seguir o Plano de resposta a incidentes.

A prevenção de vazamento de informações combina acesso mínimo e nominal, MFA, criptografia, bloqueio de acesso público ao armazenamento, serviços em sub-redes privadas, canais aprovados e as restrições de uso da seção 2.

## 10 Pessoas e confidencialidade

Antes de acessar informações confidenciais ou restritas, cada profissional deve:

1. Estar vinculado a obrigação de confidencialidade por NDA, termo ou cláusula equivalente, que subsista após o término da atuação enquanto a informação conservar caráter confidencial.
2. Concluir orientação de segurança e privacidade, incluindo proteção de dados pessoais e relato de incidentes.
3. Ter o acesso autorizado conforme a seção 3.

A orientação deve ser renovada anualmente e após mudanças ou incidentes relevantes. Quando um contrato exigir termo específico ou orientação adicional, esses requisitos devem ser cumpridos antes do acesso às informações do cliente. A participação e os termos devem ser registrados com nome, data, versão do material ou do instrumento e resultado.

Ao término da atuação, o profissional deve devolver os bens e as informações da Hineh e de clientes, cessar o acesso e colaborar com a exclusão verificável das cópias autorizadas.

## 11 Terceiros, incidentes e continuidade

Terceiros somente podem receber o mínimo necessário, após avaliação e contrato adequado, conforme os Procedimentos de proteção de dados e terceiros. Fornecedores críticos devem ser revisados anualmente e antes de mudanças materiais.

Qualquer suspeita de incidente, como perda de equipamento, acesso indevido, malware, vazamento, envio a destinatário errado ou credencial exposta, deve ser comunicada imediatamente ao responsável por incidentes, com preservação das evidências. Os incidentes são tratados conforme o Plano de resposta a incidentes. Nenhum profissional deve apagar registros ou ocultar o evento, e a contenção deve seguir a orientação do responsável.

As informações necessárias à prestação dos serviços devem ter cópias de segurança e procedimentos de recuperação conforme o Plano de backup, continuidade e recuperação.

## 12 Exceções, evidências e revisão

Exceções a esta política precisam de descrição do risco, medidas compensatórias, responsável, prazo de expiração de no máximo 90 dias e decisão da direção registrada. Não se admite exceção para ocultar incidente, usar dados sem autorização, declarar controle inexistente ou afastar obrigação legal. O registro de uma pendência não substitui a base legal do tratamento nem o mecanismo exigido para transferência internacional de dados pessoais.

A Hineh deve manter registros verificáveis da execução dos controles desta política, com data, escopo, origem, responsável e resultado. Os registros devem ser guardados em pasta corporativa com acesso nominal, por 24 meses, ressalvados os prazos legais ou contratuais aplicáveis.

A direção deve revisar esta política ao menos anualmente e após incidente relevante, mudança de arquitetura ou de requisito contratual. Cada versão deve indicar o responsável, a data de aprovação e a próxima revisão, e as alterações devem ser comunicadas aos profissionais.

Esta política observa a Lei nº 13.709/2018, especialmente as disposições sobre segurança, sigilo e boas práticas no tratamento de dados pessoais.