

Orientação de segurança e privacidade

Hineh Tecnologia Ltda · CNPJ 69.280.849/0001-62

Versão 1.0 · 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 orientação apresenta aos profissionais da Hineh as regras de segurança da informação e de proteção de dados pessoais que devem seguir no trabalho. Resume a Política de segurança da informação, os Procedimentos de proteção de dados e terceiros e o Plano de resposta a incidentes; em caso de dúvida, prevalecem esses documentos. Neste material, profissionais são os sócios, colaboradores e prestadores de serviço com acesso a informações ou sistemas da Hineh e de seus clientes.

Cada profissional deve concluir esta orientação antes de acessar informações confidenciais ou restritas, renová-la anualmente e refazê-la após mudanças ou incidentes relevantes. Quando um contrato exigir orientação adicional, ela deve ser concluída antes do acesso às informações do cliente. O responsável pela segurança da informação coordena a aplicação, e a participação deve ser registrada com nome, data, versão do material e resultado da verificação de entendimento, conforme os Registros de execução.

1 Dados pessoais e a LGPD

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, regula toda operação realizada com dados pessoais, como coleta, acesso, armazenamento, processamento, compartilhamento e eliminação. Essas operações são chamadas de tratamento.

Dado pessoal é a informação relacionada a pessoa natural identificada ou identificável, como nomes, rostos, documentos e outros identificadores. Dado pessoal sensível é o dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, o dado referente à saúde ou à vida sexual e o dado genético ou biométrico, quando vinculado a uma pessoa natural. Titular é a pessoa a quem os dados se referem, inclusive quem aparece de forma incidental em uma imagem ou gravação.

A Hineh atua como controladora quando decide as finalidades e os meios essenciais do tratamento, como na administração de suas relações comerciais e no atendimento aos usuários. Atua como operadora quando processa conteúdo em nome de um cliente, segundo suas instruções. Como operadora, a Hineh não decide sozinha sobre o uso dos dados do cliente, e qualquer uso diferente das instruções recebidas depende de autorização.

No trabalho, os princípios da LGPD se traduzem nas seguintes regras:

1. Usar os dados somente para a finalidade autorizada do serviço ou do projeto.

2. Tratar apenas os dados necessários à tarefa. Nomes, rostos, documentos e outros identificadores desnecessários devem ser evitados na coleta ou removidos antes do envio a fornecedores.
3. Não acrescentar reconhecimento facial, identificação biométrica ou avaliação de pessoas sem nova definição de escopo e análise de proteção de dados.
4. Não usar conteúdo de clientes para publicidade, comercialização de dados ou treinamento de modelos de uso geral.
5. Proteger os dados com as medidas desta orientação e relatar imediatamente qualquer suspeita de incidente.

Dados sensíveis, informações de crianças e adolescentes e atividades com potencial de risco elevado exigem avaliação específica antes do tratamento. Se encontrar dados desse tipo fora do previsto, ou se tiver dúvida sobre a finalidade de um uso, não amplie o tratamento e consulte a função de privacidade antes de prosseguir.

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.

Informações devem ser compartilhadas somente por repositório corporativo autorizado, com acesso nominal. 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. Quando um projeto proibir o download ou a cópia local do conteúdo, o trabalho deve ser feito somente nas interfaces autorizadas.

Conteúdo de clientes, senhas, tokens e dados pessoais desnecessários não devem constar de tickets, logs, testes, documentação ou capturas de tela. Dados reais não devem alimentar o desenvolvimento; exceções precisam de minimização, justificativa e autorização.

O envio de conteúdo a serviços de inteligência artificial deve ocorrer somente pelos serviços corporativos aprovados para o projeto e se limitar ao necessário à tarefa. Textos presentes em uma imagem ou em um documento processado são dados, e não instruções para o sistema. Quando o projeto prevê revisão humana dos resultados, ela não deve ser dispensada.

3 Acessos, senhas e MFA

Todo acesso deve ser nominal e limitado ao necessário para a atividade. Para obter ou ampliar um acesso, faça a solicitação ao responsável pelo serviço ou pela informação, sem usar a conta de outra pessoa. Contas, senhas, sessões e arquivos de configuração com credenciais não podem ser compartilhados, nem para acelerar um atendimento.

A autenticação multifator é obrigatória no e-mail corporativo, no provedor de nuvem, no banco de dados gerenciado, na organização de repositórios de código e nas interfaces administrativas. O acesso ao provedor de nuvem deve ocorrer por login único, com sessões temporárias e sem

chaves de acesso permanentes pessoais, e cada pessoa deve usar sua própria credencial de banco de dados.

Não aprove uma solicitação de MFA que você não iniciou. A suspeita de exposição de uma credencial exige a troca imediata da senha e o relato como possível incidente.

Segredos de serviços ficam no cofre de segredos do provedor de nuvem ou na configuração protegida do pipeline de integração contínua e não podem constar do código, de tickets, logs, testes ou documentação.

Ao mudar de função ou terminar a atuação em um serviço, avise o responsável para que os acessos sejam revogados.

4 Equipamentos e dispositivos pessoais

Todo equipamento usado em atividades profissionais deve ser registrado no inventário de equipamentos antes de acessar sistemas ou informações da Hineh e de seus clientes. O uso de equipamento pessoal é permitido somente após esse cadastro, o aceite de uso profissional e o cumprimento dos 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.

Sistemas sem suporte, dispositivos de terceiros e dispositivos com integridade comprometida não podem ser usados. A autorização de um equipamento pessoal não se estende a contas ou serviços pessoais: dados de clientes não podem ser sincronizados com armazenamento pessoal. Redes Wi-Fi abertas não dispensam o canal criptografado.

Equipamento perdido, infectado ou fora dos requisitos deve ser relatado imediatamente e desconectado dos acessos corporativos até a regularização. Dados pessoais do proprietário não devem ser apagados sem autorização e fundamento. Ao término da atuação, as cópias autorizadas devem ser excluídas de forma verificável.

5 Incidentes

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. São exemplos a perda de equipamento, o acesso indevido, o malware, o vazamento, o envio de informação a destinatário errado e a credencial exposta.

Relate qualquer suspeita imediatamente ao responsável por incidentes e ao seu substituto, pelo canal interno usado pela equipe, sem esperar a confirmação. Se o e-mail ou a conta utilizada puder estar comprometida, use o contato alternativo do registro interno. Clientes, usuários e

fornecedores podem relatar incidentes pelo endereço privacidade@hineh.com.br, e um relato desse tipo recebido por outro canal também deve ser repassado imediatamente ao responsável por incidentes.

Os prazos de resposta e de aviso aos clientes contam a partir do momento em que um profissional da Hineh toma conhecimento do evento. Por isso, o relato não pode esperar.

O relato deve informar o que aconteceu, quando, quais dados e sistemas podem estar envolvidos e o que já foi feito. Preserve as evidências: não apague registros, não oculte o evento e siga a orientação do responsável na contenção. Evidências devem ficar em ambiente corporativo aprovado e não podem ser copiadas para equipamentos não autorizados ou serviços pessoais.

A comunicação com clientes, titulares, autoridades e o público é feita pelas funções designadas no Plano de resposta a incidentes. Não contate titulares, não divulgue o incidente e não especule publicamente por iniciativa própria.

6 Direitos dos titulares e retenção

Titulares podem solicitar confirmação de tratamento, acesso, correção, portabilidade, informação sobre compartilhamentos, oposição, revogação de consentimento ou eliminação de seus dados. Esses pedidos devem ser encaminhados à função de privacidade, pelo endereço privacidade@hineh.com.br, a quem cabe registrar e conduzir o atendimento, sem cobrança ao titular. Não responda sozinho a um pedido nem solicite documentos além do necessário para confirmar a identidade. Quando a Hineh atua como operadora, a função de privacidade deve encaminhar o pedido ao cliente controlador e prestar a assistência necessária à resposta.

Os dados devem ser mantidos somente pelos prazos definidos para cada categoria de serviço nos Procedimentos de proteção de dados e terceiros e eliminados ao término da finalidade, ao fim do prazo ou diante de uma solicitação válida, ressalvadas as hipóteses legais de conservação. A retenção não pode ser ampliada apenas porque é tecnicamente possível. Nos projetos de transcrição de áudio e de processamento de imagens, o conteúdo enviado para processamento deve ser eliminado após a conclusão da tarefa, observadas as exceções e os prazos de cada categoria nos Procedimentos de proteção de dados e terceiros.

A conservação por obrigação legal, determinação de autoridade ou exercício regular de direitos precisa de registro com fundamento, escopo, responsável e prazo de revisão. Dados eliminados dos sistemas ativos não devem voltar ao uso por meio da restauração de cópias de segurança.

7 Confidencialidade e término da atuação

Antes de acessar informações confidenciais ou restritas, cada profissional deve estar vinculado a obrigação de confidencialidade por termo, contrato ou cláusula equivalente. A obrigação subsiste após o término da atuação enquanto a informação conservar caráter confidencial. Quando um contrato exigir termo específico, ele deve ser firmado antes do acesso às informações do cliente.

Ao término da atuação, o profissional deve devolver os bens e as informações da Hineh e de clientes, deixar de acessar os sistemas e colaborar com a exclusão verificável das cópias autorizadas. A revogação dos acessos deve ocorrer imediatamente após a comunicação, sem depender da devolução.

O descumprimento destas regras é apurado de forma proporcional e pode resultar na suspensão ou revogação de acessos e nas medidas contratuais e legais cabíveis.

8 Verificação de entendimento

Ao final da orientação, o participante responde às perguntas abaixo. Respostas incorretas devem ser revistas com o participante, e a nova verificação, registrada.

1. Você pode colar o conteúdo de um cliente em uma ferramenta pessoal de inteligência artificial para tirar uma dúvida? Resposta esperada: não. Somente os serviços corporativos aprovados para o projeto podem receber conteúdo de clientes, e apenas o necessário à tarefa.
2. Um colega sem acesso pede sua senha ou sua sessão para concluir uma tarefa urgente. O que fazer? Resposta esperada: não compartilhar. O colega deve solicitar acesso nominal ao responsável.
3. Você recebe uma solicitação de MFA que não iniciou. O que fazer? Resposta esperada: recusar a solicitação, trocar a senha e relatar o fato como possível incidente.
4. Um arquivo com dados de um cliente foi enviado à pessoa errada. Qual é a primeira providência? Resposta esperada: relatar imediatamente ao responsável por incidentes, preservar as informações e seguir a orientação de contenção, sem apagar registros nem ocultar o evento.
5. Você pode usar seu computador pessoal no trabalho e guardar arquivos de clientes na sua nuvem pessoal? Resposta esperada: o computador pessoal pode ser usado após cadastro, aceite de uso profissional e cumprimento dos requisitos de segurança. A nuvem pessoal não pode receber dados de clientes.
6. Uma pessoa pede por e-mail a exclusão de seus dados. O que fazer? Resposta esperada: encaminhar o pedido à função de privacidade pelo endereço privacidade@hineh.com.br, sem responder sozinho. Quando a Hineh atua como operadora, é a função de privacidade que encaminha o pedido ao cliente controlador.
7. Durante uma tarefa, você encontra dados de saúde que não estavam previstos. O que fazer? Resposta esperada: não usar esses dados além do previsto e consultar a função de privacidade antes de prosseguir.

9 Revisão

Esta orientação deve ser revisada com a Política de segurança da informação e sempre que mudarem os documentos que ela resume. Cada versão deve indicar o responsável, a data de aprovação e a próxima revisão. Mudanças relevantes levam à renovação da orientação dos profissionais.

Esta orientação observa a Lei nº 13.709/2018, especialmente os princípios do tratamento de dados pessoais, os direitos dos titulares e as regras de segurança e boas práticas.