

Registros de execução

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](#)

Modelos de registro, sem dados preenchidos. Registros de execução, inventários, contatos internos e evidências são mantidos sob acesso restrito.

Este documento reúne os modelos de registro da execução dos controles previstos na Política de segurança da informação, nos Procedimentos de proteção de dados e terceiros, no Manual de operação e desenvolvimento seguro, no Plano de resposta a incidentes, no Plano de backup, continuidade e recuperação, na Orientação de segurança e privacidade e nos termos de confidencialidade. Aplica-se aos produtos e serviços da Hineh e às pessoas responsáveis pela execução desses controles. Os registros apoiam a responsabilização, a prestação de contas e o registro das operações de tratamento previstos na Lei nº 13.709/2018.

Cada registro deve ser preenchido quando a atividade ocorrer, com dados reais, pela pessoa que a executou ou pelo responsável indicado no documento que a exige. O registro deve refletir o resultado observado, inclusive falhas, desvios e pendências. Um modelo em branco ou uma regra escrita não comprova a execução de um controle, e nenhum registro deve ser preenchido por antecipação.

Todo registro deve conter identificador, data e fuso horário, escopo, responsável, origem, resultado, versão do documento ou do sistema aplicável e pendências, além dos campos específicos indicados nas seções abaixo. Os registros podem ser mantidos em documento, planilha ou sistema corporativo, desde que contenham os campos aplicáveis.

Os registros não devem conter senhas, tokens, chaves, conteúdo de clientes ou dados pessoais além do necessário à sua finalidade. Quando uma evidência demonstrar uma configuração, os segredos e os identificadores desnecessários devem ser ocultados, sem retirar o contexto que permite verificá-la.

Os registros devem ser guardados em pasta corporativa com acesso nominal, por 24 meses, ressalvados os prazos legais ou contratuais aplicáveis. Registros de incidentes que envolvam dados pessoais devem ser mantidos por no mínimo cinco anos, conforme o Plano de resposta a incidentes. Correções devem preservar o registro anterior e identificar a data e o responsável pela alteração.

1 Registro de tratamento de dados pessoais

Antes de iniciar um tratamento ou alterar materialmente seu escopo, o responsável pelo serviço deve registrar, conforme os Procedimentos de proteção de dados e terceiros:

1. Serviço ou projeto, responsável pelo serviço e data do registro.

2. Papel da Hineh na atividade, como controladora ou operadora, com a identificação do controlador e dos operadores.
3. Finalidade e fundamento legal aplicável.
4. Categorias de dados e de titulares, indicando a presença de dados sensíveis ou de informações de crianças e adolescentes.
5. Origem dos dados.
6. Sistemas envolvidos e permissões de acesso.
7. Destinatários e fornecedores, com os países em que os dados são armazenados ou acessados e o mecanismo de transferência internacional aplicável.
8. Prazos de retenção e eliminação de cada categoria de dados, com o evento que inicia a contagem e o ciclo de expiração das cópias de segurança.
9. Instruções e limites definidos pelo cliente, quando a Hineh atua como operadora.
10. Referência à avaliação de risco da seção 2, quando exigida.
11. Data da última revisão.

O registro deve ser revisto quando houver mudança de finalidade, inclusão de novas categorias de dados ou contratação de novo destinatário.

2 Avaliação de risco do tratamento

Tratamentos de dados sensíveis, de informações de crianças e adolescentes ou com potencial de risco elevado aos titulares devem receber avaliação específica antes do início, registrada com:

1. Tratamento avaliado, com referência ao registro da seção 1, e o motivo da avaliação.
2. Riscos identificados aos titulares e ao serviço, incluindo os relativos a pessoas que apareçam de forma incidental no conteúdo.
3. Impacto estimado de cada risco.
4. Medidas adotadas para reduzir cada risco, como minimização, pseudonimização, restrição de acesso e revisão humana.
5. Risco residual e decisão de prosseguir, prosseguir com condições ou não prosseguir.
6. Responsável pela avaliação, decisão da direção sobre o risco residual e data.
7. Evento ou data que exige nova avaliação.

3 Avaliação de terceiros

Antes de permitir que um fornecedor acesse ou processe dados pessoais, e em cada reavaliação, o responsável pelo serviço e a função de privacidade devem registrar:

1. Fornecedor, serviço contratado e serviços da Hineh em que é utilizado.
2. Finalidade e necessidade do compartilhamento, categorias de dados e criticidade.
3. Avaliação de segurança, confidencialidade, controle de acesso, localização dos dados, subcontratação, retenção, eliminação, resposta a incidentes e apoio ao exercício de direitos.

4. Documentação analisada, como termos de tratamento de dados, informações técnicas, relatórios de auditoria e certificações, com a data da consulta.
5. Instrumento contratual aplicável e mecanismo de transferência internacional, quando houver.
6. Lacunas identificadas e medidas compensatórias.
7. Decisão, restrições de uso, responsáveis e data.
8. Data da próxima revisão.
9. No encerramento da relação, a data, a revogação dos acessos, a devolução ou eliminação dos dados e as confirmações recebidas.

Fornecedores que tratem dados pessoais ou sustentem atividades críticas devem ser reavaliados ao menos anualmente e sempre que houver mudança relevante, incidente ou alteração das condições contratuais.

4 Acessos e equipamentos

Inventário de acessos

Cada acesso concedido a sistemas e informações da Hineh deve ser registrado no inventário de acessos com:

1. Pessoa ou identidade de serviço e seu responsável.
2. Sistema e ambiente.
3. Perfil ou permissões concedidas, indicando quando se trata de acesso administrativo.
4. Justificativa e prazo, quando o acesso for temporário.
5. Solicitante, aprovador e data da aprovação.
6. Data da concessão e pessoa que a executou.
7. Forma de autenticação: MFA, para acesso humano; escopo e local de guarda da credencial, para identidade de serviço, sem registrar seu valor.
8. Indicação de acesso emergencial, com a data da revisão no dia útil seguinte.
9. Data da última revisão e seu resultado.
10. Data e hora da revogação, quando houver.

Identidades de serviço podem ser registradas por referência à configuração versionada que as declara, desde que o inventário indique o responsável e o escopo de cada uma.

Revisão de acessos

A revisão de acessos deve ocorrer ao menos trimestralmente e sempre que houver mudança de função, e seu registro deve conter:

1. Data da revisão e responsável.
2. Sistemas revisados e origem da lista conferida, como console ou exportação administrativa, com a data da consulta.
3. Contas, grupos, permissões, credenciais de serviço e acessos temporários conferidos.

4. Permissões removidas ou ajustadas, com a data de cada alteração.
5. Contas compartilhadas, sem responsável ou sem MFA encontradas e a providência adotada.
6. Resultado e data prevista da próxima revisão.

Revogação de acessos

No desligamento, no término da atuação em um serviço ou na mudança de função, o registro de revogação deve conter:

1. Pessoa, motivo e data e hora da comunicação.
2. Sistemas abrangidos.
3. Contas bloqueadas, sessões encerradas, grupos removidos e tokens revogados, com a data e a hora de cada ação.
4. Segredos conhecidos pela pessoa e decisão sobre sua rotação.
5. Devolução de bens e informações e exclusão das cópias autorizadas, com as datas de conclusão. A revogação não depende dessas etapas.
6. Responsável pela execução e pela verificação.

Inventário de equipamentos

Cada equipamento usado em atividades profissionais, da empresa ou pessoal autorizado, deve ser registrado antes de acessar sistemas ou informações da Hineh e de seus clientes, com:

1. Identificador reduzido do equipamento e pessoa responsável.
2. Propriedade do equipamento: da empresa ou pessoal autorizado para uso profissional.
3. Data do cadastro e do aceite de uso profissional, e autorização de acesso, com a data e quem autorizou.
4. Sistema operacional e versão, com indicação do suporte vigente e da data das últimas atualizações de segurança do sistema e do navegador.
5. Antivírus ou EDR ativo.
6. Firewall do sistema operacional habilitado.
7. Criptografia do disco ativa.
8. Bloqueio automático da tela após, no máximo, cinco minutos de inatividade.
9. Conta de usuário individual, sem compartilhamento da sessão profissional.
10. Forma de verificação de cada requisito, data e pessoa que verificou, sem registrar chaves de recuperação ou outros segredos.
11. Requisito não atendido, exceção registrada conforme a seção 5 e data da regularização.
12. Ocorrências de perda, infecção ou desconexão dos acessos corporativos, com data.
13. Data do término do uso profissional e confirmação da exclusão das cópias autorizadas.

As conferências periódicas previstas no Manual de operação e desenvolvimento seguro devem atualizar os campos 4 a 10.

5 Vulnerabilidades, exceções e mudanças

Vulnerabilidades

Cada vulnerabilidade confirmada em código, dependências, imagens ou equipamentos deve ser registrada com:

1. Identificador, ativo afetado e versão.
2. Origem, como ferramenta de verificação, alerta do provedor ou relato, e data da identificação.
3. Severidade, impacto e contexto, indicando exploração ativa ou exposição pública.
4. Prazo de correção conforme o Manual de operação e desenvolvimento seguro.
5. Responsável.
6. Contenção ou mitigação adotada, com data.
7. Correção aplicada, com a versão ou o commit e a data.
8. Nova verificação após a correção, com resultado e data.
9. Encerramento ou referência à exceção aprovada.

Exceções

O registro de cada exceção à Política de segurança da informação ou ao Manual de operação e desenvolvimento seguro deve conter:

1. Regra excepcionada, com o documento e a seção.
2. Descrição do risco.
3. Medidas compensatórias.
4. Responsável.
5. Decisão da direção, com a data e a identificação de quem decidiu.
6. Data de expiração, no máximo 90 dias após a decisão.
7. Encerramento ou nova decisão, com data.

Mudanças

Mudanças no código e na infraestrutura definida como código são registradas pelo pull request, com o resultado das verificações automatizadas exigidas no repositório. As publicações feitas pela ferramenta de release geram registro que identifica a versão publicada e é guardado em armazenamento privado, conforme o Manual de operação e desenvolvimento seguro. Mudanças feitas fora desse fluxo, como a publicação de aplicativos nas lojas ou a alteração da configuração do banco de dados gerenciado, devem ser registradas com data, responsável, escopo e resultado. A recuperação de uma versão anterior pela ferramenta de release também gera registro de publicação. Após uma reversão automática de implantação, a verificação do restabelecimento do serviço deve ser registrada. Mudanças emergenciais devem registrar também a justificativa e as aprovações e validações aplicáveis, conforme o Plano de resposta a incidentes.

6 Incidentes e exercícios

Registro de incidente

O primeiro relato de um possível incidente deve abrir um registro, atualizado durante toda a resposta e mantido em local de acesso restrito, com:

1. Identificador.
2. Data e hora da ciência, com fuso horário, e origem do relato ou do alerta.
3. Serviços e ativos envolvidos e sintomas observados.
4. Classificação inicial e suas revisões, com data e justificativa.
5. Responsável pela resposta, data e hora da triagem e papel da Hineh, como controladora ou operadora, quanto aos dados envolvidos.
6. Medidas de contenção, com a data, a hora e a identificação de quem decidiu cada medida.
7. Evidências preservadas, local de guarda, pessoas que as coletaram e acessaram, datas e verificação de integridade.
8. Avaliação de dados pessoais: serviços, categorias de dados e titulares afetados, volume estimado, fatores de risco, conclusão, justificativa e incertezas.
9. Comunicações realizadas ou dispensadas, com destinatário, data e hora, conteúdo resumido e justificativa da decisão.
10. Erradicação e recuperação: causa corrigida, credenciais substituídas, cópia usada na restauração, verificação de integridade e autorização da reabertura.
11. Análise inicial dos incidentes críticos e altos, com cronologia, causa ou hipóteses, controles envolvidos, ações corretivas, responsáveis, prazos e pendências com previsão de atualização.
12. Encerramento, com data, critério atendido e risco remanescente aceito, quando houver.
13. Prazo de guarda e eliminação das cópias de evidências que deixarem de ser necessárias.

Eventos que não configurem incidente devem ser encerrados no próprio registro, com a justificativa.

Registro de exercício

Cada exercício de resposta a incidentes deve usar cenário fictício, sem dados reais, e registrar:

1. Data, participantes e responsável pela condução.
2. Versão do Plano de resposta a incidentes exercitada.
3. Cenário utilizado.
4. Tempos observados para ciência, triagem, contenção e comunicação simulada.
5. Decisões tomadas.
6. Falhas e lacunas identificadas.
7. Ações corretivas, responsáveis e prazos.

Comunicações simuladas não devem ser enviadas a clientes, titulares ou autoridades.

7 Teste de restauração

O registro de cada teste de restauração de cópias de segurança deve conter, conforme o Plano de backup, continuidade e recuperação:

1. Identificador, data, pessoa que executou e pessoa que acompanhou, quando houver.
2. Serviço e sistema restaurados.
3. Cópia utilizada e momento dos dados que ela contém.
4. Ambiente isolado de restauração e controle de acesso aplicado.
5. Horários de início e de fim.
6. Verificação de integridade, como contagens, amostras e consistência dos dados.
7. Exclusões pendentes reaplicadas antes da liberação.
8. Perda de dados observada em relação ao último ponto íntegro.
9. Comparação dos tempos e da perda observados com os objetivos de recuperação do plano.
10. Falhas, desvios e ações corretivas, com responsáveis.
11. Resultado e aprovação técnica.
12. Proteção e eliminação da cópia restaurada ao término do teste.

O registro deve declarar a falha quando os objetivos não forem atingidos. Restaurações realizadas fora de teste, em incidente ou na operação, devem ser registradas com o mesmo modelo.

8 Titulares, eliminação e encerramento

Solicitações de titulares

O registro de cada solicitação de titular deve conter:

1. Protocolo, data de recebimento e canal.
2. Serviço envolvido e papel da Hineh, como controladora ou operadora.
3. Tipo de solicitação.
4. Verificação de identidade realizada, proporcional ao risco.
5. Prazo aplicável.
6. Data do encaminhamento ao controlador e assistência prestada, quando a Hineh atua como operadora.
7. Decisão, providência executada e sistemas consultados.
8. Resposta enviada, com data, e eventuais impedimentos e sua justificativa.
9. Data do encerramento.

O registro deve preservar apenas as informações necessárias à comprovação do atendimento.

Eliminação de dados

O registro de cada eliminação decorrente de prazo, encerramento ou solicitação deve conter:

1. Motivo: expiração do prazo, encerramento da finalidade ou solicitação válida.
2. Serviço, categorias de dados e escopo.
3. Sistemas e cópias abrangidos, como bancos de dados, objetos armazenados, arquivos temporários, filas e índices.
4. Mecanismo aplicado e data da execução.
5. Verificação após a eliminação e resultado, sem reproduzir o conteúdo eliminado.
6. Cópias de segurança que ainda contenham os dados e data de expiração da última.
7. Fornecedores acionados e confirmações recebidas.
8. Conservação por obrigação legal, determinação de autoridade ou exercício regular de direitos, com fundamento, escopo, responsável e prazo de revisão.
9. Falhas e correções.

Encerramento e devolução

O registro do encerramento de contrato, conta, integração ou autorização de acesso deve conter:

1. Objeto encerrado, solicitante autorizado e data efetiva.
2. Sistemas, dados, fornecedores e acessos abrangidos.
3. Data da interrupção de novas coletas e processamentos.
4. Acessos, sessões e credenciais revogados, com data.
5. Devolução dos dados, quando cabível: destinatário confirmado, canal seguro, formato e data.
6. Referência ao registro de eliminação e data prevista de expiração das cópias de segurança.
7. Exceções legais, com sua data limite ou condição de término.
8. Confirmação entregue ao cliente, quando solicitada, com o escopo concluído, as datas e a retenção residual.

A confirmação de encerramento não deve afirmar eliminação integral enquanto houver cópias conhecidas cuja retenção ainda esteja em curso.

9 Governança e pessoas

Aprovação e revisão de documentos

O registro de cada versão de política, procedimento, plano ou modelo deve conter:

1. Documento e versão.
2. Responsável pelo documento.
3. Data da aprovação e identificação de quem aprovou.
4. Principais alterações em relação à versão anterior.
5. Data da última revisão e seu resultado, como manutenção sem alterações ou nova versão.
6. Data da próxima revisão.
7. Data e forma da comunicação da nova versão aos profissionais.

8. Endereço e data de publicação, quando o documento for publicado.

A data de aprovação deve ser a do ato efetivo da direção e não pode retroagir.

Ciência das políticas

A ciência de cada profissional deve ser registrada antes da liberação de acesso, com:

1. Profissional e função.
2. Documentos e versões apresentados.
3. Data e meio verificável da ciência, como assinatura, aceite eletrônico ou mensagem identificável.
4. Responsável pelo registro.

Funções e contatos

O registro de funções e contatos deve conter:

1. Função: direção, responsável pela segurança da informação, responsável por incidentes, função de privacidade, responsável pelo relacionamento com cada cliente e responsável por cada serviço.
2. Pessoa designada e substituto.
3. Meios de contato, incluindo ao menos um que não dependa do e-mail corporativo.
4. Contatos de incidente de cada cliente e fornecedor.
5. Data da designação e da última revisão.

O registro deve ser mantido em local de acesso restrito e revisto sempre que houver mudança na equipe, nos clientes ou nos fornecedores, e ao menos a cada seis meses, conforme o Plano de resposta a incidentes.

Orientação de segurança e privacidade

O registro de cada participação na orientação deve conter:

1. Participante e função.
2. Versão da Orientação de segurança e privacidade utilizada.
3. Data e motivo: antes do primeiro acesso, renovação anual ou mudança ou incidente relevante.
4. Pessoa que conduziu.
5. Resultado da verificação de entendimento e reforço realizado, quando houver.
6. Data prevista da próxima renovação.

Orientações adicionais exigidas em contrato devem ser registradas da mesma forma, com a identificação do material utilizado.

Termos de confidencialidade

Cada vínculo de confidencialidade deve ser registrado antes do acesso a informações confidenciais ou restritas, com:

1. Profissional, vínculo e função.

2. Instrumento utilizado, como termo individual, contrato ou cláusula equivalente, e sua versão.
3. Data e meio da assinatura ou do aceite verificável.
4. Informações e clientes abrangidos, incluindo termo específico exigido por contrato.
5. Vigência e subsistência da obrigação após o término da atuação.
6. Local de guarda do instrumento assinado.
7. Responsável pela liberação do acesso.

10 Índice de evidências

Para responder a questionários de clientes, auditorias e verificações contratuais, o índice de evidências deve relacionar cada pergunta ou requisito às evidências que o demonstram, com:

1. Pergunta ou requisito e seu identificador.
2. Controle e documento, versão e seção que o estabelecem.
3. Natureza da evidência: documento, configuração ou registro de execução.
4. Origem, data e hora da coleta, com fuso horário.
5. Escopo: serviço ou categoria de serviço, sistema e período abrangidos.
6. Responsável pela coleta.
7. Resultado observado e limites do que a evidência demonstra.
8. Local de guarda e, quando útil, verificação de integridade.
9. Informações ocultadas na cópia compartilhada.
10. Data prevista de nova conferência, quando a evidência perder validade com o tempo.
11. Destinatário e data do envio, quando a evidência for compartilhada externamente.

Uma evidência de configuração demonstra o estado de um sistema na data da coleta. Não comprova, por si, a execução contínua de um controle nem sua aplicação a outros sistemas.

11 Revisão

Estes modelos devem ser revisados com a Política de segurança da informação e sempre que mudar um documento que exija registro. Cada versão deve indicar o responsável, a data de aprovação e a próxima revisão.