

Plano de backup, continuidade e recuperação

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](#)

Este plano estabelece como a Hineh mantém cópias de segurança das informações necessárias à prestação de seus serviços, como recupera dados, código, infraestrutura e serviços após falhas e como conduz a operação e a comunicação com os clientes durante uma interrupção. Aplica-se aos produtos e serviços da Hineh, incluindo projetos de transcrição de áudio, processamento de imagens e integração com serviços externos, abrangendo bancos de dados, armazenamento de arquivos, código-fonte, infraestrutura, segredos e fornecedores.

Este plano complementa a Política de segurança da informação e é aplicado em conjunto com os Procedimentos de proteção de dados e terceiros, que definem os prazos de retenção, com o Plano de resposta a incidentes e com o Manual de operação e desenvolvimento seguro.

1 Escopo e responsabilidades

Cada serviço deve ter cópias de segurança das informações necessárias à sua prestação e à sua reconstrução: os dados mantidos pelo serviço, como resultados, regras, configurações e metadados, além do código, das definições de infraestrutura e dos registros de publicação. Os segredos devem ser recuperados por mecanismo próprio, com acesso restrito, e não podem ser copiados para registros ou relatórios.

Quando o cliente mantém o conteúdo original em seu próprio ambiente e autoriza seu processamento pela Hineh, a fonte primária desse conteúdo permanece com o cliente. Nesse caso, o backup da Hineh deve abranger os resultados, as regras, os metadados necessários e a configuração do serviço, sem cópia permanente do conteúdo original.

A direção aprova este plano e decide sobre os recursos necessários à recuperação e sobre os riscos residuais. O responsável pela segurança da informação coordena a aplicação deste plano, as restaurações e os testes. O responsável por cada serviço mantém o inventário de backup do serviço e os registros correspondentes. O responsável pelo relacionamento com cada cliente conduz as comunicações sobre a interrupção e a recuperação. Quando a interrupção decorrer de incidente de segurança, o responsável por incidentes conduz a resposta conforme o Plano de resposta a incidentes.

Essas funções podem ser exercidas pela mesma pessoa em uma equipe pequena. Cada função deve ter um substituto designado, com os acessos necessários para executar a recuperação, e a indisponibilidade de uma pessoa transfere suas atribuições ao substituto.

2 Cópias de segurança

Os bancos de dados que sustentam os serviços devem ter cópias de segurança automáticas, ao menos diárias, realizadas pelo serviço de banco de dados gerenciado. O inventário de backup de cada serviço deve identificar as bases incluídas, a periodicidade, a retenção, a localização, a última cópia válida e o responsável.

As cópias de segurança devem ser criptografadas em repouso, conforme a Política de segurança da informação, e o acesso a elas deve ser restrito às pessoas designadas para administrá-las. A identidade utilizada pela aplicação não deve poder excluir cópias de segurança nem alterar sua retenção.

Falhas na execução das cópias devem ser notificadas aos responsáveis e analisadas quando recebidas. Disponibilidade em múltiplas zonas, replicação e versionamento reduzem o impacto de falhas, mas não substituem cópias de segurança verificáveis.

Retenção e eliminação

As cópias de segurança seguem os prazos dos Procedimentos de proteção de dados e terceiros e não podem ampliar a retenção prevista para cada categoria de serviço. Prazos mais curtos previstos no aviso de privacidade ou no contrato de um serviço prevalecem.

Nos projetos de processamento de imagens, as imagens brutas temporárias devem ficar fora das rotinas de backup, e cada cópia de segurança deve expirar em até 35 dias de sua criação. Esse prazo pode terminar depois da exclusão dos dados nos sistemas ativos, e o cronograma de encerramento deve informar a data de expiração da última cópia que ainda contenha os dados.

Dados eliminados dos sistemas ativos podem permanecer em cópia de segurança até sua expiração e, durante esse período, devem permanecer inacessíveis ao uso cotidiano. As cópias não devem ser reutilizadas para desenvolvimento. Em qualquer restauração, as exclusões pendentes devem ser reaplicadas antes da liberação do ambiente.

3 Recuperação de código, infraestrutura e serviços

O código-fonte dos serviços é mantido em repositórios versionados da organização de repositórios de código. Em cada repositório, a branch principal bloqueia envio direto, reescrita do histórico e exclusão, e as mudanças chegam a ela por pull request.

A infraestrutura de nuvem é definida como código, versionada da mesma forma, e seu estado é guardado em armazenamento privado, criptografado e versionado, com trava contra alterações simultâneas. Exclusões ou substituições destrutivas de recursos protegidos, como armazenamento de arquivos, serviços, registros, segredos, imagens e chaves, são bloqueadas na operação diária.

Os serviços de backend são publicados como imagens imutáveis, e cada publicação é registrada. As imagens e os arquivos de publicações anteriores ficam preservados para recuperação. Falhas de implantação acionam a reversão automática para a versão anterior. A recuperação para uma publicação anterior usa a imagem e o commit registrados, e a imagem deve corresponder a um commit do histórico da branch principal.

Os arquivos das aplicações web ficam em armazenamento de objetos com versionamento, o que permite recuperar versões anteriores. As credenciais dos serviços declaradas na infraestrutura

como código ficam no cofre de segredos do provedor de nuvem, em que uma exclusão pode ser revertida em até 30 dias. As chaves de criptografia criadas no serviço de chaves do provedor de nuvem têm período de espera de 30 dias antes da exclusão definitiva.

A recuperação deve usar os mecanismos de publicação aprovados, sem contornar as proteções operacionais.

4 Objetivos de recuperação

Salvo objetivo diferente previsto em contrato ou no inventário do serviço, a Hineh adota os seguintes objetivos para os dados mantidos em banco de dados:

1. Perda máxima de dados (RPO) de até 24 horas, correspondente ao intervalo entre as cópias diárias.
2. Retomada do serviço (RTO) em até um dia útil após o acionamento da recuperação, desde que as dependências externas necessárias estejam disponíveis.

O período em que uma dependência externa, como um fornecedor ou a origem de dados do cliente, permanecer indisponível deve ser registrado separadamente e não pode ser omitido da medição.

Esses objetivos orientam o planejamento e devem ser verificados nos testes de restauração. A Hineh não mantém operação em regime contínuo, e esses objetivos não constituem garantia de disponibilidade.

5 Continuidade diante de falhas

Durante uma interrupção, a Hineh prioriza a integridade dos dados e a comunicação com o cliente. As situações abaixo seguem estas regras:

1. Indisponibilidade de fornecedor de inteligência artificial ou de outro serviço externo necessário ao processamento: o processamento automatizado afetado é pausado, e somente as referências permitidas permanecem em fila, dentro dos prazos de retenção aplicáveis. O cliente é informado do atraso e, quando acordado, pode receber revisão humana dentro da capacidade disponível. Os dados não são enviados a fornecedor alternativo sem a avaliação e a autorização previstas nos Procedimentos de proteção de dados e terceiros e, quando aplicável, no contrato com o cliente.
2. Indisponibilidade de serviço da Hineh: nos serviços em que o cliente mantém a fonte primária, o reproprocessamento após a recuperação parte dessa fonte, somente com autorização do cliente, e usa identificação única de cada tarefa para evitar resultados duplicados.
3. Indisponibilidade ou inconsistência da origem de dados do cliente: o serviço não gera resultados com base em conteúdo incompleto.
4. Suspeita de comprometimento: a resposta segue o Plano de resposta a incidentes e precede a retomada, com preservação das evidências antes da restauração.

O responsável pelo relacionamento com o cliente informa o escopo afetado, a previsão de retomada, a alternativa manual disponível, quando houver, e os próximos marcos. Quando a interrupção envolver dados pessoais ou incidente de segurança, as comunicações seguem os

prazos do Plano de resposta a incidentes. A Hineh não promete continuidade irrestrita nem atendimento em regime contínuo; a capacidade de operação humana e os horários de atendimento de cada projeto são definidos com o cliente.

6 Procedimento de restauração

A restauração de dados segue as etapas abaixo:

1. Abrir o registro da ocorrência com o início, a falha observada, os sistemas afetados e o último ponto íntegro conhecido. Se houver suspeita de incidente, acionar o Plano de resposta a incidentes e preservar as evidências antes de alterar os sistemas.
2. Selecionar a cópia de segurança e restaurá-la em ambiente isolado sempre que possível, com permissões verificadas e sem conexão de usuários. Não restaurar sobre a única cópia disponível de uma evidência.
3. Implantar a versão da aplicação compatível com os dados restaurados pelos mecanismos de publicação aprovados e recuperar os segredos pelo mecanismo autorizado, sem copiá-los para registros ou relatórios.
4. Validar a integridade com contagens e amostras sintéticas ou minimizadas, a consistência dos resultados, os índices, a versão das regras e os registros. Reaplicar as exclusões pendentes e as limitações de retenção e verificar a autenticação, o isolamento entre clientes e os registros de acesso.
5. Registrar o tempo de recuperação e a perda de dados observada, comparar com os objetivos da seção 4 e liberar o serviço com autorização do responsável pela segurança da informação ou, em incidente, do responsável por incidentes. Reprocessar lacunas a partir da fonte do cliente somente com autorização e controle de duplicidade, acompanhar os erros após a liberação e concluir o registro.

7 Testes de restauração

A Hineh deve realizar teste de restauração ao menos trimestralmente, antes de um novo serviço entrar em produção e após mudança material no banco de dados ou no processo de backup. Cada teste deve restaurar, em ambiente isolado, uma cópia de segurança real do ambiente aplicável: a de um serviço em produção nos testes periódicos e após mudança material, e a do ambiente preparado para o novo serviço no teste anterior à sua entrada em produção. O teste deve verificar a integridade dos dados, a reaplicação das exclusões e o tempo de recuperação.

O ambiente restaurado que contenha dados reais deve ter proteção equivalente à da produção e ser eliminado ao término do teste.

O registro do teste deve indicar o início e o fim, a cópia utilizada, o escopo, o resultado, a perda de dados e o tempo de recuperação observados, os desvios, as correções e a aprovação. Quando os objetivos não forem atingidos, o registro deve declarar a falha, e o teste deve ser repetido após a correção.

8 Registros e revisão

Os registros de backup, restauração, testes e interrupções devem ser guardados em pasta corporativa com acesso nominal, por 24 meses, ressalvados os prazos legais ou contratuais aplicáveis e os prazos de guarda dos registros de incidentes.

A direção deve revisar este plano 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 às pessoas responsáveis por sua execução.

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