

Manual de operação e desenvolvimento seguro

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 manual detalha como a Hineh executa os controles técnicos e operacionais previstos na Política de segurança da informação: concessão, revisão e revogação de acessos, conferência de equipamentos, gestão de vulnerabilidades, desenvolvimento, testes e implantação, registros e monitoramento e guarda de evidências. Aplica-se aos produtos e serviços da Hineh, incluindo projetos de transcrição de áudio, processamento de imagens e integração com serviços externos, e às pessoas que operam seus sistemas.

O responsável pela segurança da informação coordena a execução destes procedimentos, e o responsável por cada serviço os aplica ao serviço sob sua gestão. Exigências contratuais específicas de um projeto, como canais de acesso, restrições de cópia ou testes adicionais, devem ser cumpridas além destas regras. Suspeitas de incidente identificadas na execução destes procedimentos seguem o Plano de resposta a incidentes.

1 Concessão, revisão e revogação de acessos

Concessão

A concessão segue as etapas da Política de segurança da informação. O pedido identifica a pessoa ou o serviço, o sistema e o ambiente, o perfil, a justificativa, a duração e quem aprova. O responsável pelo serviço ou pela informação deve aprovar o pedido, e quem administra o sistema deve conceder o perfil mínimo e confirmar o uso de MFA antes de liberar o acesso de uma pessoa. O acesso administrativo exige justificativa distinta do acesso operacional.

Quando o sistema atende a mais de um cliente, deve-se confirmar que o perfil concedido não permite consultar dados de outros clientes. O registro no inventário de acessos não deve conter senhas, tokens ou conteúdo de clientes.

Cada conta de serviço deve ter responsável, sistema, escopo, data de revisão e procedimento de substituição da credencial. Credenciais não podem ser enviadas por e-mail nem anexadas a registros; os segredos ficam no cofre de segredos do provedor de nuvem ou na configuração protegida do pipeline de integração contínua.

Revisão periódica

Ao menos trimestralmente e sempre que houver mudança de função, o responsável pela segurança da informação deve revisar as contas, os grupos, as funções, as chaves e os acessos temporários de cada sistema. O responsável por cada sistema ou informação deve confirmar a necessidade de cada acesso, os acessos desnecessários devem ser removidos e o resultado deve ser registrado com a data, os sistemas revisados e as alterações feitas.

Desligamento e término da atuação

Quando um profissional é desligado ou deixa de atuar em um serviço, a revogação começa imediatamente após a comunicação, com meta de conclusão em até uma hora, e não depende da devolução de equipamentos ou informações. A revogação segue as etapas abaixo:

1. Registrar a data e a hora da comunicação e identificar, no inventário de acessos, os sistemas e serviços aos quais a pessoa tinha acesso.
2. Bloquear as contas da pessoa no e-mail e na identidade corporativos, no provedor de nuvem, no banco de dados gerenciado, na organização de repositórios de código, nos provedores de inteligência artificial e nos demais serviços com informações da Hineh ou de clientes. Nos sistemas e canais de acesso administrados por clientes, solicitar ao cliente a remoção do acesso.
3. Encerrar as sessões ativas e revogar tokens, chaves de acesso e credenciais pessoais de banco de dados.
4. Remover a pessoa de grupos, funções e repositórios de arquivos compartilhados.
5. Avaliar a rotação dos segredos conhecidos pela pessoa e registrar a decisão.
6. Registrar a data e a hora de cada revogação e a verificação do bloqueio, feita por outra pessoa quando houver alguém disponível.
7. Solicitar a devolução dos bens e das informações e a exclusão verificável das cópias autorizadas, conforme a Política de segurança da informação.

A comunicação tardia de um desligamento e a revogação concluída depois da meta devem ser registradas com a causa e as correções adotadas.

2 Equipamentos

Antes da liberação de acesso, o equipamento usado em atividades profissionais, inclusive o equipamento pessoal autorizado, deve ser registrado no inventário com proprietário, identificador, sistema operacional e versão, situação do suporte, criptografia do disco, antivírus ou EDR, firewall, bloqueio automático de tela e atualizações. O registro guarda também o aceite de uso profissional e a autorização de acesso. A evidência pode ser uma exportação do sistema ou capturas de tela datadas, com o nome do equipamento reduzido e sem chaves de recuperação.

O cumprimento dos requisitos de equipamento da Política de segurança da informação deve ser conferido mensalmente e registrado no inventário. As atualizações de segurança do sistema operacional e do navegador seguem os prazos da seção 3.

Equipamentos não cadastrados, de terceiros, sem suporte vigente ou com integridade comprometida não podem acessar sistemas ou informações da Hineh e de clientes. Dados de

clientes não podem ser sincronizados com armazenamento pessoal, inclusive no equipamento pessoal autorizado.

Equipamento perdido, infectado ou fora dos requisitos deve ser desconectado dos acessos corporativos até a regularização, com o encerramento das sessões e a revogação das credenciais nele utilizadas quando houver risco de exposição. Dados pessoais do proprietário não devem ser apagados sem autorização e fundamento. A perda ou a suspeita de comprometimento é tratada como incidente.

3 Vulnerabilidades e correções

Identificação e análise

As vulnerabilidades em código, dependências, imagens de contêiner e serviços utilizados devem ser identificadas pelas verificações automatizadas executadas a cada mudança no pipeline de integração contínua, pela verificação das imagens no envio ao registro de contêineres e pelos alertas de segurança dos provedores e dos repositórios de código. Em conjunto, essas fontes devem cobrir os segredos, as dependências e, quando houver, as imagens de cada serviço. As vulnerabilidades dos sistemas operacionais e dos navegadores dos equipamentos são tratadas pelas atualizações de segurança e pela conferência previstas na seção 2, nos prazos desta seção.

Os resultados e os alertas devem ser analisados quando recebidos, com a eliminação de duplicados e a avaliação da possibilidade de exploração e da exposição do ativo. Cada achado confirmado deve ser incluído no registro de vulnerabilidades, conforme os Registros de execução, com ativo, versão, severidade, impacto, responsável, prazo e ação.

Prazos de correção

Os prazos contam da confirmação do achado:

1. Severidade crítica: até 72 horas.
2. Severidade alta: até sete dias corridos.
3. Severidade média: até 30 dias.
4. Severidade baixa: até 90 dias.

Exploração ativa ou exposição pública exige contenção prioritária em até 24 horas, inclusive com a desativação da função afetada, se necessário. O indício de exploração contra sistemas da Hineh ou de clientes é tratado como incidente, conforme o Plano de resposta a incidentes, com contenção imediata quando o evento for crítico. A severidade pode ser elevada pelo contexto do cliente ou dos dados envolvidos.

Após a correção, a verificação que identificou o achado deve ser repetida, com registro da versão ou do commit, do resultado e da data.

Exceções

Quando não houver correção disponível ou ela não puder ser aplicada no prazo, a exceção segue a Política de segurança da informação: descrição do risco residual, medidas compensatórias, responsável, prazo de expiração de no máximo 90 dias e decisão da direção registrada.

4 Desenvolvimento, testes e implantação

Planejamento e desenvolvimento

Antes de desenvolver um serviço ou uma mudança relevante, o responsável pelo serviço deve definir os dados tratados, as fronteiras de autorização, os usos indevidos previsíveis e os critérios de segurança que os testes devem verificar. Alterações em autenticação, autorização, upload, exportação, integrações e isolamento entre clientes devem ser revisadas quanto a esses riscos antes do merge. O autor pode solicitar a revisão por outra pessoa, que não é condição para o merge.

O código-fonte e a infraestrutura de nuvem definida como código são versionados na organização de repositórios de código da Hineh. A branch principal de cada repositório bloqueia alterações diretas, push forçado e exclusão, e toda mudança chega a ela 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. Segredos não podem constar do código-fonte nem do repositório.

Os testes automatizados e o desenvolvimento dos serviços de backend devem usar bases locais ou temporárias, separadas da produção. Dados reais não devem alimentar o desenvolvimento; exceções precisam de minimização, justificativa e autorização. 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, deve ter identidade, base e chaves próprias.

Testes de segurança antes da produção

Antes da entrada em produção de um serviço novo ou de uma mudança relevante, os critérios de segurança definidos no planejamento devem ser verificados por testes automatizados ou por verificações registradas. Conforme o risco do serviço, os testes cobrem a autorização e o isolamento entre clientes, a validação de entradas e arquivos, o tratamento de segredos e a ausência de dados sensíveis nos registros. Os testes usam dados sintéticos ou um conjunto autorizado e minimizado. A aprovação funcional de um cliente não substitui essas verificações.

Implantação e reversão

O merge não publica automaticamente. A publicação dos serviços web e de backend usa a ferramenta de release aprovada, que exige a cópia local da branch principal limpa e igual à versão remota e confere a origem dos commits antes de alterar a produção. Os serviços de backend são publicados como imagens de contêiner imutáveis, verificadas quanto a vulnerabilidades ao serem enviadas ao registro, e os achados seguem a seção 3. A publicação de aplicativos nas lojas deve partir de uma versão da branch principal aprovada nas verificações automatizadas do repositório. Mudanças de infraestrutura exigem a conferência do plano antes da aplicação, e exclusões ou substituições destrutivas de recursos são bloqueadas na operação diária. A publicação de cada serviço de backend gera um registro com a identificação do commit e da imagem, guardado em armazenamento privado. A publicação deve se limitar ao escopo aprovado no pull request.

Falhas de implantação dos serviços de backend acionam a reversão automática para a versão anterior. A recuperação manual de um serviço de backend usa uma publicação anterior registrada, cujo código pertence ao histórico da branch principal e cuja imagem corresponde ao

mesmo commit. Após a reversão, deve-se verificar a compatibilidade dos dados e confirmar o restabelecimento do serviço.

Mudanças emergenciais seguem o mesmo fluxo de pull request, verificações e publicação, com validações proporcionais à urgência e registro. A urgência não autoriza contornar as proteções operacionais.

5 Registros, monitoramento e prevenção de vazamento

Eventos registrados

Os serviços devem registrar autenticação, falhas de acesso, concessão e revogação de privilégios, leitura e exportação de informações sensíveis, alterações de configuração, exclusões e execução de tarefas. Cada registro deve conter data e hora em UTC, usuário ou serviço, cliente, ação, resultado, identificador pseudonimizado do objeto e identificador de correlação. Os registros não devem conter senhas, tokens, imagens ou o conteúdo integral de informações de clientes.

Retenção e proteção

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, com criptografia por chave gerenciada no serviço de chaves do provedor, 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.

As identidades das aplicações devem ter permissão apenas para gravar registros, sem apagá-los ou alterar sua retenção, e a leitura dos registros é restrita às pessoas autorizadas. Os registros necessários à investigação de um incidente devem ser preservados antes do fim de sua retenção, conforme o Plano de resposta a incidentes.

Alarmes e análise

Alarmes automáticos acompanham a execução dos serviços, os erros, o uso de recursos e as falhas na coleta dos registros de acesso. Cada alarme que exige ação deve ter um responsável e notificá-lo por um meio que permita ação imediata nos eventos críticos. A entrega da notificação deve ser testada antes da entrada em produção de cada serviço.

Os alertas e os eventos suspeitos devem ser analisados pelos responsáveis quando recebidos. A Hineh não mantém equipe de monitoramento em regime contínuo, e os prazos de resposta contam da ciência, conforme o Plano de resposta a incidentes. O alerta ou evento que indique possível incidente, como acesso indevido, credencial exposta ou vazamento, deve ser registrado e tratado conforme esse plano.

No desenho de cada serviço que trate informações confidenciais, o responsável pelo serviço deve avaliar, conforme o risco, a criação de alertas para acessos anormais, exportações em volume incomum e destinos de saída não autorizados.

Prevenção e detecção de vazamento

A prevenção de vazamento combina os controles da Política de segurança da informação: acesso mínimo e nominal, MFA, criptografia, bloqueio de acesso público ao armazenamento, serviços em sub-redes privadas, canais aprovados e as restrições de uso das informações. A detecção deve se apoiar na verificação de segredos no pipeline de integração contínua dos repositórios de serviços em produção, que identifica credenciais incluídas no código antes do merge, nos registros de acesso, que permitem rastrear o acesso às informações, e no relato imediato de suspeitas por qualquer profissional.

6 Evidências e revisão

Cada execução de controle deve gerar um registro com identificador, data e fuso horário, escopo, responsável, origem, resultado, versão do documento ou do sistema e pendências. Exportações administrativas e relatórios verificáveis são preferidos; capturas de tela são complementares e devem conter contexto suficiente para identificar o sistema, a data e a configuração. Segredos, dados de terceiros e identificadores desnecessários devem ser ocultados sem retirar a informação que comprova o controle.

As evidências devem ficar em pasta corporativa com acesso nominal e ser guardadas por 24 meses, ressalvados os prazos legais ou contratuais, conforme a Política de segurança da informação. Os registros de incidentes seguem os prazos do Plano de resposta a incidentes.

O índice de evidências deve ser conferido antes de cada envio a cliente ou auditoria e na revisão anual deste manual, para confirmar que cada evidência continua válida. Formulários em branco e regras escritas não comprovam a execução de um controle; cada controle novo precisa de seus próprios registros.

A direção deve revisar este manual ao menos anualmente e após incidente relevante ou mudança de arquitetura, de ferramenta 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.