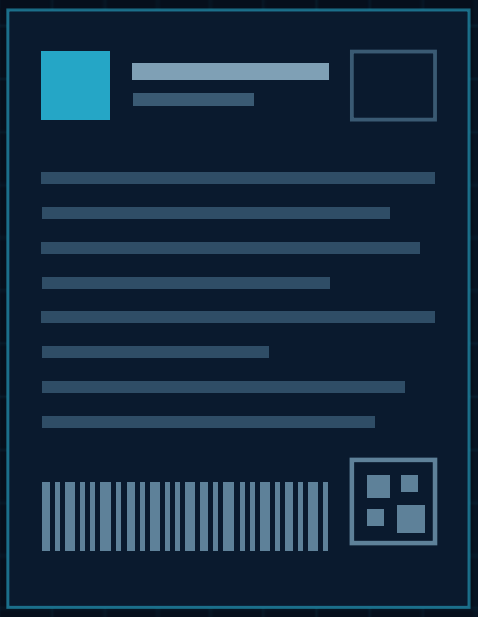
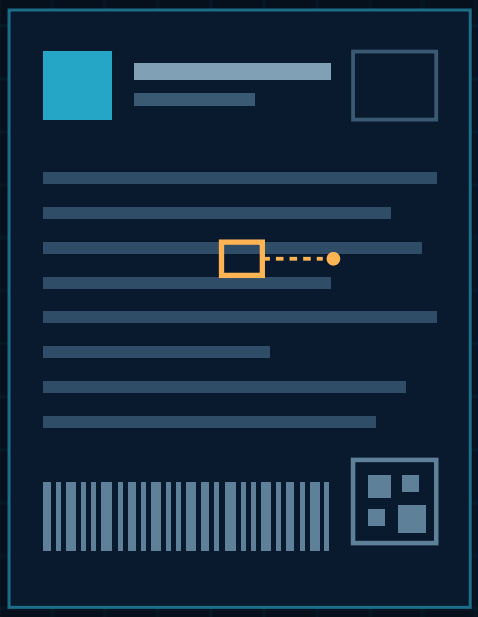
MetaScope

Versão 2, novembro de 2026

Arquivo original



Cópia com um caractere alterado



`81a76d130c92533a8136ed41471a555c`
`c5586ecdfc50fc2330dfece4c78d1c99`

≠

hashes diferentes

`d1f5a9906dbd1ca7a7e320af59b145de`
`b7ceebf8bee0495985236a99ebfaadcf`

À vista, os dois arquivos são iguais. Um caractere mudou, e o hash mudou em 61 dos 64 caracteres.

Quando o arquivo engana

Guia prático de segurança e integridade digital para empresas

Como conferir boletos, notas, contratos, fotos e links antes de agir, e como guardar o que importa para provar depois.

Comece pela sua área

Para escritórios de contabilidade, advocacia, RH, imobiliárias, construtoras, transportadoras e qualquer empresa que recebe e envia arquivos pela internet.

Qual é a sua área?

Escolha o seu setor. Cada página mostra os riscos da área e o que fazer, em poucos passos.

Contabilidade e financeiro
Boletos, notas fiscais e comprovantes
p. 9

Advocacia e jurídico
Contratos, provas de clientes e intimações
p. 10

Recursos humanos
Documentos funcionais, atestados e currículos
p. 11

Imobiliárias, obras e transporte
Fotos e vídeos de vistorias, obras e entregas
p. 12

Outra empresa
Comece pelo essencial
p. 3

Quem vai implantar
Checklist, modelos e política interna
p. 16

Desconfiou de um arquivo agora?
Vá direto ao protocolo. Página 4.

O essencial

Guarde o arquivo original

Não abra e salve de novo, não converta, não reenvie por aplicativo que comprime.

Não clique em link inesperado

Copie o endereço e verifique antes.

Confirme o que é crítico por outro canal

Valor, beneficiário, chave da nota e entrada do dinheiro se confirmam no banco, no portal oficial ou por um telefone que você já conhecia.

Anote o hash dos arquivos importantes

É a impressão digital do arquivo.

Registre no Guardião o que vai precisar provar depois

Contratos, vistorias, fotos de obra, comprovantes de entrega.

Desconfiou? Pare

Não pague, não assine, não encaminhe. Siga o protocolo.

Três ideias para entender o resto

Arquivo original

É o arquivo como foi gerado ou recebido. Aplicativos de mensagem e e-mail podem recomprimir fotos e apagar informações escondidas no arquivo.

Verificar não é provar

Verificar é procurar sinais de problema. Sem alertas quer dizer que nada foi encontrado, não que o documento é legítimo. Provar exige confirmar na fonte.

Hash

Código de 64 caracteres (SHA-256) calculado a partir do conteúdo. Se um único caractere do arquivo mudar, o hash muda, como na capa. Hashes iguais, arquivos idênticos. O hash não diz quem fez o arquivo nem se o conteúdo é verdadeiro.

Desconfiou? Pare aqui.

Use quando uma análise apontar problema, quando dois hashes não baterem ou quando algo parecer estranho.

1	**Interrompa**	Não pague, não assine, não encaminhe, não use o arquivo.
2	**Preserve**	Não edite, converta ou sobrescreva o arquivo recebido.
3	**Registre**	Data, canal, remetente declarado, responsável e operação.
4	**Confirme**	Fale com o emissor por um canal independente.
5	**Compare**	Recalcule o hash e confirme que são as mesmas versões.
6	**Escale**	Gestor, financeiro, jurídico ou segurança da informação.
7	**Documente**	O que foi verificado, o que foi decidido e por quem.

Outro canal é

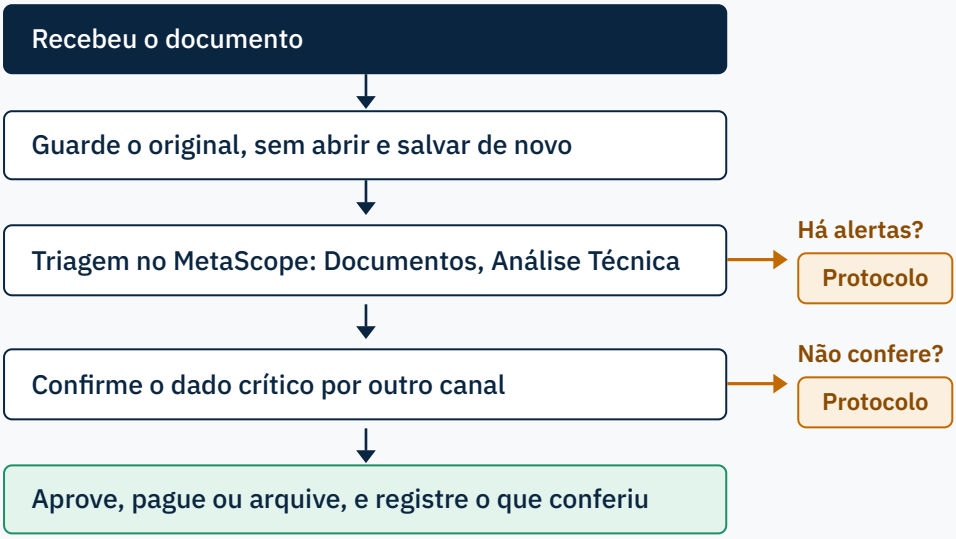
O aplicativo do seu banco, conferindo o beneficiário antes de pagar; o portal oficial, como a consulta da NF-e; um telefone ou endereço que você já conhecia. Nunca o contato que veio na mensagem suspeita.

Atenção

Hashes diferentes não provam fraude. Regravar, converter ou comprimir um arquivo também muda o hash. Mas a causa precisa ser esclarecida antes de seguir.

Receber com cuidado

Quando usar Boletos, notas, comprovantes, contratos e documentos de fornecedores, clientes ou candidatos.



No MetaScope

A Análise Técnica examina a estrutura, os metadados e os sinais de edição do arquivo, sem créditos e sem inteligência artificial. Em boletos e notas fiscais, faz conferências próprias (veja Contabilidade e financeiro).

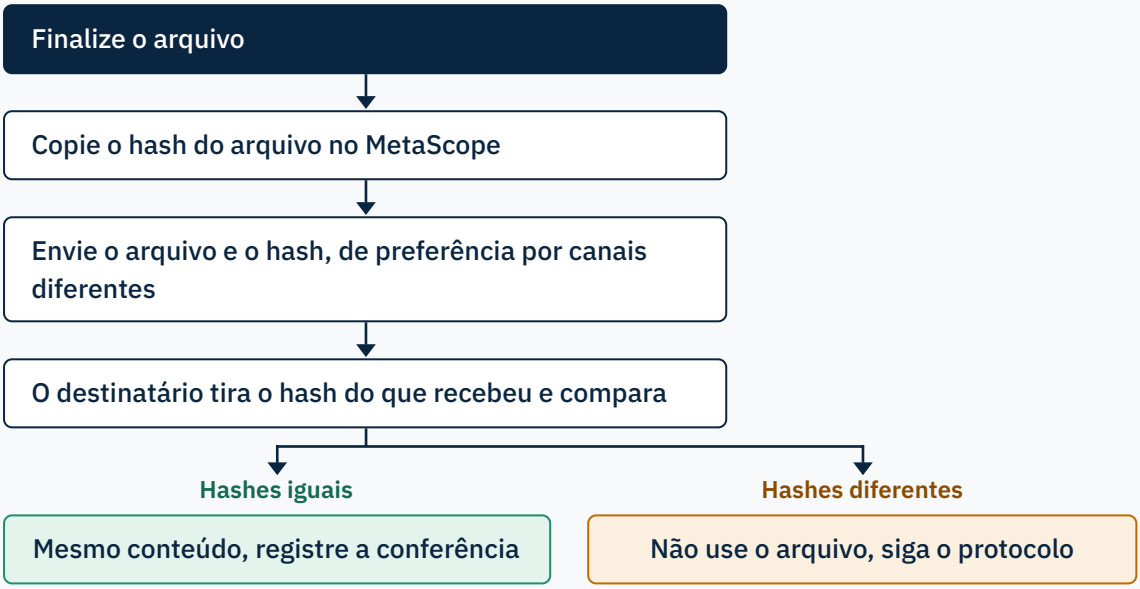
O que isso não prova

Sem alertas não quer dizer que o documento é autêntico nem que a cobrança é devida. O MetaScope não confirma nada no banco, na SEFAZ ou com o emissor.

Próximo passo Contabilidade e financeiro Enviar com selo Protocolo

Enviar com selo

Quando usar Contratos, pareceres, boletos, relatórios e projetos. Todo arquivo que o destinatário precisa receber sem alteração.



Como tirar o hash. Quem envia e quem recebe faz igual:

1. Entre no MetaScope com uma conta gratuita.
2. Abra **Documentos** e mantenha o modo **Análise Técnica**, marcado como “Sem créditos”.
3. Envie o arquivo e clique em **Copiar hash**.
4. Compare os 64 caracteres inteiros.

Fotos e vídeos: mesmo caminho, em **Mídia**. Limites: PDF até 25 MB; Word, Excel, PowerPoint e CSV até 15 MB; imagens e vídeos até 100 MB.

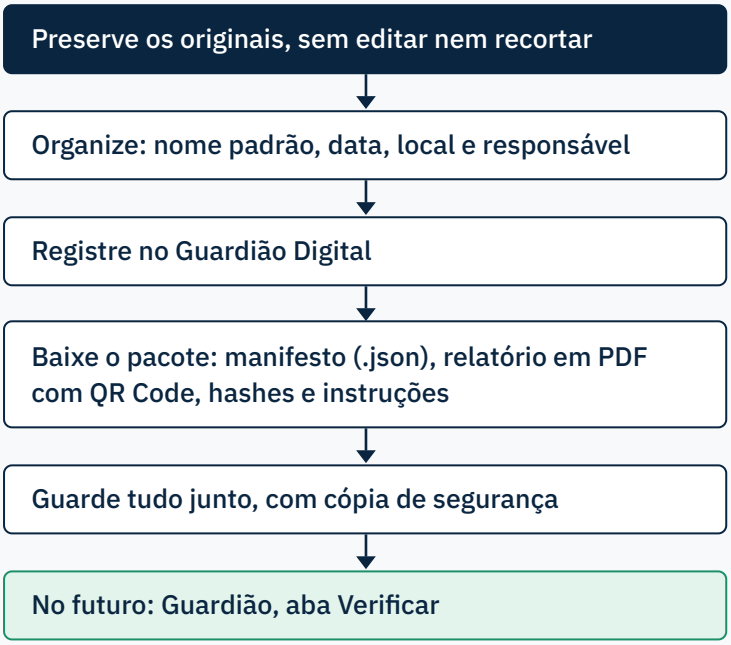
> **Atenção**
> Se o arquivo e o hash viajam juntos e o canal for invadido, quem trocou o arquivo pode trocar o hash. No mesmo canal, o hash protege contra erro, não contra quem controla a conversa.

> **O que isso não prova**
> Hashes iguais mostram arquivos idênticos. Não mostram que o documento é legítimo nem que a cobrança é devida.

Próximo passo Modelo de mensagem Guardar para provar

Guardar para provar depois

Quando usar Contratos fechados, documentos funcionais, fotos de vistoria e de obra, comprovantes de entrega e ocorrências.



No MetaScope

O Guardião calcula o hash no seu navegador, sem enviar o conteúdo dos arquivos, e gera um manifesto com assinatura digital, data e QR Code. Verificar depois não exige login nem créditos.

- **Custo:** de 1 a 5 créditos por operação, conforme o número de arquivos (até 50). Exige login.
- **O que vai ao servidor:** hash, nome, tamanho e tipo de cada arquivo. Não use dados pessoais no nome.
- **Prazo:** a página do QR Code vale 12 meses e é apagada cerca de 30 dias depois. O manifesto (.json) baixado continua verificável sem o MetaScope. Guarde-o junto dos originais.

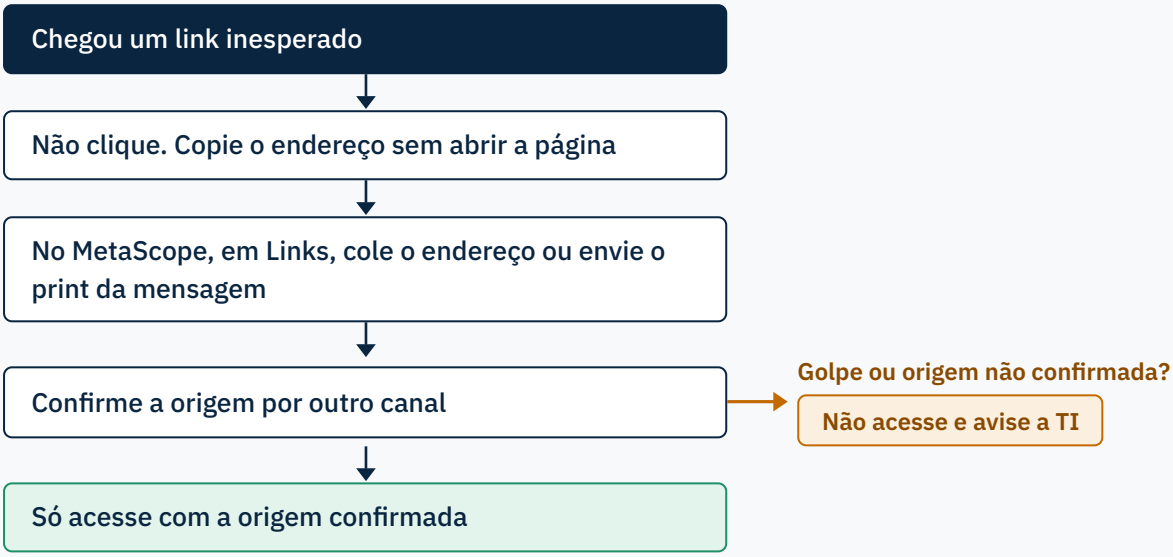
O que isso não prova

Quando o arquivo foi criado ou fotografado, quem é o autor ou se o conteúdo é verdadeiro. O selo atesta que esses hashes foram registrados naquela data. Não é carimbo do tempo da ICP-Brasil nem cadeia de custódia.

Próximo passo Imobiliárias, obras e transporte Recursos humanos

Verificar um link

Quando usar Links inesperados em e-mail, SMS, WhatsApp e redes sociais, supostas intimações, pastas compartilhadas e pedidos de “atualização cadastral”.



No MetaScope

O verificador analisa o texto do endereço: imitação de marcas, letras de outros alfabetos, destino escondido dentro do link e idade do domínio. Ele não abre a página nem segue redirecionamentos, para não expor você. Se a mensagem mostrava um botão diferente do endereço real, envie o print.

O que isso não prova

Sem alertas, o link não está garantido. A verificação não substitui o antivírus, a política da empresa nem a confirmação da origem.

Próximo passo Advocacia e jurídico Protocolo

Contabilidade e financeiro

Situação O escritório encaminha o boleto do fornecedor e o cliente paga. Depois descobre que o código de barras era de outra conta, ou que o QR Code Pix levava a outro recebedor.

Risco Pagar para a conta errada, escriturar nota inválida, dar baixa por comprovante falso.

Quando chega	Faça isto
Boleto	Triagem em Documentos. Antes de pagar, confira beneficiário e valor no aplicativo do banco.
Nota fiscal	O MetaScope analisa o DANFE em PDF; o XML, não. Consulte a chave no Portal da NF-e.
Comprovante	Confira a entrada do dinheiro no extrato. Comprovante perfeito não prova pagamento.
Boleto para o cliente	Envie com o hash e peça que ele confira o beneficiário no banco.

No MetaScope, no boleto

Confere os dígitos do código de barras e da linha digitável; se o valor impresso é o mesmo do código; o CPF ou CNPJ do beneficiário e, se for CNPJ, a situação na base pública da Receita; o Nosso Número e a Carteira, nos bancos de layout conhecido; e se o QR Code Pix bate com o boleto, sem acessar o endereço do Pix. Na nota, confere a chave de acesso e o CNPJ do emitente. “Não verificável” não é problema: o dado não pôde ser lido com segurança.

O que isso não prova

O MetaScope não consulta a SEFAZ nem o banco. Essa confirmação é sempre sua.

Próximo passo Receber com cuidado Enviar com selo

Advocacia e jurídico

Situação Chega uma “intimação” com link para uma pasta compartilhada, num endereço parecido com o de um órgão público. Ou, meses depois, ninguém sabe dizer qual versão do contrato foi enviada.

Risco Discussão sobre versões, perda do valor de uma prova por manuseio inadequado, golpe da falsa intimação.

Quando	Faça isto
Vai enviar contrato, parecer ou procuração	Hash do arquivo final e orientação ao destinatário. Nos documentos relevantes, registro no Guardião.
Recebe arquivos de cliente	Peça os originais, anote origem, data e quem recebeu, registre no Guardião e trabalhe em cópias.
Recebe link de intimação ou pasta	Não clique. Verifique o endereço e confirme a origem por canal independente.
A questão exige conclusão técnica	Encaminhe a perícia. O MetaScope tem o serviço de Laudo Pericial, feito por perito humano.

> **O que isso não prova**
> O registro de integridade não substitui assinatura eletrônica, certificação digital, reconhecimento de firma nem os requisitos legais do documento. Não comprova autoria nem concordância das partes. O relatório em PDF do aplicativo não é laudo pericial.

Próximo passo Enviar com selo | Guardar para provar | Verificar um link

Recursos humanos

Situação Numa controvérsia trabalhista, ninguém consegue demonstrar qual versão de uma advertência existia na época. Ou chega um atestado que parece estranho.

Risco Não conseguir demonstrar o documento, tratar dado sensível de forma inadequada, abrir link malicioso de “candidato”.

Quando	Faça isto
Documentos funcionais: advertências, termos, entrega de equipamentos	Registro no Guardião. Guarde original e manifesto com acesso restrito. Defina o prazo de guarda com seu jurídico ou contador.
Atestados e documentos de saúde	São dados sensíveis (LGPD). Só envie para análise se houver dúvida real. Na dúvida, confirme com quem emitiu.
Links de candidatos	Não abra links inesperados. Verifique o endereço e peça documentos por canal institucional.

Atenção

Nas análises do MetaScope, o arquivo passa pelos servidores da plataforma. Em PDF com assinatura digital, a validação oficial envia o arquivo ao ITI, do governo. A opção pode ser desmarcada antes do envio.

O que isso não prova

O registro mostra que o arquivo não mudou. Não prova que o empregado recebeu, leu ou concordou. Para isso, use assinatura ou confirmação de recebimento.

Próximo passo Guardar para provar Privacidade

Imobiliárias, obras e transporte

Situação Seis meses depois da vistoria, inquilino e imobiliária discordam do estado do imóvel. Cada um tem fotos, e ninguém consegue demonstrar que as suas são as de antes. O mesmo acontece com a foto da obra e o comprovante de entrega.

Risco Não conseguir demonstrar que as imagens apresentadas depois são as mesmas do registro.

Passo	Faça isto
Capture	Com o aparelho definido pela empresa. Guarde o original, sem editar nem recortar.
Organize	Por imóvel, obra ou ordem de transporte, etapa, data e responsável. Sem dados pessoais no nome.
Registre	No Guardião, logo após a captura e em lotes. Quanto mais perto da captura, mais útil.
Vincule	Ao laudo de vistoria, ao diário de obra, à ordem de transporte ou à nota fiscal.
Compartilhe	Envie cópias às partes. Os originais ficam guardados.
Na contestação	Guardião, aba Verificar, com o manifesto e os arquivos apresentados.

Fotos ou vídeos recebidos de terceiros: peça o original e use **Mídia** para examinar metadados e sinais técnicos. Vídeos até 100 MB; recorte o trecho relevante e guarde o vídeo inteiro.

> **O que isso não prova**
> Quando, onde ou por quem a foto foi feita, nem que a mercadoria foi entregue. A data do registro no Guardião é a de quando você registrou, não a da captura. Isso depende dos registros da operação: diário de obra, ordem de transporte, identificação do recebedor.

Próximo passo Guardar para provar Enviar com selo

No MetaScope

O MetaScope Forense é uma plataforma brasileira de análise forense digital.

Recurso	Conta	Créditos
Academia Forense e ferramentas gratuitas	Não	● Não
Análise Técnica: Documentos, Mídia e Links	Gratuita	● Não
Verificar um registro do Guardião	Não	● Não
Registrar no Guardião	Sim	● De 1 a 5 por operação
Deep Research: análise aprofundada com IA	Sim	● De 1 a 4 por análise, após 5 acessos iniciais nos primeiros 7 dias
Laudo Pericial, feito por perito humano	Sim	● Cobrado à parte

Análise Técnica é a triagem rápida, sem inteligência artificial e sem créditos. **Deep Research** é a leitura aprofundada para casos sensíveis: usa IA, consome créditos e pode variar de uma execução para outra em casos limítrofes.

O relatório em PDF registra a triagem: o hash do arquivo e as fontes oficiais de fato consultadas. Hoje, só o validador do ITI, para PDF assinado; SEFAZ e SEI/PJe aparecem como “Não verificado”. O relatório não é laudo pericial.

Documentos
app.metascopeforense.com/document-forensics

Mídia
app.metascopeforense.com/forensic

Links
app.metascopeforense.com/link-checker

Guardião
app.metascopeforense.com/guardian

Créditos
app.metascopeforense.com/pricing

Academia Forense
app.metascopeforense.com/academy

O que sai do seu computador

Ferramenta	O que acontece
Academia e ferramentas gratuitas	Rodam no seu navegador. Nada é enviado.
Guardião	O conteúdo não sai. Vão o hash, o nome, o tamanho e o tipo de cada arquivo.
Análise Técnica	O arquivo vai ao MetaScope e é processado em memória, sem IA, sem ser gravado em disco. Vídeos usam um arquivo temporário, apagado em seguida.
PDF com assinatura digital	Por padrão, vai inteiro ao validador do governo (ITI). Se for sigiloso, desmarque a opção antes de enviar.
Links	O texto do endereço é analisado e o domínio é consultado em registros públicos. A página não é aberta.
Deep Research	Envia conteúdo à OpenAI: um trecho do documento (boleto escaneado: o arquivo inteiro), a imagem inteira com o GPS, se houver, ou três quadros do vídeo. O endereço do link também vai ao Google Web Risk.

O que o MetaScope guarda: de cada análise, o nome do arquivo, o tipo, o tamanho, o hash e o resumo do resultado. O nome e o resumo são apagados depois de 12 meses; o restante fica 5 anos, assim como o registro de custódia (usuário, IP, nome do arquivo e hash). Detalhes na Política de Privacidade.

A LGPD trata de obrigações legais; este guia traz recomendações técnicas. Defina com o seu jurídico o que pode ser enviado a serviços externos.

Hash sem enviar o arquivo

Para arquivos sigilosos ou de outros tipos, como XML ou ZIP, calcule no próprio computador. O resultado é o mesmo SHA-256 do MetaScope.

Windows: `certutil -hashfile "arquivo" SHA256`

Linux ou macOS: `sha256sum "arquivo"`

O que nada disso prova

O hash não é certificado de autenticidade

Mostra que dois arquivos são idênticos. Não mostra autoria, origem, veracidade nem data de criação.

O registro do Guardião não é cadeia de custódia nem assinatura

Registra que certos hashes foram declarados e selados numa data.

Triagem não é perícia

Scores e alertas são indícios e riscos, não decisões jurídicas. Quando a questão exigir conclusão técnica, procure um profissional habilitado.

Sem alertas não é garantia

Um boleto consistente pode ser fraude. Uma nota pode não existir na SEFAZ. Um link limpo pode vir de quem você não esperava.

Metadado não decide nada sozinho

A ausência não prova fraude, e a presença não prova autenticidade.

Este guia é orientação geral

Não é parecer jurídico, auditoria, laudo pericial nem certificação, e não substitui as políticas e normas da sua organização.

Para quem vai implantar

Marque o que a sua empresa já faz. O que ficar em branco é o próximo passo.

Receber

- [ ] Há um canal oficial para receber documentos?
- [ ] Os arquivos originais são guardados?
- [ ] Documentos relevantes passam por triagem?
- [ ] Dados críticos são confirmados por canal independente?
- [ ] Existe um protocolo para divergências?

Enviar

- [ ] A versão final é conferida antes do envio?
- [ ] O hash é calculado depois de finalizar o arquivo?
- [ ] O destinatário recebe instruções para conferir?
- [ ] O canal de envio combina com a sensibilidade do documento?

Guardar

- [ ] Está definido o que preservar e por quanto tempo?
- [ ] Manifestos e hashes ficam junto dos originais?
- [ ] Há cópia de segurança e acesso restrito?
- [ ] Alguém confere de tempos em tempos se os arquivos continuam íntegros?

Links e pedidos

- [ ] A equipe sabe que não deve clicar em link inesperado?
- [ ] Há um canal para relatar tentativas de golpe?
- [ ] Pedidos de pagamento são confirmados por outro canal?

Governança

- [ ] Cada procedimento tem um responsável?
- [ ] A equipe recebe orientação periódica?
- [ ] Os controles são proporcionais ao risco?
- [ ] O tratamento de dados pessoais segue a LGPD?

Modelos para copiar

Mensagem ao destinatário

> Encaminhamos o arquivo em anexo. Como medida adicional de segurança, registramos o hash SHA-256 do arquivo antes do envio.
>
> **SHA-256:** `INSERIR O HASH COMPLETO`
>
> Para conferir: crie uma conta gratuita no MetaScope Forense (app.metascopeforense.com), abra **Documentos**, mantenha o modo **Análise Técnica** (sem créditos), envie o arquivo que você recebeu e compare o **Hash SHA-256** com o código acima. Os 64 caracteres devem ser idênticos.
>
> Essa conferência mostra que o arquivo recebido é idêntico ao enviado. Ela não substitui a conferência do beneficiário, dos valores e dos dados junto à instituição responsável.

Para boletos, acrescente: *"Antes de pagar, confira no aplicativo do seu banco se o beneficiário é o esperado."*

Ficha de registro de envio

Campo	Informação
Operação	
Arquivo	
Responsável pelo envio	
Data e hora	
Hash SHA-256 completo	
Destinatário	
Canal do arquivo e canal do hash	
Resultado da conferência	Correspondente / Divergente / Não realizada

Política interna resumida

Política de verificação e integridade de arquivos digitais

A organização adota procedimentos de verificação e preservação de arquivos digitais nas operações relevantes, em especial pagamentos, contratos, documentos fiscais, registros de entrega, vistorias, ocorrências e documentos enviados a terceiros.

Sempre que aplicável, os colaboradores devem:

1. Preservar os arquivos originais recebidos ou produzidos.
2. Confirmar informações críticas por canais independentes.
3. Verificar links suspeitos antes de acessá-los.
4. Usar ferramentas de análise quando a natureza do arquivo justificar.
5. Calcular e registrar o hash dos arquivos que precisarão ser conferidos depois.
6. Informar ao destinatário como conferir os arquivos enviados com hash.
7. Comunicar divergências e suspeitas e seguir o protocolo de divergência.
8. Respeitar a confidencialidade, a proteção de dados e o controle de acesso, inclusive no envio de arquivos a serviços externos.

Estes procedimentos são proporcionais ao risco e não substituem as validações legais, fiscais, contábeis, técnicas ou profissionais de cada atividade.

A segurança digital também se constrói nos pequenos procedimentos de todos os dias.

MetaScope Forense

- Aplicação
- Apresentação institucional
- Documentação de uso e limites
- Política de Privacidade
- Ferramentas gratuitas

Referências

- Lei Geral de Proteção de Dados, Lei nº 13.709/2018
- Instituto Nacional de Tecnologia da Informação (ITI)
- Portal da Nota Fiscal Eletrônica
- NIST, Secure Hash Standard (FIPS 180-4)
- NIST, Cybersecurity Framework
- CERT.br, Cartilha de Segurança para Internet

Documento de orientação geral. Não constitui parecer jurídico, auditoria, laudo pericial, certificação de autenticidade ou substituto das políticas internas e normas aplicáveis a cada organização.

MetaScope