teztor



Dossiê de Segurança da Informação e Proteção de Dados

CANAL DE DENÚNCIAS TEZTOR | Versão 2.0 | Novembro de 2026

Segurança, confidencialidade, anonimato e governança de dados aplicados à operação do Canal Teztor.

1. Apresentação

A Teztor disponibiliza às empresas um canal externo de denúncias, independente, gratuito e acessível pela internet, destinado ao recebimento, registro, organização, triagem e encaminhamento de manifestações. A plataforma foi concebida para favorecer o relato seguro de irregularidades e apoiar a consolidação de ambientes corporativos éticos e íntegros.

A segurança da informação integra a arquitetura e a operação do Canal, combinando proteção criptográfica, autenticação, segregação de acesso, rastreabilidade, controles de confidencialidade e medidas de proteção de dados pessoais. Os mecanismos são organizados segundo os princípios de *privacy by design*, *security by design*, necessidade e menor privilégio.

2. Visão executiva da segurança

Dimensão	Medidas adotadas
Confidencialidade	Criptografia AES-256-GCM de campos sensíveis dos relatos e tráfego protegido por HTTPS/TLS.
Controle de acesso	Autenticação multifator, perfis específicos, vínculo entre usuários e empresas e autorização verificada no servidor.
Segregação	Isolamento lógico dos registros de cada empresa e acesso limitado a pessoas autorizadas.
Anonimato	Possibilidade de relato sem identificação e acompanhamento por protocolo e senha.
Evidências	Anexos em repositório privado, com acesso por links temporários após verificação de permissão.
Rastreabilidade	Registros de acessos, mensagens, alterações de status e eventos operacionais relevantes.
Governança	Papéis de Controladora e Operadora, retenção definida, gestão de subprocessadores e resposta a incidentes.

3. Infraestrutura tecnológica e armazenamento

O conteúdo dos relatos é hospedado em infraestrutura de nuvem gerenciada, utilizando Amazon Web Services (AWS), na região da Irlanda (eu-west-1), e serviços Supabase para banco de dados, autenticação e funções de servidor. A arquitetura utiliza banco de dados PostgreSQL dedicado ao projeto e controles de acesso lógico por empresa e por perfil.

As páginas do Canal são disponibilizadas em infraestrutura de distribuição web, com conexões protegidas por HTTPS/TLS. As operações que envolvem dados confidenciais são processadas por serviços de backend, responsáveis por validar a identidade, o perfil e a autorização de quem solicita acesso.

Os documentos e anexos são mantidos em armazenamento privado. Sua disponibilização depende de autorização contextual e da emissão de links temporários. A infraestrutura gerenciada também contempla rotinas automatizadas de backup e mecanismos de continuidade oferecidos pelos provedores contratados.

4. Criptografia e confidencialidade

- **Criptografia em repouso:** campos sensíveis dos relatos são cifrados por AES-256-GCM antes do armazenamento. O algoritmo combina confidencialidade e verificação de integridade do conteúdo criptografado.

- **Criptografia em trânsito:** as comunicações entre os navegadores e os serviços da plataforma são protegidas por HTTPS/TLS.
- **Proteção das chaves:** os segredos de criptografia são mantidos fora do código da aplicação e não são disponibilizados no navegador.
- **Decifragem controlada:** o acesso ao conteúdo sensível ocorre por funções protegidas de servidor, mediante validação de identidade, permissões e vínculo empresarial.
- **Confidencialidade operacional:** o acesso de pessoas da Teztor às manifestações é limitado às atividades necessárias à operação, triagem e encaminhamento, sob deveres de confidencialidade.

5. Identidade, autenticação e autorização

A Teztor aplica perfis de acesso distintos para denunciantes, representantes das empresas e administradores da plataforma. As permissões são verificadas no serviço, e não apenas na interface apresentada ao usuário.

Perfil	Mecanismo de acesso e proteção
Denunciante	Registro sem cadastro obrigatório; acompanhamento por protocolo e senha, com consulta limitada ao próprio relato.
Empresa aderente	Acesso por usuário autorizado, senha e verificação adicional, com vínculo explícito à empresa correspondente.
Administração Teztor	Autenticação multifator por aplicativo autenticador, perfis administrativos segregados e renovação periódica de senhas.

Os fluxos de autenticação e recuperação empregam códigos temporários, expiração de credenciais e limitação de tentativas. Senhas de acompanhamento não são armazenadas em texto legível. O gerenciamento de perfis observa concessão e revogação controladas e o princípio do menor privilégio.

6. Anonimato e proteção do denunciante

O Canal admite denúncias anônimas, sem exigir nome, e-mail, telefone ou cadastro. Ao finalizar a manifestação, o denunciante recebe protocolo e senha de acompanhamento, que permitem consultar o andamento e trocar mensagens pelo próprio Canal sem identificação obrigatória.

O endereço IP não é armazenado no banco de dados associado ao protocolo nem disponibilizado à empresa para identificação do denunciante. O eventual processamento técnico transitório de informações de rede é empregado em mecanismos de segurança e prevenção de abuso, sem vinculação ao relato. A jornada de denúncia não utiliza ferramentas de rastreamento publicitário, como Google Analytics, Google Tag Manager ou pixels de marketing.

> A proteção do anonimato também depende do conteúdo voluntariamente fornecido. Informações narradas, circunstâncias específicas e propriedades de documentos anexados podem permitir identificação indireta. Por isso, a plataforma e suas orientações incentivam o envio apenas das informações necessárias à descrição dos fatos.

7. Gestão das denúncias e rastreabilidade

A manifestação pode ser encaminhada pelo formulário convencional ou pela Tezzy, assistente conversacional opcional. Após o registro, o conteúdo integra o fluxo de recebimento, triagem e encaminhamento aos Contatos Designados pela empresa aderente. A investigação, a avaliação dos fatos e a adoção de medidas corretivas, disciplinares ou legais permanecem sob responsabilidade da empresa.

O histórico de cada protocolo reúne comunicações, atualizações e registros de acompanhamento. As operações relevantes nos ambientes administrativo e corporativo produzem trilhas de auditoria com dados de autoria, data e ação, favorecendo rastreabilidade e prestação de contas.

A Teztor recomenda a designação de mais de um contato responsável, preferencialmente de áreas ou linhas hierárquicas distintas, para proporcionar tratamento adequado a situações de conflito de interesses. Cada empresa deve manter atualizada sua relação de pessoas autorizadas e proteger os arquivos e comunicações recebidos fora da plataforma.

8. Proteção contra ameaças cibernéticas

Risco	Proteções aplicadas
Acesso não autorizado	Autenticação multifator, segregação de perfis, autorização no backend e vinculação por empresa.
Tentativas de força bruta e automação abusiva	Limitação de tentativas, validade limitada de códigos e sessões e controles de frequência.
Manipulação de registros	Validações no servidor, regras de autorização e histórico das alterações relevantes.
Exposição de credenciais	Gestão de segredos fora do navegador e do código distribuído publicamente.
Anexos indevidos	Restrições de tamanho e formato, armazenamento privado e acesso temporário autorizado.
Exposição indevida de dados	Criptografia, segregação lógica, controle de acesso e minimização de informações.

Os mecanismos atuam de forma complementar, reduzindo as superfícies de exposição e fortalecendo a proteção das informações ao longo de seu ciclo de vida.

9. Inteligência artificial e Canal Tezzy

A Tezzy oferece uma modalidade opcional de atendimento conversacional para auxiliar o denunciante na organização e descrição dos fatos. O formulário padrão permanece disponível. A assistente não realiza investigações, não determina responsabilidades, não aplica medidas e não substitui a análise humana.

O fluxo da Tezzy incorpora orientações contra a inclusão desnecessária de dados pessoais, controles para mitigar tentativas de manipulação de instruções e proteções relacionadas à exposição de informações internas. O conteúdo estruturado é apresentado para revisão antes da conclusão do registro.

A solução utiliza modelo Google Gemini por meio de gateway de inteligência artificial, exclusivamente no fluxo escolhido pelo denunciante. O uso do conteúdo dos relatos para treinamento de modelos e para finalidades próprias do fornecedor é vedado pelos compromissos de tratamento aplicáveis.

> A Teztor não utiliza denúncias, anexos, evidências ou informações de apuração para comercialização, publicidade, benchmarking ou treinamento de inteligência artificial. Os dados são tratados para as finalidades relacionadas à prestação do serviço e nos limites das autorizações aplicáveis.

10. Proteção de dados pessoais e LGPD

No tratamento de informações relacionadas aos relatos, a empresa aderente atua, em regra, como Controladora, definindo a finalidade da apuração e as decisões sobre as informações recebidas; a Teztor atua como Operadora, executando as atividades necessárias ao serviço conforme as instruções da Controladora. Quanto aos seus próprios dados cadastrais e comunicações institucionais, a Teztor exerce as responsabilidades correspondentes de Controladora.

A operação observa os princípios de finalidade, adequação, necessidade, segurança, prevenção, transparência e responsabilização estabelecidos pela Lei nº 13.709/2018 (LGPD). As hipóteses legais de tratamento são definidas conforme a finalidade concreta e a natureza dos dados, incluindo, quando cabíveis, cumprimento de obrigação legal ou regulatória e exercício regular de direitos. Dados pessoais sensíveis eventualmente presentes nos relatos são tratados de acordo com as hipóteses específicas do artigo 11 da LGPD.

A plataforma não exige o preenchimento de campos de dados sensíveis para a apresentação de uma denúncia anônima. A Teztor coopera com as empresas aderentes no atendimento aos direitos dos titulares, preservados o sigilo das apurações, a segurança dos envolvidos e os direitos de terceiros.

11. Retenção, devolução e eliminação de dados

Como regra contratual, as informações dos relatos são retidas pelo período de cinco anos, contado do encerramento da apuração ou do último registro no protocolo, ressalvadas instruções expressas da Controladora e hipóteses de conservação por prazo legal diferente.

No encerramento da adesão, a empresa pode solicitar a devolução dos dados sob sua responsabilidade. O procedimento contratual prevê devolução ou eliminação em até 30 dias, respeitadas as hipóteses de guarda necessárias ao cumprimento de obrigações legais e regulatórias ou ao exercício regular de direitos. A eliminação ou anonimização é realizada conforme as regras aplicáveis ao tratamento.

12. Subprocessadores e transferências internacionais

A prestação do Canal envolve fornecedores especializados, com funções delimitadas e compromissos de proteção de dados. A infraestrutura principal dos relatos permanece localizada na Irlanda, enquanto serviços complementares podem envolver operações em outras jurisdições.

Fornecedor	Finalidade	Localização operacional
Amazon Web Services (AWS)	Infraestrutura de nuvem e armazenamento	Irlanda (eu-west-1)
Supabase	Banco gerenciado, autenticação e funções de servidor	Irlanda (eu-west-1)
Lovable	Hospedagem e distribuição das páginas web	Estados Unidos / CDN global
Resend	Envio de e-mails transacionais, códigos e notificações	Estados Unidos / União Europeia
Google Gemini (gateway de IA)	Processamento opcional das mensagens da Tezzy	União Europeia / Estados Unidos
BrasilAPI	Consulta de dados públicos de CNPJ na adesão	Brasil

As transferências internacionais são disciplinadas por compromissos contratuais de proteção de dados e mecanismos jurídicos aplicáveis, incluindo acordos de tratamento e cláusulas de transferência pertinentes à LGPD.

Alterações relevantes de subprocessadores são comunicadas ao Contato Designado com antecedência contratual de 30 dias. A empresa dispõe de 15 dias para apresentar objeção fundamentada e pode encerrar a adesão sem ônus caso a objeção permaneça sem solução. Substituições emergenciais necessárias à segurança ou continuidade são comunicadas em até cinco dias úteis.

13. Resposta a incidentes e responsabilidades

A Teztor mantém procedimento de resposta a incidentes que abrange identificação, avaliação, contenção, recuperação e comunicação, de acordo com a natureza e a gravidade do evento. A plataforma registra eventos operacionais relevantes para apoiar a análise e a rastreabilidade.

> Em caso de incidente de segurança com potencial de risco ou dano relevante aos titulares, a Teztor comunica a empresa Controladora por escrito em até **48 horas** da ciência, com informações sobre o evento, os riscos identificados e as providências adotadas, observados os termos contratuais. A Controladora conserva suas responsabilidades legais perante a Autoridade Nacional de Proteção de Dados e os titulares, com cooperação da Teztor.

A segurança é uma responsabilidade compartilhada. À Teztor competem os controles técnicos e organizacionais de sua operação; às empresas aderentes, a gestão de seus usuários autorizados, a proteção de suas credenciais e dispositivos, a condução das apurações e a guarda adequada de informações exportadas ou encaminhadas fora do Canal.

14. Compromisso institucional

A Teztor foi criada para ampliar o acesso de empresas brasileiras a instrumentos profissionais de integridade, sem que o custo de implantação de um canal de denúncias seja uma barreira. A gratuidade do serviço não depende da comercialização dos dados dos usuários ou das informações contidas nas manifestações.

A confidencialidade, a proteção do denunciante e o tratamento responsável das informações orientam a atuação da Teztor e integram o compromisso de oferecer uma solução segura, acessível e alinhada às exigências de integridade corporativa e proteção de dados.

Canal institucional para questões de segurança e privacidade: **contato@teztor.com.br** | **www.teztor.com.br**