DOCUMENTO PÚBLICO

Política de Divulgação Responsável de Vulnerabilidades

Como reportar vulnerabilidades de segurança de forma responsável.

LEXXEN LTDA — CNPJ 63.987.111/0001-53
Rua 15, nº 721, Quadra H12, Lote 12, Sala 1, Setor Marista — Goiânia/GO — CEP 74.150-020
Versão 1.0 · Vigência 31 de agosto de 2026 · compliance@lexxen.com

1. Nosso compromisso

1.1. A **LEXXEN LTDA**, CNPJ 63.987.111/0001-53, reconhece o valor do trabalho da comunidade de segurança e mantém canal aberto para o **reporte responsável** de vulnerabilidades.

1.2. Quem reporta de boa-fé e segue esta Política **não será alvo de medidas legais** pela Lexxen (seção 5).

1.3. Esta Política é pública e vale para qualquer pessoa, no Brasil ou no exterior.

English summary: Lexxen welcomes good-faith security research. Report vulnerabilities to compliance@lexxen.com. Researchers who follow this policy will not face legal action from Lexxen. See Section 5 for the safe harbor terms.

---

2. Escopo

2.1. Dentro do escopo

- Domínio **www.lexxen.com** e subdomínios operados pela Lexxen
- Aplicações web e aplicativos móveis da Lexxen
- APIs públicas da Lexxen
- Infraestrutura sob controle direto da Lexxen

Fora do escopo	Por quê
Sistemas de **parceiros** (instituições de pagamento, PSAV, emissores de cartão)	não são controlados pela Lexxen — reporte diretamente à instituição; podemos intermediar o contato
Serviços de terceiros (provedores de nuvem, e-mail, CDN)	têm seus próprios canais
Ataques de **negação de serviço** (DoS/DDoS)	causam indisponibilidade real a usuários
Engenharia social contra colaboradores, clientes ou parceiros	envolve pessoas, não sistemas
Ataques físicos a instalações	idem
Spam, força bruta e testes automatizados de alto volume	degradam o serviço
Relatos apenas de saída de scanner, sem impacto demonstrado	não caracterizam vulnerabilidade
Ausência de *headers* ou boas práticas sem exploração demonstrável	idem

3. Regras de conduta

3.1. Ao pesquisar, você **deve**:

a) agir de boa-fé, com o objetivo de **melhorar a segurança**; b) usar **apenas contas próprias** ou criadas para teste; c) **parar imediatamente** ao obter acesso a dado de terceiro, e reportar sem copiar, armazenar, divulgar ou transferir esse dado; d) limitar-se à prova de conceito mínima necessária para demonstrar o problema; e) evitar qualquer ação que degrade o serviço ou afete usuários reais; f) dar à Lexxen **prazo razoável** para corrigir antes de qualquer divulgação pública.

3.2. Você **não deve**:

a) acessar, modificar ou destruir dados que não sejam seus; b) exfiltrar dados — a comprovação se faz com evidência mínima, não com volume; c) usar a vulnerabilidade para obter vantagem, própria ou de terceiro; d) exigir pagamento como condição para revelar a falha — isso **não é pesquisa, é extorsão**; e) divulgar publicamente antes do prazo acordado.

4. Como reportar

4.1. Envie para **compliance@lexxen.com** com o assunto `[VULN]`.

4.2. Inclua:

Tipo de vulnerabilidade	ex.: XSS, IDOR, falha de autenticação
Onde	URL, endpoint ou tela afetada
Passos para reproduzir	passo a passo, na ordem
Impacto	o que um atacante conseguiria fazer
Evidências	capturas de tela, requisições, vídeo curto
Contato	como retornamos (opcional se preferir anonimato)

4.3. Reportes em **português ou inglês**.

4.4. Havendo dado pessoal de terceiro na evidência, **anonimize** antes de enviar e nos avise que o fez.

5. Porto seguro (*safe harbor*)

5.1. A Lexxen **não adotará medidas judiciais ou extrajudiciais** contra quem, de boa-fé:

- seguir esta Política;
- respeitar o escopo da seção 2 e as regras da seção 3;
- reportar prontamente e não divulgar antes do prazo.

5.2. Consideraremos a pesquisa conduzida nesses termos como **acesso autorizado** para os fins da legislação aplicável, inclusive o art. 154-A do Código Penal.

5.3. O porto seguro **não se aplica** a quem exfiltrar dados, causar dano intencional, extorquir, usar a falha em proveito próprio ou violar direitos de terceiros.

5.4. O porto seguro é dado **pela Lexxen** e **não vincula terceiros** — parceiros, provedores ou autoridades. Testar sistemas de terceiros é responsabilidade de quem testa.

6. Nossos prazos

Etapa	Prazo
Confirmação de recebimento	**até 3 dias úteis**
Triagem inicial e classificação	**até 10 dias úteis**
Retorno sobre procedência e plano de correção	**até 20 dias úteis**
Correção — severidade crítica	**até 15 dias corridos**
Correção — severidade alta	**até 30 dias corridos**
Correção — média e baixa	conforme planejamento, informado ao pesquisador

6.1. Manteremos o pesquisador informado sobre o andamento e avisaremos quando a correção for concluída.

7. Divulgação pública

7.1. Pedimos **90 dias** entre o reporte e qualquer divulgação pública, ou até a correção — o que ocorrer primeiro.

7.2. Estamos abertos a divulgação coordenada e a acordar prazo diferente caso a caso.

7.3. Com sua autorização, podemos **reconhecer publicamente** sua contribuição. Se preferir anonimato, respeitaremos.

8. Recompensas

8.1. A Lexxen **não mantém programa de recompensa financeira** (*bug bounty*) no momento.

8.2. Reconhecemos contribuições relevantes por meio de agradecimento público, quando autorizado, e carta de reconhecimento mediante solicitação.

8.3. Havendo programa de recompensa no futuro, esta Política será atualizada.

9. Dados pessoais

Dados de contato do pesquisador são tratados para conduzir a análise e retornar, conforme a **Política de Privacidade**, em https://www.lexxen.com/privacy.

10. Contato

compliance@lexxen.com — assunto `[VULN]`

Para incidente **em curso** com impacto a usuários, use o mesmo endereço com o assunto `[VULN-URGENTE]`.

LEXXEN LTDA — CNPJ 63.987.111/0001-53 Goiânia/GO, 31 de agosto de 2026 — versão 1.0