ÍNDICE

1. FINALIDADE E ESCOPO....2
2. DOCUMENTOS DE REFERÊNCIA....2
3. TERMOS E DEFINIÇÕES....2
4. COMO RELATAR UMA VULNERABILIDADE....3
4.1. Canal oficial....3
4.2. Informações que ajudam a análise....3
4.3. Diretrizes para pesquisa....3
4.4. Pesquisa de boa-fé....3
5. RETORNO AO RELATOR....3
6. PRAZOS E LIBERAÇÃO DAS CORREÇÕES....4
6.1. Prazos de correção....4
6.2. Como as correções chegam aos clientes....4
7. DIVULGAÇÃO COORDENADA E BOLETINS DE SEGURANÇA....5
8. PRIVACIDADE DOS RELATORES....5
9. REVISÃO....5
10. CONTROLE DE REVISÕES....5

1. FINALIDADE E ESCOPO

A e-Safer é a fabricante das plataformas TRIO e Rastro Digital. Esta política informa publicamente como relatar uma vulnerabilidade nesses produtos, como a e-Safer trata os relatos, em que prazos corrige as falhas, como as correções chegam aos clientes e como as vulnerabilidades corrigidas são divulgadas.

A política abrange todo o sistema de cada produto, sua infraestrutura e seus componentes, incluindo os componentes de terceiros incorporados a eles.

Os ambientes dos clientes e os produtos de outros fabricantes não estão no escopo desta política. Vulnerabilidades em produtos de terceiros relatadas à e-Safer são encaminhadas ao respectivo fabricante.

O tratamento descrito aqui segue o processo de gestão de vulnerabilidades do Sistema de Gestão de Segurança da Informação da e-Safer, certificado na ABNT NBR ISO/IEC 27001.

2. DOCUMENTOS DE REFERÊNCIA

Referência	Aplicação
ABNT NBR ISO/IEC 27001:2022	Controle A.8.8 – Gestão de vulnerabilidades técnicas
ISO/IEC 29147	Divulgação de vulnerabilidades
ISO/IEC 30111	Processos de tratamento de vulnerabilidades
CVSS e CVE	Pontuação de severidade e identificação pública de vulnerabilidades
Lei nº 13.709/2018 (LGPD)	Proteção de dados pessoais

3. TERMOS E DEFINIÇÕES

- Vulnerabilidade – fraqueza em um produto, em sua configuração ou em seus componentes que pode ser explorada para comprometer a confidencialidade, a integridade ou a disponibilidade das informações;
- Relator – pessoa ou organização que comunica uma vulnerabilidade à e-Safer;
- Severidade – gravidade da vulnerabilidade segundo a pontuação CVSS, na versão vigente;
- Correção – eliminação da vulnerabilidade por atualização, alteração de configuração, substituição de componente ou ajuste de código;
- Mitigação – medida que reduz o risco enquanto a correção definitiva não é aplicada;
- Divulgação coordenada – publicação de informações sobre uma vulnerabilidade somente depois que a correção estiver disponível, em acordo com o relator;

- Boletim de segurança – comunicado público da e-Safer que descreve uma vulnerabilidade corrigida, os produtos afetados e a correção aplicada.

4. COMO RELATAR UMA VULNERABILIDADE

4.1. Canal oficial

Clientes, pesquisadores, fornecedores e demais interessados podem relatar vulnerabilidades exclusivamente pelo canal eletrônico da e-Safer, que registra cada relato e permite o envio de anexos, como capturas de tela e provas de conceito:

- e-mail: relatar-vulnerabilidade@e-safer.com.br, com o assunto "Vulnerabilidade de segurança".

Os relatos podem ser enviados em português ou em inglês. Todo relato é registrado, recebe um número de acompanhamento e é tratado conforme esta política.

4.2. Informações que ajudam a análise

- o produto, a versão e o endereço ou a funcionalidade afetada;
- o tipo de vulnerabilidade e o impacto esperado;
- os passos para reproduzir a falha, com capturas de tela ou prova de conceito, quando houver;
- um contato para retorno e se o relator deseja ser identificado nos créditos.

4.3. Diretrizes para pesquisa

- teste apenas com contas próprias ou de teste, sem acessar, alterar ou apagar dados de terceiros;
- interrompa o teste e avise a e-Safer assim que tiver acesso a dados que não são seus, sem guardá-los nem compartilhá-los;
- não prejudique a disponibilidade dos produtos e não realize engenharia social nem ataques físicos;
- mantenha a vulnerabilidade em sigilo até a divulgação coordenada (seção 7).

4.4. Pesquisa de boa-fé

A e-Safer considera de boa-fé a pesquisa feita conforme estas diretrizes e não tomará medidas judiciais ou administrativas contra o relator por essa atividade.

5. RETORNO AO RELATOR

Etapa	Prazo
Confirmação do recebimento, com o número de acompanhamento	Até 3 dias úteis

Etapa	Prazo
Resultado da análise e severidade atribuída	Até 10 dias úteis
Atualização do andamento até a correção	A cada 15 dias
Confirmação da correção e combinação da divulgação	Após a liberação da correção

6. PRAZOS E LIBERAÇÃO DAS CORREÇÕES

6.1. Prazos de correção

A prioridade de cada vulnerabilidade considera a severidade, a existência de exploração ativa e a exposição do produto. Os prazos máximos para a correção ou a mitigação, contados a partir da confirmação da vulnerabilidade, são:

Severidade (CVSS)	Prazo máximo
Crítica	Até 7 dias corridos
Alta	Até 15 dias corridos
Média	Até 30 dias corridos
Baixa	Até 60 dias corridos

Vulnerabilidades com exploração ativa conhecida são tratadas como críticas, independentemente da pontuação. Quando a correção depende de um fornecedor de componente, a e-Safer aplica mitigações até a correção definitiva.

6.2. Como as correções chegam aos clientes

O TRIO e o Rastro Digital são fornecidos como serviço. A e-Safer aplica as correções no ambiente de produção, para todos os clientes, sem custo e sem necessidade de ação por parte do cliente.

Quando um componente do produto estiver instalado no ambiente do cliente, a correção é disponibilizada como atualização, com as instruções de aplicação e, quando necessário, medidas provisórias de mitigação.

Os clientes afetados por vulnerabilidades de severidade crítica ou alta são comunicados pelo contato técnico cadastrado, com a orientação necessária. Se uma vulnerabilidade resultar em acesso indevido a dados de clientes, a e-Safer notifica os clientes afetados nos termos do contrato e da Lei Geral de Proteção de Dados Pessoais.

7. DIVULGAÇÃO COORDENADA E BOLETINS DE SEGURANÇA

A e-Safer divulga as vulnerabilidades corrigidas de forma coordenada com o relator: somente depois que a correção estiver disponível e, como regra, em até 90 dias do relato. O prazo pode ser estendido em comum acordo, quando a correção for complexa, ou antecipado, quando houver exploração ativa.

Vulnerabilidades de severidade crítica, alta ou média nos produtos da e-Safer geram boletim de segurança publicado junto desta política, com:

- o identificador do boletim e, quando aplicável, o código CVE;
- os produtos e as versões afetadas;
- a descrição da falha, sem detalhes que facilitem a exploração;
- a severidade e a nota CVSS;
- a correção ou a mitigação aplicada, a data de liberação e eventuais ações necessárias do cliente;
- os créditos ao relator, quando autorizados.

Os boletins não identificam clientes nem divulgam dados de clientes.

8. PRIVACIDADE DOS RELATORES

Os dados pessoais dos relatores são usados apenas para tratar o relato e comunicar o andamento, conforme a Lei Geral de Proteção de Dados Pessoais, e não são compartilhados sem autorização. A e-Safer não mantém programa de recompensa financeira; com autorização, os relatores são reconhecidos nos boletins.

9. REVISÃO

Esta política é revisada, no mínimo, anualmente e sempre que houver mudança relevante nos produtos, nos riscos ou nos requisitos aplicáveis.

10. CONTROLE DE REVISÕES

Data	Revisão	Histórico
25/11/2026	01	Publicação inicial.