Empresa FPT Industrial		Política de Divulgação Coordenada de Vulnerabilidades de Cibersegurança	
Função Technical Certification and Compliance	**Versão** **1.0**	**Data** 03/09/2026	**Páginas** 5

1 OBJETIVO 2

2 ESCOPO 2

3 RELATO DE VULNERABILIDADES 2

3.1 Canais de relato 2

3.2 O que esperamos 2

4 PRINCÍPIOS DE TRATAMENTO DE VULNERABILIDADES 3

4.1 Receber e confirmar o recebimento de relatórios de vulnerabilidade 3

4.2 Validar vulnerabilidades reportadas 3

4.3 Avaliar o risco de cibersegurança 3

4.4 Definir medidas de remediação 3

5 COORDENAÇÃO COM OS CLIENTES 3

6 COORDENAÇÃO COM FORNECEDORES 3

7 DIVULGAÇÃO COORDENADA 4

8 AVISO DE SEGURANÇA 4

9 AVALIAÇÃO CONJUNTA DE RISCOS 4

10 RELATÓRIOS REGULATÓRIOS 4

11 CONFIDENCIALIDADE 5

12 CLÁUSULA DE SALVAGUARDA 5

Para obter orientação sobre esta Política ou denunciar uma infração, entre em contato com o Departamento Legal, Compliance and Corporate Governance do Iveco Group ou use a Compliance Helpline: ivecogroupcompliancehelpline.com

1 OBJETIVO

A FPT Industrial está empenhada na identificação, avaliação, remediação e divulgação coordenada, em tempo útil, de vulnerabilidades de cibersegurança que afetem seus produtos com elementos digitais.
Esta política define os princípios que regem o recebimento, tratamento, compartilhamento e divulgação de informações sobre vulnerabilidades em conformidade com os requisitos regulatórios aplicáveis, incluindo o Regulamento (UE) 2024/2847 (CRA - Cyber Resilience Act)

2 ESCOPO

Esta política aplica-se às vulnerabilidades de cibersegurança que afetam os produtos da FPT:

- Unidades de Controle Eletrônico (ECUs)
- Software integrado
- Serviços de diagnóstico
- Interfaces de comunicação
- Serviços e dispositivos FPT conectados
- Ferramentas de desenvolvimento e manutenção
- Software e componentes de terceiros integrados nos produtos da FPT

3 RELATO DE VULNERABILIDADES

As vulnerabilidades podem ser relatadas por:

- Clientes (OEMs)
- Fornecedores
- Pesquisadores de segurança
- Fontes de inteligência de ameaças
- Equipe interna
- Outros

Os relatos devem ser enviados através do canal de notificação de cibersegurança estabelecido pela FPT.

3.1 Canais de reporte

Para comunicar uma vulnerabilidade ou um incidente de cibersegurança envolvendo um produto da FPT, por favor envie uma mensagem para o endereço de e-mail:
FPT-CyberVulnerability@ivecogroup.com

Inclua as seguintes informações no seu relato:

- Assunto do e-mail: “Vulnerabilidade Potencial”
- Produto, modelo e versão
- Descrição da questão ou vulnerabilidade – inclua o CVE, quando aplicável
- Informação que ajude a nossa equipa a reproduzir o problema (por exemplo, detalhes de configuração)
- Informações de contato

3.2 O que esperamos

Solicita-se aos relatores externos que comuniquem vulnerabilidades que:

- Não divulguem a vulnerabilidade publicamente sem acordo prévio com a FPT
- Não excluam e nem destruam quaisquer dados
- Não realizem ataques negativos de serviço
- Concordem com um prazo para a correção

Para obter orientação sobre esta Política ou denunciar uma infração, entre em contato com o Departamento Legal, Compliance and Corporate Governance do Iveco Group ou use a Compliance Helpline: ivecogroupcompliancehelpline.com

4 PRINCÍPIOS DE TRATAMENTO DE VULNERABILIDADES

4.1 Receber e confirmar o recebimento de relatórios de vulnerabilidade

Todas as vulnerabilidades reportadas deverão ser registadas e avaliadas pela FPT.

4.2 Validar vulnerabilidades reportadas

A FPT determinará:
- a validade do problema reportado;
- os produtos e versões afetados;
- o impacto potencial;
- a explorabilidade.

4.3 Avaliar o risco de cibersegurança

Uma avaliação de cibersegurança deve ser realizada utilizando os processos e métodos de cibersegurança aplicáveis.

4.4 Definir medidas de remediação

Quando adequado, a FPT deverá:
- desenvolver ações corretivas;
- definir medidas de mitigação;
- preparar atualizações de software;
- determinar recomendações de implementação.

5 COORDENAÇÃO COM OS CLIENTES

Para os produtos fornecidos a clientes OEM, a FPT adota uma abordagem de divulgação coordenada de vulnerabilidades.
As informações sobre vulnerabilidades validadas serão partilhadas com os clientes afetados para apoiar uma avaliação conjunta de:
- frotas de veículos afetadas;
- impacto operacional;
- risco de cibersegurança;
- medidas de mitigação disponíveis;
- estratégia de remediação.

Esta abordagem coordenada permite às partes afetadas implementar medidas adequadas de tratamento de riscos antes da divulgação pública.

6 COORDENAÇÃO COM FORNECEDORES

A FPT espera que os fornecedores comuniquem prontamente vulnerabilidades que afetem componentes, software ou serviços integrados com os produtos da FPT.

Os fornecedores devem fornecer:
- descrição da vulnerabilidade;
- versões afetadas;
- avaliação da gravidade;
- opções de mitigação;
- cronograma de remediação;
- restrições de divulgação, se aplicável.

A FPT avaliará as informações sobre vulnerabilidades fornecidas pelos fornecedores no âmbito do seu próprio processo de gestão de riscos de cibersegurança.

7 DIVULGAÇÃO COORDENADA

A FPT apoia a divulgação responsável e coordenada de vulnerabilidades de cibersegurança.

As atividades de divulgação devem ter em conta:

- a disponibilidade de medidas de mitigação ou correções;
- os riscos potenciais de uma divulgação prematura;
- a coordenação com os clientes afetados;
- as obrigações de notificação regulamentar.

A divulgação pública pode ser adiada quando a publicação imediata puder aumentar os riscos de cibersegurança ou facilitar a exploração da vulnerabilidade.

8 AVISO DE SEGURANÇA

Quando apropriado, a FPT poderá emitir um Comunicado de Segurança contendo informações necessárias para apoiar a análise de riscos e o planeamento da remediação por parte do cliente.

O comunicado deve incluir:

Descrição: Descrição da vulnerabilidade.

Produtos Afetados: Produtos, componentes e versões envolvidos.

Impacto: Potenciais efeitos na cibersegurança.

Gravidade: Avaliação da gravidade e classificação de risco.

Mitigações: Medidas temporárias disponíveis.

Remediação: Correções de software disponíveis ou atualizações planeadas.

Referências: Identificadores relevantes (por exemplo, CVE, referências CERT).

9 AVALIAÇÃO CONJUNTA DE RISCOS

Para os produtos fornecidos a clientes OEM, são compartilhadas informações sobre vulnerabilidades para viabilizar uma avaliação conjunta dos riscos.

A avaliação pode considerar:

- explorabilidade técnica;
- definições dos produtos afetados;
- contexto operacional;
- controles de segurança existentes;
- viabilidade de remediação.

Os resultados desta avaliação fundamentam decisões relacionadas com a remediação, ações de implementação e comunicações aos clientes

10 RELATÓRIOS REGULATÓRIOS

Quando exigido pelas regulamentações aplicáveis, incluindo o Cyber Resilience Act, a FPT realizará as atividades de reporte regulamentar necessárias através dos processos definidos nos procedimentos de cibersegurança aplicáveis.

Para obter orientação sobre esta Política ou denunciar uma infração, entre em contato com o Departamento Legal, Compliance and Corporate Governance do Iveco Group ou use a Compliance Helpline: ivecogroupcompliancehelpline.com

11 CONFIDENCIALIDADE

As informações sobre vulnerabilidades devem ser tratadas como confidenciais e partilhadas apenas com as partes que tenham uma necessidade legítima de as conhecer, a menos e até que a divulgação seja autorizada.

12 CLÁUSULA DE SALVAGUARDA

A FPT Industrial não tomará medidas legais contra os pesquisadores de cibersegurança que:

- • Atuem de boa-fé
- • Cumpram esta Política de Divulgação
- • Não acessem, copiem ou destruam dados sem autorização
- • Não prejudiquem os serviços através de ataques de suspensão de serviço
- • Não coloquem em risco terceiros afetados