Incident Response Policy

G ERP · Grubtech · Effective from November 10, 2026

> **Company:** RAPHAEL DE ARAUJO SILVA (trade name GRUBTECH), CNPJ 30.444.499/0001-97
> R. Costa Barros, 698, Conj 3, Vila Alpina, São Paulo/SP, Brazil, CEP 03210-000
> **Incident and privacy contact:** privacidade@grubtech.com.br · +55 11 97466-4832

1. Purpose and scope

This policy defines how Grubtech detects, handles, and reports security incidents affecting G ERP, its servers, its databases, and the personal data it processes, including data received from marketplaces (such as Mercado Livre, TikTok Shop, SHEIN, Shopee, Amazon, and Magalu). A security incident is any confirmed or suspected event that compromises the confidentiality, integrity, or availability of systems or data, such as unauthorized access, data leakage, loss of data, or misuse of credentials.

2. Roles and responsibilities

Role	Who	Responsibilities
Incident Response Lead and Data Protection Officer (Encarregado, LGPD)	Raphael de Araujo Silva, owner	Receives reports, classifies the incident, coordinates containment and recovery, decides and sends notifications, and keeps the incident record.
Customers (data controllers)	Companies that use G ERP	Receive Grubtech's notification and decide on communication to their own customers and data subjects, as controllers under the LGPD.
Marketplace partners	Platforms whose data G ERP receives	Are notified when an incident involves data obtained through their APIs, according to their policies.

3. Reporting channel

Anyone (customers, users, partners, or third parties) can report a suspected incident to **privacidade@grubtech.com.br**. Reports are acknowledged within 1 business day.

4. Response process

1. **Detection and reporting:** through the reporting channel, server and application logs, failed-login blocking, and alerts from the cloud provider.
2. **Triage:** confirm the incident, identify affected systems, customers, and data, and classify severity (high: personal data exposed or systems unavailable; medium: contained attempt with possible impact; low: no data or service impact).
3. **Containment:** block the involved accounts or access, revoke and rotate affected credentials and keys (including marketplace authorization tokens and app secrets), and isolate the affected server or database when needed.

4. **Eradication and recovery:** remove the cause, apply fixes and updates, restore data from backups when needed, and verify that the service is working normally.
5. **Notification:** according to section 5.
6. **Post-incident review:** record the root cause, the actions taken, and the improvements adopted to prevent recurrence.

5. Notification

- **Affected customers:** without undue delay, within 24 hours of confirming an incident that affects their data or service.
- **Marketplace partners:** within 24 hours of confirming an incident involving data obtained through their APIs, or within the shorter period required by that partner's policy, through the channel the partner defines.
- **Brazilian Data Protection Authority (ANPD) and data subjects:** when the incident may cause relevant risk or damage to data subjects, within the period set by ANPD regulations (currently 3 business days), together with the controller where applicable.
- Notifications describe what happened, the data and people affected, the measures taken, and the contact for questions.

6. Records and review

Every incident is recorded with date, description, data and customers affected, actions taken, and notifications sent. Records are kept for at least 5 years. This policy is reviewed at least once a year and after any high-severity incident.

Política de Resposta a Incidentes

G ERP · Grubtech · Em vigor a partir de 10 de novembro de 2026

> **Empresa:** RAPHAEL DE ARAUJO SILVA (nome fantasia GRUBTECH), CNPJ 30.444.499/0001-97
> R. Costa Barros, 698, Conj 3, Vila Alpina, São Paulo/SP, CEP 03210-000
> **Contato para incidentes e privacidade:** privacidade@grubtech.com.br · (11) 97466-4832

1. Objetivo e abrangência

Esta política define como a Grubtech identifica, trata e comunica incidentes de segurança que afetem o G ERP, seus servidores, seus bancos de dados e os dados pessoais tratados, inclusive os recebidos dos marketplaces (como Mercado Livre, TikTok Shop, Shein, Shopee, Amazon e Magalu). Incidente de segurança é qualquer evento, confirmado ou suspeito, que comprometa a confidencialidade, a integridade ou a disponibilidade dos sistemas ou dos dados, como acesso não autorizado, vazamento, perda de dados ou uso indevido de credenciais.

2. Funções e responsabilidades

Função	Quem	Responsabilidades
Responsável pela resposta a incidentes e Encarregado de dados (LGPD)	Raphael de Araujo Silva, titular	Recebe os avisos, classifica o incidente, coordena a contenção e a recuperação, decide e faz as comunicações e mantém o registro dos incidentes.
Clientes (controladores)	Empresas que usam o G ERP	Recebem a comunicação da Grubtech e decidem a comunicação aos próprios clientes e titulares, como controladores pela LGPD.
Marketplaces parceiros	Plataformas cujos dados o G ERP recebe	São comunicados quando o incidente envolve dados obtidos pelas APIs deles, conforme as políticas de cada um.

3. Canal de comunicação

Qualquer pessoa (clientes, usuários, parceiros ou terceiros) pode avisar sobre um incidente suspeito em **privacidade@grubtech.com.br**. O recebimento é confirmado em até 1 dia útil.

4. Como o incidente é tratado

1. **Identificação e aviso:** pelo canal de comunicação, pelos registros (logs) dos servidores e do sistema, pelo bloqueio de tentativas de senha erradas e pelos alertas do provedor de nuvem.
2. **Triagem:** confirmar o incidente, identificar sistemas, clientes e dados afetados e classificar a gravidade (alta: dados pessoais expostos ou sistema fora do ar; média: tentativa contida com possível impacto; baixa: sem impacto em dados ou no serviço).
3. **Contenção:** bloquear as contas ou acessos envolvidos, revogar e trocar as credenciais e chaves afetadas (inclusive autorizações e segredos dos apps dos marketplaces) e isolar o servidor ou o banco afetado, quando preciso.

4. **Correção e recuperação:** eliminar a causa, aplicar correções e atualizações, restaurar dados das cópias de segurança quando preciso e conferir que o serviço voltou ao normal.
5. **Comunicação:** conforme o item 5.
6. **Revisão depois do incidente:** registrar a causa, as ações tomadas e as melhorias adotadas para não se repetir.

5. Comunicação

- **Clientes afetados:** sem demora, em até 24 horas da confirmação de um incidente que afete os dados ou o serviço deles.
- **Marketplaces parceiros:** em até 24 horas da confirmação de um incidente com dados obtidos pelas APIs deles, ou no prazo menor que a política do parceiro exigir, pelo canal que ele definir.
- **ANPD e titulares:** quando o incidente puder causar risco ou dano relevante aos titulares, no prazo da regulamentação da ANPD (hoje, 3 dias úteis), junto com o controlador quando for o caso.
- A comunicação diz o que aconteceu, os dados e as pessoas afetadas, as medidas tomadas e o contato para dúvidas.

6. Registro e revisão

Todo incidente é registrado com data, descrição, dados e clientes afetados, ações tomadas e comunicações feitas. Os registros são guardados por no mínimo 5 anos. Esta política é revista pelo menos uma vez por ano e depois de qualquer incidente de gravidade alta.