PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA E PRIVACIDADE

Plataformas JunqueiraTecnologia, ResultFácil e ResultAgro

Última atualização: 20/05/2026

PREÂMBULO

Este Plano de Resposta a Incidentes ("**Plano**") estabelece o processo formal adotado pela **EDUARDO JUNQUEIRA ME** ("Licenciante") para identificar, classificar, conter, erradicar e aprender com incidentes de segurança da informação e de privacidade nas plataformas **JunqueiraTecnologia**, **ResultFácil** e **ResultAgro** (em conjunto, "Plataforma").

Este documento **complementa**, sem duplicar:

- o **Termo de Uso** — limites de responsabilidade e regras gerais de uso;
- a **Política de Privacidade** — bases legais, direitos do titular e comunicação à ANPD (art. 48 da LGPD);
- a **Política de Backup, RTO e RPO** — recuperação operacional, indicadores e fluxo técnico.

As definições, prazos e canais ali previstos aplicam-se integralmente a este Plano e **não serão repetidos aqui**. Em caso de eventual divergência, prevalece o documento mais específico para o ponto em questão.

---

1. OBJETO DESTE PLANO

Este Plano trata especificamente:

a) da **organização interna** da equipe de resposta (papéis e responsabilidades); b) da **classificação de severidade** dos incidentes; c) das **fontes complementares de detecção** além das já citadas em outros documentos; d) das **fases de contenção, erradicação e aprendizado** — não cobertas pela Política de Backup, que trata apenas da recuperação; e) do **conteúdo mínimo das comunicações** a titulares e à ANPD; f) do **Registro Interno de Incidentes**; g) do programa de **treinamento e revisão**.

---

2. PAPÉIS DE RESPOSTA

A resposta a incidentes é organizada por **papéis funcionais**, que podem ser exercidos cumulativamente pelas mesmas pessoas conforme a natureza e a gravidade da ocorrência.

Papel	**Atribuição**
Coordenador de Incidente	Confirma a ocorrência, classifica a severidade, conduz a resposta e autoriza comunicações externas
Responsável Técnico	Executa as ações de contenção, erradicação e suporte à recuperação
Encarregado (DPO)	Avalia impactos de privacidade, decide sobre comunicação à ANPD e aos titulares, interage com autoridades

Responsável pela Comunicação	Elabora os comunicados aos Licenciados afetados

Os papéis são exercidos pelos **Tech Leaders** e pelo **DPO** da Licenciante, conforme escala interna mantida em registro controlado.

2.1. Acionamento

- **Horário comercial:** pelos canais oficiais (portal de suporte e e-mail).
- **Fora do horário comercial — incidentes urgentes:** pelo contato emergencial disponível em https://junqueiratecnologia.com.br/.

---

3. FONTES DE DETECÇÃO

Além do **Zabbix** já mencionado na Política de Backup, integram o processo de detecção:

- **Cloudflare** — alertas de segurança de borda, anomalias de tráfego e bloqueios automáticos contra ataques (DDoS, força bruta, injeção, varreduras);
- **Health checks** internos da aplicação;
- **Logs locais** de sistema, aplicação e processamento, mantidos por **30 dias** na infraestrutura da Licenciante (sem prejuízo da retenção de **logs de acesso à aplicação** prevista na Política de Privacidade, conforme art. 15 do Marco Civil da Internet);
- **Comunicações de Licenciados** pelos canais oficiais.

Qualquer colaborador que identifique evento suspeito deve reportá-lo imediatamente ao Coordenador de Incidente, ainda que sem confirmação.

---

4. CLASSIFICAÇÃO DE SEVERIDADE

Todo incidente confirmado recebe classificação de severidade, que determina o tempo máximo para **resposta inicial** (acionamento da equipe e início das ações de contenção). A classificação **não altera** os indicadores de **RTO e RPO** previstos na Política de Backup.

Nível	Critério	Tempo para resposta inicial
P1 — Crítico	Indisponibilidade total da Plataforma, ou suspeita de incidente envolvendo dados pessoais com risco a múltiplos titulares	1 hora
P2 — Alto	Indisponibilidade parcial relevante, ou suspeita de acesso indevido limitado	4 horas
P3 — Médio	Falha funcional sem perda de dados, ou anomalia detectada sem impacto confirmado	8 horas úteis
P4 — Baixo	Eventos suspeitos isolados, sem impacto operacional ou de privacidade	1 dia útil

Incidentes envolvendo **dados pessoais** acionam automaticamente o procedimento da Seção 6, independentemente do nível de severidade.

---

5. CICLO COMPLEMENTAR DE RESPOSTA

A Política de Backup descreve o fluxo de **recuperação** (item 7.3 daquele documento). Este Plano complementa esse fluxo com as fases que **antecedem e sucedem** a recuperação técnica.

5.1. Contenção

Ações imediatas para impedir a propagação ou ampliação do dano, antes mesmo de erradicar a causa:

- isolamento de servidor, serviço ou recurso afetado;
- bloqueio de IPs, contas ou credenciais suspeitas;
- ativação de regras adicionais no Cloudflare (rate limit, WAF, geo-blocking);
- suspensão temporária de funcionalidades específicas, quando necessário;
- preservação de evidências para análise posterior.

5.2. Erradicação

Identificação e remoção da causa-raiz:

- aplicação de patches e correções;
- remoção de artefatos maliciosos;
- revogação e rotação de credenciais comprometidas;
- ajuste de configurações inseguras;
- validação de que vetores semelhantes não permanecem ativos.

5.3. Lições aprendidas (post-mortem)

Após o encerramento de incidentes de severidade **P1 ou P2**, a equipe realiza análise estruturada para:

a) documentar causa-raiz e linha do tempo; b) identificar melhorias de processo, ferramentas, automação ou treinamento; c) atualizar este Plano e demais documentos correlatos, se necessário; d) registrar o aprendizado no Registro Interno de Incidentes (Seção 7).

Para incidentes **P3 e P4**, o aprendizado é registrado de forma sumária, sem necessidade de análise estruturada formal.

---

6. CONTEÚDO MÍNIMO DAS COMUNICAÇÕES

Os **canais** de comunicação a Licenciados, à ANPD e a titulares estão definidos na Política de Privacidade e na Política de Backup. Este Plano detalha o **conteúdo mínimo** dessas comunicações.

6.1. Comunicação à ANPD (em incidentes com dados pessoais)

A comunicação observará os requisitos do **art. 48, § 1º, da LGPD** e da regulamentação da ANPD vigente, contendo no mínimo:

a) descrição da natureza dos dados pessoais afetados; b) informações sobre os titulares envolvidos; c) indicação das medidas técnicas e de segurança utilizadas; d) riscos relacionados ao incidente; e) razões da demora na comunicação, se aplicável; f) medidas adotadas para reverter ou mitigar os efeitos.

6.2. Comunicação aos titulares afetados

Em linguagem clara e acessível, contendo, no que couber, as mesmas informações enviadas à ANPD (item 6.1), além de:

a) orientações práticas ao titular (ex.: troca de senha, atenção a tentativas de fraude); b) canal para esclarecimentos.

6.3. Comunicação a outras autoridades

Quando exigido por lei ou determinação judicial/administrativa, a Licenciante comunicará outras autoridades competentes.

---

7. REGISTRO INTERNO DE INCIDENTES

A Licenciante mantém **Registro Interno de Incidentes** em ambiente controlado, com acesso restrito à equipe de resposta. Cada registro contém:

a) identificação e classificação do incidente; b) datas e horários de detecção, contenção, erradicação e recuperação; c) sistemas e dados envolvidos; d) ações executadas e responsáveis; e) comunicações realizadas (Licenciados, ANPD, titulares, autoridades); f) lições aprendidas e ações de melhoria.

O Registro é mantido por **5 (cinco) anos** e pode ser disponibilizado a auditorias e à ANPD quando regularmente requisitado.

---

8. TREINAMENTO E REVISÃO

a) Revisões **ordinárias** deste Plano ocorrem **anualmente**; b) Revisões **extraordinárias** são realizadas após incidentes P1/P2, mudança regulatória relevante ou alteração significativa de infraestrutura; c) A equipe de resposta participa de atualização contínua sobre boas práticas de segurança da informação e proteção de dados; d) A prática operacional dos procedimentos técnicos de recuperação ocorre por meio dos **testes semanais** de scripts já previstos na Política de Backup, RTO e RPO.

---

9. RELAÇÃO COM OUTROS DOCUMENTOS

Este Plano integra o conjunto de documentos de governança da Plataforma e deve ser lido em conjunto com:

- **Termo de Uso**
    - https://junqueiratecnologia.com.br/assets/003-Termo_de_uso_RESULTFACIL_V1.pdf
- **Política de Privacidade**
    - https://junqueiratecnologia.com.br/assets/002-Politica_Privacidade_RESULTFACIL_V1.pdf

- **Política de Backup, RTO e RPO**
    - https://junqueiratecnologia.com.br/assets/004-Politica_de_Backup_Recovery_RTO_RPO_RESULTFACIL_V1.pdf

Pontos como canais de contato, identificação do DPO, indicadores de RTO/RPO, prazos de retenção de logs e bases legais para tratamento de dados estão regulados nos documentos acima e **não são repetidos neste Plano**.