# PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA E PRlVACIDADE

## Preparação Prévia

O Plano de Resposta a Incidentes de Segurança e Privacidade é essencialmente um processo. Descreve a forma como a PLATTANO vai responder às situações de emergência e exceção. Pelo potencial gravidade, a resposta da PLATTANO deve ser rápida e confiável, ao mesmo tempo resguardando evidências forenses que podem ajudar a prevenir novos incidentes atendendo as exigências legais de comunicação e transparência. O ciclo de vida de resposta a incidentes é a estrutura passo a passo da empresa para identificar e reagir a uma interrupção de serviço ou ameaça à segurança, atendendo os seguintes itens:

· **Formação do Time de Resposta a Incidentes (TRI)**. Consiste em um grupo de colaboradores que deve ser designado através de resolução de diretoria, com acessos, habilidades, responsabilidades, treinamento e conhecimentos chave para responder aos mais variados tipos de incidentes. O TRI deve ter reuniões periódicas para definir melhorias, verificação de pré-requisitos, mecanismos, atribuições, necessidade de preparo, bem como divulgação e treinamentos para os membros e demais colaboradores. O encarregado pelo tratamento de dados pessoais (DPO) e pelo menos um representante da equipe de segurança da informação devem fazer parte desse grupo.

· **Instalação e divulgação dos mecanismos de comunicação de incidente**. Devem ser criadas, disponibilizadas e publicadas as formas de notificação à companhia quando ocorrerem incidentes. O §1º, do Artigo 41, da Lei 13709/2018, a LGPD, estabelece: "*A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.*" Portanto, devem ser divulgados os e-mails: **dpo@plattano.com.br** e **seguranca@plattano.com.br**, bem como nosso portal de chamados: Plattano Support e pelo telefone 04831979877. Deve haver indicação de quais mecanismos são considerados rápidos e seguros e se sugere o esclarecimento de quais as expectativas de anonimato que o notificador deve ter.



Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**

· **Definição do grupo de Acionadores do TRI**. Responsáveis por receberem as notificações e a realização do tratamento inicial. Para a cobertura 24 horas, este grupo deve incluir membros do time de suporte e contatos qualificados para executar a triagem.

· **Instalação, configuração e definição de ferramentas de monitoria e alarmes.** Devem informar diretamente o TRI através de mecanismos de comunicação direta como abertura de chamado no portal de chamados, contato através do e-mail e telefone.

· **Preparo de um Plano de Comunicação de Incidentes**. Para facilitar a comunicação da Companhia deve ser criada uma biblioteca com modelos de documentos (templates) para comunicação formal do encarregado pelo Tratamento de Dados Pessoais com a ANPD, titulares de dados, notificadores e imprensa.

# Papéis e Responsabilidades

Cada área da Empresa, sejam as áreas diretamente envolvidas na governança da Empresa ou não, tem responsabilidades quando da ocorrência ou mera suspeita de um Incidente, conforme descritas a seguir:

**Obrigações de Todas as Áreas**

• comunicar imediatamente a Equipe de Resposta (conforme descrito abaixo), sobre a ocorrência ou a mera suspeita de um Incidente;

• cumprir rigorosamente a Política de Segurança da Informação da Empresa, contribuindo para a mitigação de riscos; e

• participar de treinamentos e programas de conscientização para mitigação de Incidentes.

**Obrigações da Equipe de Resposta**

A Equipe de Resposta a Incidentes da Empresa é o grupo de Colaboradores designado abaixo para atuar nas respostas a Incidentes:



Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**

# Plano de Resposta a Incidentes

A Equipe de Resposta a Incidentes da Empresa é o grupo de Colaboradores designado abaixo para atuar nas respostas a Incidentes:

| Departamento/Setor | Responsável |
|---|---|
| Tecnologia | Eduardo Scheffer |
| Administrativo | Giovanni Mantelli |

Entre suas principais responsabilidades, destacamos:

- atuar para detectar e corrigir os Incidentes;
- alertar, comunicar e aconselhar os Colaboradores sobre Incidentes emergentes;
- educar e conscientizar os Colaboradores sobre a detecção e resposta aos Incidentes;
- adotar demais medidas necessárias para prevenir Incidentes e minimizar o impacto de seus efeitos.

# Detecção do Incidente

Detectar um Incidente de forma rápida e eficiente é essencial para uma resolução bem-sucedida. São várias as formas de detecção, de modo que é impossível desenvolver uma metodologia que contemple cada uma. Desta forma, todos os Colaboradores devem atentar-se, principalmente, aos sinais mais comuns que podem desencadear um Incidente, como invasões de rede, perda ou furto de documentos, arquivos ou dispositivos, phishing, malware, instabilidades sistêmicas etc.

**Uma vez detectado um Incidente ou detectada a mera suspeita de um Incidente, o Colaborador deverá comunicar imediatamente a Equipe de Resposta a Incidentes, por meio do e-mail [-], mantendo o seu supervisor sempre em cópia.**

Na medida do possível, essa comunicação deverá conter (i) a hora e a data em que a suspeita do Incidente foi descoberta; (ii) o tipo de informações



Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**

envolvidas; (iii) a causa e a extensão do Incidente; (iv) o contexto do ocorrido; bem como (v) qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

A COMUNICAÇÃO SOBRE A SUSPEITA DE UM INCIDENTE É VITAL PARA A EMPRESA. ASSIM, CASO O COLABORADOR SUSPEITE DE UM INCIDENTE E NÃO O COMUNIQUE, SANÇÕES DISCIPLINARES PODERÃO SER-LHE APLICADAS, A DEPENDER DA GRAVIDADE DO INCIDENTE E DA COMPROVAÇÃO DE EVENTUAL NEGLIGÊNCIA DO COLABORADOR.

**Priorização do Incidente e Procedimentos para Resposta**

Uma vez que o Incidente seja identificado e classificado, é necessário priorizá-lo conforme o nível de risco oferecido à Empresa e aos titulares dos Dados Pessoais eventualmente afetados e a gravidade da ocorrência. O impacto do Incidente deve ser aferido da seguinte forma:

| | | | | |
|---|---|---|---|---|
| **volume de Dados Pessoais expostos** | Alto | **Alta Gravidade** | **Alta Gravidade** | **Alta Gravidade** |
| | Médio | **Média Gravidade** | **Alta Gravidade** | **Alta Gravidade** |
| | Baixo | **Baixa Gravidade** | **Média Gravidade** | **Média Gravidade** |
| | | Baixa | Média | Alta |
| | | **sensibilidade dos Dados Pessoais afetados** | | |

**VOLUME DE DADOS PESSOAIS EXPOSTOS**



Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**

| Criticidade | Descrição |
|---|---|
| Alto | volume de Dados Pessoais afetado superior a 10% da base de dados controlada pela Empresa |
| Médio | volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados controlada pela Empresa |
| Baixo | volume de Dados Pessoais afetado inferior a 2% da base de dados controlada pela Empresa |

| **SENSIBILIDADE DOS DADOS PESSOAIS AFETADOS** | |
|---|---|
| **Criticidade** | **Descrição** |
| Alto | Dados Pessoais de crianças ou adolescentes, Dados Pessoais Dados Sensíveis ou que possam gerar discriminação ao titular; dados bancários, de pagamento ou de proteção ao crédito |
| Médio | Dados Pessoais imediatamente identificáveis (e.g. nome, e-mail, CPF), combinados ou não com informações comportamentais (e.g. histórico de atividades, preferências etc.) |
| Baixo | Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (e.g. IP) |

De acordo com a matriz acima definida, a Equipe de Resposta a Incidentes deverá tomar as seguintes ações, simultaneamente ou, quando não for possível, em rápida sucessão:

**Baixa Gravidade**

1. tão logo tenha ciência, trabalhar prioritariamente na resolução do Incidente;



Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**

2. tomar as medidas adequadas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção;

3. comunicar o Comitê de Proteção de Dados;

4. comunicar as Áreas Envolvidas, que deverão estar à disposição da Equipe de Resposta;

5. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, conforme modelo anexo a este PRI; e

6. reunir-se para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata, que deverá ser apresentada ao Comitê de Proteção de Dados.

**Média Gravidade**

1. tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;

2. tomar as medidas imediatas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção e, se a correção não for possível de forma imediata, deve adotar as medidas temporárias para minimização de riscos;

3. comunicar o Comitê de Proteção de Dados;

4. comunicar as Áreas Envolvidas, que deverão estar à disposição para atender, com prioridade, a Equipe de Resposta;

5. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, o mais breve possível, conforme modelo anexo a este PRI;

6. reunir-se o mais breve possível para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata documentada, que deverá ser apresentada ao Comitê de Proteção de Dados; e

7. realizar, imediatamente, treinamento interno com as áreas afetadas para conscientizar os seus Colaboradores sobre o Incidente e medidas preventivas.



Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**

**Alta Gravidade**

1. tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;

2. imediatamente comunicar os diretores responsáveis pelas Áreas Envolvidas, os quais, em conjunto com outra pessoa de cada uma das respectivas Áreas Envolvidas, devem atuar de forma exclusiva no suporte à Equipe de Resposta e preferencialmente no mesmo local em que a Equipe de Resposta esteja trabalhando;

3. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, imediatamente, conforme modelo anexo a este PRI;

4. reunir-se, imediatamente, para avaliar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata, que deverá ser apresentada ao Comitê de Proteção de Dados;

5. realizar, imediatamente, treinamento interno com todos os Colaboradores da Empresa para conscientizar sobre o Incidente e medidas preventivas; e

6. comunicar, imediatamente, os Colaboradores internos sobre medidas preventivas

# Atores

· **Notificador** - pessoa ou sistema de monitoramento que notifica incidentes.

· **TRI** - Time de Resposta a Incidentes, definido na preparação prévia.

· **Acionadores do TRI** - grupo que receberá notificações de incidentes em primeira mão para triagem, estruturado em níveis distintos para viabilizar a importante cobertura 24 horas.

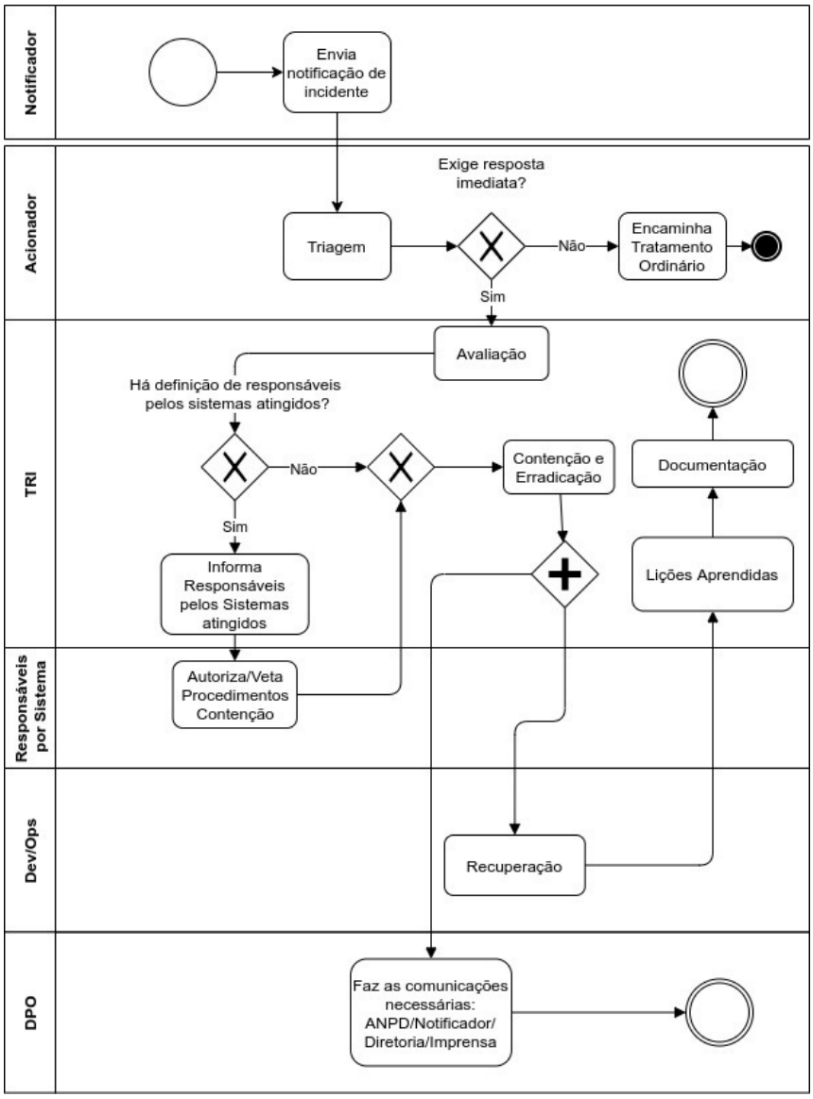
· **Responsável por Sistema ou Controlador de Sistema**, indicado que deve ser contatado e pode autorizar ou vetar procedimentos de emergência.

· **Equipe de Segurança da Informação -** equipe responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais.

· **Encarregado pelo Tratamento de Dados Pessoais (DPO)** - membro especial do TRI, responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais.

· **Engenharia/Operadores/Fornecedores dos sistemas** - atuam na engenharia da solução, implantação e acionamento de fornecedores.

# Processo






Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**

**Início**

Um novo incidente é notificado, por pessoas externas, internas ou por alarme de monitoramento, usando um dos mecanismos de comunicação definidos. Notificações são recebidas através do Acionador do TRI.

**Triagem**

O Acionador do TRI deve fazer a avaliação preliminar ou contatar imediatamente outro acionador em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.

Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.

Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para tramites regulares da companhia pela equipe de segurança da informação e encarregado pelo tratamento de dados pessoais, caso o incidente envolva dados pessoais.

Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o TRI deve ser acionado e passamos às fases seguintes.

**Avaliação**

Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente. Deve-se procurar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos sistemas afetados para colaborar e isso deve ser feito a critério do TRI a qualquer momento que julgar adequado e viável.

**Contenção e Erradicação**

Caso estejam identificados na documentação interna, devem ser acionados os responsáveis pelos sistemas impactados, conforme indicado, que irão orientar e se manifestar sobre os procedimentos de contenção e erradicação.



Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**

O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida será realizado o desligamento dos sistemas inteiros ou de funcionalidades especificas, colocação de avisos de indisponibilidade para manutenção, sempre que possível tomando cuidados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot das mesmas para posterior análise.

**Recuperação**

Caso exista Plano de Continuidade de Negócio dos sistemas impactados, eles devem ser iniciados, conforme especificado.

A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema.

O TRI tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação.

Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas.

Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do sistema operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

**Lições Aprendidas**

Com o incidente contido e sua resolução encaminhada, o TRI deve agendar e conduzir uma reunião de lições aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos

- inclusive deste Plano de Resposta a Incidentes.

As melhorias sugeridas na reunião, com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.



Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**

**Documentação**

O TRI deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

**Comunicações**

Assim que possível, no caso de incidente com vazamento de dados pessoais, o Encarregado de Tratamento de Dados (DPO) deve avaliar e fazer as comunicações obrigatórias por Lei, se houverem, bem como informar e subsidiar os Encarregados de Tratamento de Dados dos controladores do sistema. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados, relatórios formais para a ANDP.

Comunicação de incidente de segurança — Autoridade Nacional de Proteção de Dados (www.gov.br)

**DPO** → Eduardo Scheffer (eduardo@plattano.com.br)



Rua Santa Luzia, n.100 Sala 619-620 – Trindade – CEP 88036-540- Florianópolis/SC.
**Telefone: 48 3197-9877 e 48 99961-0729 e-mail: contato@plattano.com.br**