Política de Segurança da Informação (PSI)

Data:	13/05/2025
Assessor de Segurança da informaçao:	DANIEL BORGES DE JESUS

Introdução

Este manual tem como objetivo principal orientar todos os colaboradores da **Tremendão Repinturas e Auto Peças** sobre como agir imediatamente ao identificar ou tomar conhecimento de qualquer evento que possa ser um incidente de segurança da informação. O foco é garantir que essa informação chegue rapidamente à pessoa responsável na **Tremendão Repinturas e Auto Peças** para que as medidas necessárias sejam tomadas o quanto antes, protegendo nossos clientes, nossos negócios e nossos dados.

Destinatários

Aplica-se a todos os colaboradores, prestadores de serviço e sistemas que processem informações sob responsabilidade do controlador e que identifiquem qualquer evento que possa configurar um incidente de segurança da informação, conforme definido neste manual.

Este manual foi confeccionado com a Assessoria jurídica do escritório Brasil e Silveira Advogados, responsável pelo suporte jurídico no tratamento de dados e segurança da informação.

2. Definição

2.1. Incidente de Segurança da Informação

Um incidente de Segurança da Informação é qualquer evento que acontece e que pode colocar em risco a confidencialidade (informações acessadas por quem não deveria), a integridade (informações alteradas ou destruídas sem autorização) ou a disponibilidade (sistemas ou informações inacessíveis quando necessário) das informações.

São exemplos de incidente de Segurança da Informação

- O desfiguramento do portal web de uma instituição;
- A evasão de informações confidenciais;
- A propagação de um vírus ou worm por meio da lista de contatos de e-mails; Envio de spam;
- Indisponibilidade de um servidor de banco de dados;
- Tentativas não autorizadas de acesso.

Qualquer ocorrência que fuja do normal e que possa ter um impacto negativo na segurança das informações de uma organização é um incidente. O gerenciamento desses incidentes é fundamental para minimizar os danos e restabelecer a segurança o mais rápido possível.

2.2. Gerenciamento de Incidentes de Segurança da Informação

o Gerenciamento de Incidentes de Segurança da Informação é uma metodologia organizada e previamente definida por uma instituição para lidar com as consequências de uma violação de segurança da informação.

Os objetivos específicos do Gerenciamento de Incidentes de Segurança da Informação são:

- Garantir que os eventos sejam detectados e tratados de forma adequada, incluindo a correta categorização como incidentes de segurança da informação ou não.
- Assegurar que os incidentes de segurança da informação sejam identificados, avaliados e respondidos da maneira mais apropriada possível.
- Minimizar os efeitos negativos dos incidentes de segurança da informação, tratando-os o mais rapidamente possível.
- Reportar as vulnerabilidades de segurança da informação e tratá-las adequadamente.
- Contribuir para a prevenção de futuras ocorrências, mantendo uma base de "lições aprendidas" (similar a uma base de dados de erros conhecidos).

2.3. Assessor de Segurança da Informação

O Assessor de Segurança da Informação é o profissional responsável pelo processo de Gerenciamento dos Incidentes de Segurança da Informação. Entre suas atribuições estão:

- Garantir o preenchimento adequado do Relatório de Incidentes de Segurança da Informação (RISI);
- Assegurar que a avaliação de impacto seja feita de maneira adequada;
- Promover análise de riscos de segurança da informação e propor ações para mitigá-los, levando em conta o potencial impacto e os riscos envolvidos.
- Promover a melhoria contínua dos indicadores relacionados à Segurança da Informação.
- Manifestar-se sobre assuntos de Segurança da Informação, seja por iniciativa própria ou quando solicitado.
- Propor e revisar normas de Segurança da Informação.

2.4. RISI - Relatório de Incidente de Segurança da Informação

O Relatório de Incidente de Segurança da Informação é a ferramenta fundamental utilizada para o registro e acompanhamento de um incidente de segurança.

O RISI é um documento formal onde todas as informações relevantes sobre um incidente são compiladas, desde o momento em que ele é detectado até a sua resolução e análise final.

O Assessor de Segurança da Informação tem a responsabilidade de garantir que o RISI seja preenchido de forma adequada e clara.

3. Procedimento no Momento da Ciência do Incidente

Este procedimento detalha as ações a serem tomadas imediatamente após a detecção ou ciência de um possível incidente de segurança.

A informação do incidente é uma das etapas do Gerenciamento de Incidentes, que deverá ser registrado e comunicado ao Assessor de Segurança da Informação para acompanhamento e monitoração do atendimento até sua resolução.

Passo 1: Detecção e Reconhecimento:

- Ao identificar qualquer atividade suspeita, falha inesperada, acesso não autorizado, perda de dados ou qualquer outro evento que se enquadre na definição de incidente de segurança, o colaborador ou sistema deve reconhecer que um possível incidente ocorreu.
- *Ação Imediata:* Não tentar resolver o problema sozinho, a menos que seja uma ação de contenção básica e segura previamente autorizada (ex: desconectar um cabo de rede de um dispositivo suspeito, se instruído a fazê-lo). A prioridade é notificar.

Passo 2: Avaliação Inicial Rápida (Pelo Notificador):

- Realizar uma avaliação preliminar e rápida da situação para coletar informações essenciais para a notificação.
- *Informações a Coletar (se possível e seguro):*
  - O que aconteceu (descrição breve)?
  - Quando foi detectado?
  - Onde ocorreu (sistema, equipamento, local)?
  - Quem foi afetado (usuários, sistemas, dados)?
  - Qual o impacto aparente (sistema lento, inacessível, dados expostos)?
  - Qual a origem do alerta (você, um colega, um sistema de monitoramento)?

Passo 3: Notificação Imediata ao Assessor de Segurança da Informação (ou Equivalente):

- **Para incidentes de IMPACTO ALTÍSSIMO (Prioridade 1) ou ALTO (Prioridade 2):**
  - ACIONAR imediatamente (pessoalmente ou por meio de contato telefônico) relatando os fatos determinantes."
    - Utilizar os contatos de emergência fornecidos (telefone, ramal, contato pessoal) para garantir que o Assessor de Segurança da Informação seja alertado imediatamente.
    - Fornecer as informações coletadas na Etapa 2.
    - Após o contato imediato, preencher o Relatório de Incidentes de Segurança da Informação (RISI) o mais rápido possível com os detalhes disponíveis.

- **Para incidentes de IMPACTO ELEVADO (Prioridade 3) ou MÉDIO (Prioridade 4):**
  - NOTIFICAR por e-mail o Assessor de Segurança da Informação relatando os fatos determinantes e resolução do incidente.
    - Enviar um e-mail para o endereço designado do Assessor de Segurança da Informação, incluindo as informações coletadas na Etapa 2.
    - O e-mail deve ter um assunto claro indicando "Incidente de Segurança - [Breve Descrição]".
    - Em alguns casos de menor impacto, a resolução pode ocorrer antes ou junto com a notificação por e-mail. No entanto, a notificação *deve* ocorrer mesmo que a resolução pareça simples, para garantir o registro e a avaliação centralizada.

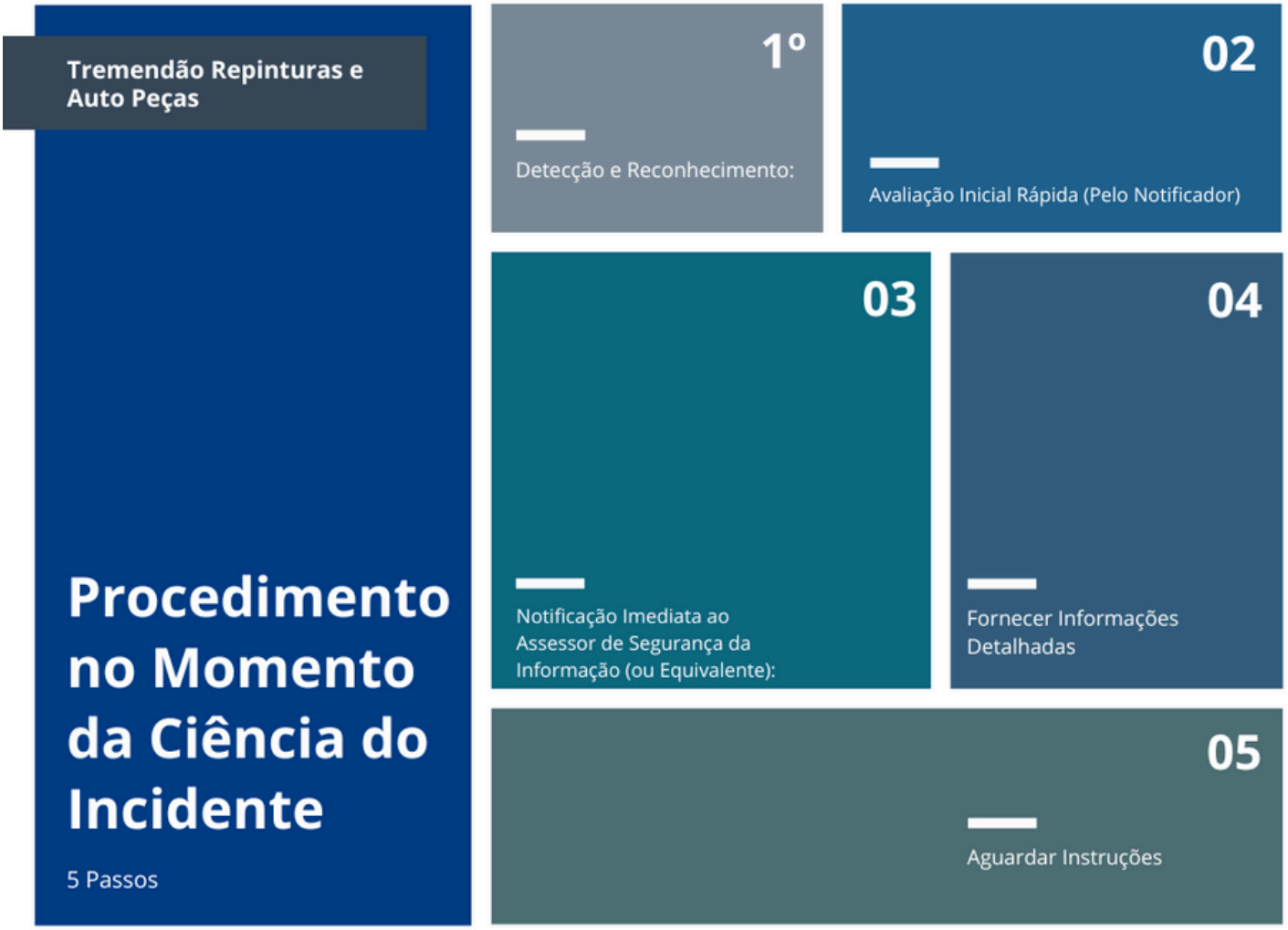
- **Para incidentes de IMPACTO BAIXO (Prioridade 5):**
  - Todo incidente de segurança deverá ser registrado e comunicado ao Assessor de Segurança da Informação.
  - Notificar por e-mail ou registrar no sistema RISI, fornecendo as informações coletadas na Etapa 2.

Passo 4: Fornecer Informações Detalhadas :

- Após a notificação inicial, o notificador deve estar disponível para fornecer mais detalhes ao Assessor de Segurança da Informação e colaborar na investigação inicial.
- *Exemplos de detalhes:* Capturas de tela, logs de erro, descrição exata das ações realizadas antes do incidente, nomes de arquivos envolvidos, etc.

Passo 5: Aguardar Instruções:

- Uma vez feita a notificação, o notificador deve aguardar as instruções do Assessor de Segurança da Informação ou da equipe de resposta a incidentes.
- Não tomar ações adicionais (como desligar equipamentos críticos, excluir arquivos, etc.) sem orientação, pois isso pode destruir evidências importantes para a investigação.



4. Avaliação de Impacto e Prioridade

Ao receber a notificação, o Assessor de Segurança da Informação realizará uma avaliação formal do impacto para determinar a prioridade da resposta e o método de comunicação interna e externa (se aplicável).

- **Prioridade 1 (Altíssimo Impacto):** Afeta toda a organização, causa dano generalizado à imagem institucional, indisponibilidade ou mau funcionamento generalizado de sistemas/recursos críticos, compromete integridade/confidencialidade de sistemas institucionais, compromete serviços de TI à comunidade judiciária, ou reportado por usuário estratégico/VIP.
- **Prioridade 2 (Alto Impacto):** Impede ou inviabiliza trabalhos de múltiplos grupos/áreas, indisponibilidade ou mau funcionamento de conjunto de serviços essenciais, equipamento/serviço operacional mas com funções principais degradadas.
- **Prioridade 3 (Elevado Impacto):** Falha impossibilita trabalho diário de um ou mais usuários em um grupo específico (ex: problema em equipamento/sistema específico, falha de rede em sala/setor, indisponibilidade de estação de trabalho, problema em serviço essencial para o usuário).
- **Prioridade 4 (Médio Impacto):** Falha afeta trabalho diário de um ou mais usuários em grupo pequeno, equipamento/serviço coletivo normal mas com funções secundárias falhas/lentas, requisição de serviço cujo não atendimento imediato não impede trabalho principal.
- **Prioridade 5 (Baixo Impacto):** Equipamento/serviço com falha mas sem possibilidade de intervenção imediata por necessidade do usuário, serviço afetado operando em modo de contingência, requisição que pode ser atendida posteriormente sem prejuízo, solicitação de mudança programada.

5. Relatório de Incidentes de Segurança da Informação (RISI)

Todo incidente, uma vez notificado, deve ser formalmente registrado. O RISI deve conter, no mínimo, as seguintes informações:

- Número do RISI e Ticket (se aplicável)
- Descrição resumida do incidente
- Período em que ocorreu (Data/Hora Início e Fim)
- Severidade (Prioridade 1 a 5)
- Tipo de Impacto (Confidencialidade, Integridade, Disponibilidade)
- Origem do alerta
- Data e Hora da Notificação ao Assessor de Segurança da Informação
- Comunicação do incidente (a quem foi informado)
- Detalhamento do Incidente (categoria, descrição completa, extensão, impactos, causas prováveis, áreas envolvidas na investigação)
- Tratamento do Incidente (ações de contenção/contorno, equipes envolvidas)
- Análise e Encerramento (ações adicionais para finalizar/evitar recorrência, lições aprendidas, identificador do chamado/problema vinculado)

É fundamental registrar *toda informação relevante durante o ciclo de vida do incidente*.

Próximos Passos (Após a Notificação Inicial):

Uma vez que o incidente é notificado internamente e o Assessor de Segurança da Informação assume a gestão, o processo segue para as etapas de:

- Contenção do incidente para limitar os danos.
- Investigação para determinar a causa raiz.
- Erradicação da causa e recuperação dos sistemas/dados.
- Avaliação final do impacto, especialmente no que diz respeito aos dados pessoais e aos direitos dos titulares.
- Decisão sobre a necessidade de comunicação externa à ANPD e/ou aos titulares dos dados, conforme os critérios estabelecidos pela LGPD e regulamentos da ANPD (como a Resolução CD/ANPD nº 15), dentro dos prazos legais (3 dias úteis para a ANPD, se aplicável).
- Implementação de medidas preventivas para evitar futuras ocorrências, com base nas lições aprendidas.

5.1. Modelo de relatório de incidentes de segurança da informação

RISI - Relatório de Incidente de Segurança da Informação

Equipe de Tratamento e Resposta a Incidentes de Segurança na empresa Tremendão Repinturas e Auto Peças *(Adaptado do modelo 2025)*

1 – Informações do RISI

- Descrição do incidente:
- Data e hora de abertura:
- Data e hora de fechamento:
- Severidade do incidente: ( ) Alta. ( ) Média ( ) Baixa
- Impacto do incidente: ( ) Confidencialidade ( ) Integridade ( ) Disponibilidade

2 – Identificador do Incidente

- Origem da identificação: ( ) Interna. ( ) Externa

3 – Detalhamento do Incidente:

4 – Investigação do incidente

- Descrição detalhada do incidente de segurança da informação:
- Descrição detalhada da investigação:
- Equipe(s) responsável(is) pela investigação:

5 – Ação de Contenção

- Descrição detalhada da(s) ação(ões) de contenção/contorno:
- Data e hora de proposição da ação:

6 – Comunicação a partes interessadas

- Informar a quem o incidente foi comunicado:
- Data e hora da comunicação: dd/mm/aaaa hh:mm
- Pessoa(s) comunicada(s) / Meio de comunicação:

Responsável pelo preenchimento do RISI:

Data do preenchimento:

TREMENDÃO
Repinturas

Documento assinado digitalmente
gov.br
DANIEL BORGES DE JESUS
Data: 19/05/2025 15:38:25-0300
Verifique em https://validar.iti.gov.br