PODER JUDICIÁRIO
de Santa Catarina

Plano de Resposta a Incidentes Cibernéticos

Out de 2025

Sumário

Controle de Versões e Aprovações

Versões

Ver.	Descrição	Autor
1.0	Criação documento	Diretoria de Tecnologia da Informação

Aprovações

Ver.	Data	Aprovador
1.0	02/10/2025	Daniel Moro de Andrade, Diretor de Tecnologia da Informação

Resumo Executivo

Este Plano de Resposta a Incidentes (PRI) define a governança, os papéis, a classificação e os indicadores estratégicos para gestão de incidentes de segurança cibernética do PJSC dentro do escope estabelecido. Os procedimentos operacionais detalhados foram organizados como playbooks operacionais separados.

Objetivo

O objetivo deste documento é fornecer orientação para a ETIR (Resolução GP Nº 38/2021 e Resolução GP Nº 27/2024) e outras partes interessadas em como responder de maneira eficiente e eficaz aos incidentes de segurança cibernética (eventualmente aqui chamados apenas incidentes) que possam afetar os pilares da segurança da informação, ou seja, a confidencialidade, integridade e disponibilidade dos ativos de TI do PJSC. Responder desta forma eficiente e eficaz é crucial para minimizar os riscos para a operação e serviços oferecidos, portanto, o TJSC por meio deste documento estratégico visa definir os procedimentos e ações que este órgão deve seguir para detectar, responder, conter e se recuperar de incidentes de segurança cibernética, como ataques cibernéticos, falhas em sistemas ou vazamento de dados, por meio de planejamento e execução de procedimentos de resposta a incidentes cuidadosamente projetados e bem mantidos.

Este Plano de Resposta a Incidentes (PRI) é projetado para:

- Descrever os requisitos e expectativas para a resposta a incidentes;
- Estabelecer os papéis e responsabilidades dos envolvidos na resposta a incidentes;
- Definir parâmetros para declarar, categorizar e priorizar incidentes;
- Estabelecer o ciclo de vida e o processo de resposta a incidente;
- Criar canais de comunicação e escalonamento durante um incidente.

Resultados esperados:

1. <u>Detecção Rápida e Precisão na Identificação de Incidentes</u>
    - Redução do tempo médio de detecção (*MTTD - Mean Time to Detect*).
    - Identificação eficaz de ameaças reais, reduzindo falsos positivos.
    - Correlação eficiente de eventos suspeitos através de ferramentas SIEM e inteligência de ameaças.
2. <u>Contenção e Mitigação Eficientes</u>
    - Bloqueio imediato de atividades maliciosas para evitar a propagação do ataque.

- Isolamento de dispositivos comprometidos sem interromper operações críticas.
- Redução do tempo médio de contenção (*MTTC - Mean Time to Contain*).

3. Resposta e Remediação Eficazes
    - Aplicação rápida de patches e correções de segurança.
    - Remoção completa de *malwares*, *backdoors* e acessos não autorizados.
    - Restauração de sistemas e serviços afetados sem perda de dados essenciais.
4. Minimização do Impacto Operacional e Financeiro
    - Redução de tempo de inatividade e continuidade dos negócios.
    - Diminuição de custos com multas, litígios e compensações devido a vazamentos de dados.
    - Preservação da reputação do órgão diante da sociedade.
5. Comunicação Transparente e Coordenação Eficiente
    - Notificação ágil de incidentes às partes interessadas, incluindo equipes internas, sociedade e órgãos reguladores.
    - Relatórios detalhados para auditorias e conformidade (ex: LGPD, GDPR, PCI DSS).
    - Comunicação estruturada entre times internos, fornecedores e parceiros de TI.
6. Aprendizado Contínuo e Melhoria do Processo
    - Geração de relatórios pós-incidente (*post-mortem*) para análise do ocorrido.
    - Atualização do Plano de Resposta a Incidentes com lições aprendidas.
    - Implementação de treinamentos e simulações (*tabletop exercises*) para reforçar a prontidão da equipe.
7. Conformidade com Regulamentações e Normas
    - Atendimento a requisitos de segurança como ISO 27001, NIST, CIS Controls e LGPD.
    - Garantia de auditorias bem-sucedidas sem penalizações.
    - Relatórios detalhados para órgãos reguladores e clientes afetados.

Gestão do Documento

Este Plano de Resposta a Incidentes (PRI) requer manutenção e revisão periódica anual ou anterior a este período caso seja necessário. O ETIR, podendo atuar em conjunto com os demais núcleos de segurança da informação, precisará estar atento sobre as informações que sejam pertinentes ao catálogo de serviços de negócios que deverão ser revisados ou incluídos, e suas respectivas mudanças, cabendo também revisar este PRI gerando uma versão mais atualizada, para que o plano esteja aderente ao negócio e cumprindo seu objetivo de forma eficiente e eficaz.

Em cada revisão, estes fatores essenciais devem ser considerados:

- A eficácia da versão anterior do PRI (ETIR);
- Mudanças na legislação relacionada (instruções normativas, resoluções e portarias) do TJSC;
- Mudanças na Política de Segurança da Informação do PJSC;
- Mudanças nas políticas de privacidade e uso aceitável em relação aos ativos do PJSC;
- Mudanças nas definições regulatórias de dados protegidos;
- As peculiaridades e vulnerabilidades de novos sistemas e software;
- O custo e a necessidade de armazenar dados relacionados a eventos de segurança cibernética;
- Políticas de minimização e destruição de dados;

Além das revisões formais, o PRI deve ser revisto sempre que sejam reveladas deficiências nas políticas ou procedimentos durante a remediação de um incidente de segurança.

Gestão das Informações do Incidente

Toda a informação gerada ou coletada durante um incidente de cibersegurança será classificada como sigilosa, em conformidade com a política vigente para classificação de processos sigilosos no SEI. A concessão de credencial para acesso a informações sigilosas será autorizada exclusivamente pelo Gestor do Incidente ou pelo Coordenador do NSEC.

É necessário manter um registro minucioso das decisões tomadas e das ações executadas, documentando a data, o horário e as pessoas envolvidas em cada uma dessas ações e decisões.

Termos e Definições

- Ameaça: É a exposição à qualquer evento ou circunstância que possa causar danos, prejuízos ou impactos negativos. Exemplos: infecção por *malware* (abreviação de *malicious software*, ou "software malicioso" em português), um desastres naturais, falhas técnicas, ou até mesmo ações maliciosas de pessoas.

- Ataque: É a técnica de explorar vulnerabilidades em sistemas computacionais sem autorização. Essas ações criminosas podem ocorrer em diversos tipos de sistemas e, quando direcionadas às aplicações, podem comprometer a infraestrutura corporativa. Além disso, também existem ataques de engenharia social, nos quais o criminoso busca convencer a vítima a realizar ações que possam causar danos.

- *Malware*: É qualquer tipo de programa ou código desenvolvido com a intenção de prejudicar, explorar ou obter acesso não autorizado a sistemas, redes ou dispositivos. Exemplos: Vírus, *Ransomware* dentre outros.

- Risco: É a combinação da probabilidade de que uma ameaça ocorra e o impacto que ela pode ter, considerando tanto a possibilidade do evento negativo quanto as consequências que poderia trazer. Exemplo: se um determinado computador não tem antivírus e o impacto de um *malware* seria significativo, o risco associado a essa situação é considerado alto.

- SOC (*Security Operations Center*): Centro de Operações de Segurança responsável por monitoramento e resposta a incidentes.

- *Threat Intelligence:* Processo de coleta e análise de informações sobre ameaças cibernéticas.

- TTPs (Táticas, Técnicas e Procedimentos): Conjunto de métodos usados por atacantes, conforme o MITRE ATT&CK.

- Vulnerabilidade: Fraqueza dentro do ambiente que o deixa exposto a riscos. Exemplos na Segurança Cibernética: Software desatualizado; Senhas Fracas; Software instalado de forma padrão, sem a devida customização para segurança.

- *Zero Trust Security*: Modelo de segurança baseado no princípio de "nunca confiar, sempre verificar".