PLANO DE RESPOSTA A INCIDENTES

CONTROLE DE REVISÕES DESTE DOCUMENTO

ITEM	EMISSÃO / REVISÃO	DATA
00	Emissão deste documento	25/10/2024
01	Revisão de Layout e aprovação	25/10/2024

SUMÁRIO

1. INTRODUÇÃO

Este Plano de Resposta a Incidentes de Segurança da Informação define os processos e procedimentos que o SITRANS seguirá para detectar, responder, mitigar e aprender com incidentes de segurança da informação, garantindo que as informações e os sistemas do Sindicato permaneçam protegidos.

O plano foi criado para assegurar a continuidade dos negócios em caso de incidentes minimizar os impactos à operação.

2. Objetivo

O objetivo deste plano é estabelecer as diretrizes para garantir que os sejam gerenciados de maneira eficiente, minimizando os impactos na confidencialidade, integridade e disponibilidade das informações.

3. Escopo

Este plano se aplica a todos os colaboradores, prestadores de serviços, sistemas e dados sob a responsabilidade do Sindicato. Inclui qualquer incidente que possa comprometer a segurança das informações ou das operações do Sindicato.

4. Definições e Classificações de Incidentes

4.1. Definição de Incidente de Segurança da Informação

Um incidente de segurança da informação é qualquer evento que possa comprometer a confidencialidade, integridade ou disponibilidade das informações ou dos sistemas de informação.

4.2. Classificação de Incidentes

Os incidentes serão classificados de acordo com a gravidade e o impacto sobre as operações da Sindicato:

- **Baixa Gravidade**: Incidentes que afetam poucos usuários ou sistemas, com impacto mínimo.
- **Média Gravidade**: Incidentes que causam impacto moderado nas operações, mas que podem ser gerenciados com recursos internos.
- **Alta Gravidade**: Incidentes que causam impacto significativo nas operações, potencialmente exigindo uma parada operacional ou a intervenção de especialistas externos.
- **Crítica**: Incidentes que resultam em perda significativa de dados, interrupção prolongada de serviços ou comprometimento severo de segurança.

4.3. Prioridade de incidentes

A resposta a incidentes será priorizada de acordo com a sua classificação que será realizada pela equipe técnica. Incidentes de baixa gravidade terão prioridade 4 (P4), enquanto incidentes de classificação crítica terão prioridade 1 (P1).

Nível de prioridade	Resumo das prioridades	Definição de prioridade	Resposta ao cliente	Resposta operacional (SLA)
P1	Perda total de serviço ou violação legal/regulamentar	- Violação de dados; - Emergência; - As operações do cliente não podem continuar; - Ninguém pode fazer login, o que afeta todos os usuários; - O sistema trava indefinidamente; - O aplicativo trava constantemente; - Módulo de missão crítica não disponível; - Não há solução alternativa disponível	**Intervenção Comercial:** Imediatamente **Atualizações aos clientes:** Assim que o incidente for resolvido **Resolução do problema:** O mais brevemente possível	**Intervenção técnica:** Imediatamente **Atualizações as partes interessadas:** Sempre que houver evolução na resolução do problema **Resolução do problema:** Em menos de 24hrs

P2	Perda grave de serviço	- Componente principal indisponível; - Parte corrompida ou gravemente degradada; - Afeta vários usuários - >5%; - Afeta vários clientes; - Problema de conformidade; - Não há solução alternativa sustentável disponível	**Intervenção Comercial:** Imediatamente **Atualizações aos clientes:** Assim que o incidente for resolvido **Resolução do problema:** Em acordo com prazos estipulados pela equipe técnica	**Intervenção técnica:** Em até 01 hora **Atualizações as partes interessadas:** Sempre que houver evolução na resolução problema **Resolução do problema:** Em até 24 horas
P3	Pequena perda de serviço	- Problema funcional do sistema; - O módulo utilizável não está funcionando como projetado; - Afeta vários usuários - <5%	**Intervenção Comercial:** Imediatamente **Atualizações aos clientes:** Assim que o incidente for resolvido **Resolução do problema:** Em acordo com prazos estipulados pela equipe técnica	**Intervenção técnica:** Em até 02 horas **Atualizações as partes interessadas:** Sempre que houver evolução na resolução do problema **Resolução do problema:** Em até 01 semana
P4	Informativo	Não afeta o serviço core empresarial Falhas de consulta específicas Solicitação de documentação Funcionando conforme projetado, mas afetando a experiência do cliente	**Intervenção Comercial:** Imediatamente **Atualizações aos clientes:** Assim que o incidente for resolvido **Resolução do problema:** Em acordo com prazos estipulados pela equipe técnica	**Intervenção técnica:** Em até 04 horas **Atualizações as partes interessadas:** Sempre que houver evolução na resolução do problema **Resolução do problema:** Em até 15 dias.

5. Time de Resposta a Incidentes (TRI)

5.1. Funções e Responsabilidades

O Time de Resposta a Incidentes (TRI) é o grupo de pessoas com acessos, habilidades, responsabilidades, treinamento e conhecimentos para responder aos mais variados tipos de incidentes. No caso do Sindicato, o TRI será composto pela Comissão de Lei Geral de Proteção de Dados e pelo Encarregado de dados Pessoais, que poderá solicitar auxílio de qualquer outra área, pilar ou profissional do SINDICATO, sendo recomendável, quando necessário, que antes de qualquer resposta consulte o setor jurídico para que este leia e faça considerações pertinentes sobre o teor da resposta.

5.2. Tabela de Responsabilidades por Função

Esta tabela define claramente as funções e responsabilidades de cada membro envolvido no processo de resposta a incidentes de segurança da informação, assegurando que cada etapa do plano seja executada de forma eficaz e dentro dos prazos estabelecidos. Destaca-se, desde já, que o DPO dever ser comunicado em qualquer incidente envolvendo dados pessoais, tão logo seja identificado o incidente.

Função	Responsabilidades	Escalonamento
Responsável pelo Incidente (Central de Serviços de TI)	- Receber notificações iniciais de incidentes - Avaliar a criticidade do incidente - Notificar as partes envolvidas - Gerenciar comunicação com todas as partes interessadas, se necessário	Escalonar para: Gerência de TI em incidentes P1 e P2
Departamentos Comercial e de Tecnologia	- Avaliar a gravidade do incidente - Coordenar medidas de contenção e recuperação - Documentar todas as etapas do	Escalonar para: Gerência Administrativa em casos de P1 e P2

Função	Responsabilidades	Escalonamento
	incidente - Assegurar a comunicação interna e externa	
Equipe Técnica de TI (Colaboradores e fornecedores)	- Implementar ações de contenção e recuperação - Monitorar a integridade dos sistemas após a resolução do problema - Realizar testes de verificação e garantir restauração completa	Escalonar para: TRI em caso de dificuldades técnicas
Jurídico (Assessoria externa)	- Revisar e aprovar a comunicação oficial com reguladores e titulares de dados - Assessorar em conformidade com a LGPD e outras regulamentações aplicáveis	Escalonar para: DPO em caso de exigências legais urgentes
Comitê de Tecnologia (Gerentes de TI de todas as Filiais)	- Reavaliar os riscos relacionados ao incidente - Propor ajustes na matriz de risco - Participar de reuniões de lições aprendidas pós-incidente	Escalonar para: Alta Administração em casos críticos
Alta Administração (Coordenação Administrativa de todas as filiais)	- Autorizar medidas emergenciais para contenção - Validar relatórios pós-incidente	Escalonar para: Presidente em incidentes de grande escala

Função	Responsabilidades	Escalonamento
	- Tomar decisões estratégicas em incidentes com impacto financeiro	

6. Processo de Resposta a Incidentes

6.1. Detecção de Incidentes

A identificação de qualquer Incidente de Segurança é aspecto chave para a boa implementação de um Plano de Resposta a Incidentes. Os incidentes podem ser detectados de diversas formas, incluindo:

- Monitoramento de sistemas
- Relatórios de usuários
- Auditorias e testes de vulnerabilidade

É fundamental, ainda, um trabalho contínuo de sensibilização e capacitação dos profissionais do Sindicato, para que tenham a capacidade de identificar e informar eventual incidente de segurança, de que tenham conhecimento/acesso.

A comunicação inicial do incidente pode ser proveniente de qualquer fonte, devendo todas serem registradas, diretamente pelo Notificador.

A Notificação inicial é recebida pelo Encarregado de Dados Pessoais, que deverá fazer uma análise preliminar e acionar o Time de Resposta a Incidentes para realizar a avaliação e classificação.

Na avaliação preliminar, devem ser buscadas informações sobre os sistemas/processos que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco de a situação agravar-se, caso não haja resposta imediata.

6.2. Avaliação e Classificação

Após a detecção, o incidente será avaliado pelo Time de Resposta a Incidentes, para determinar sua gravidade e o impacto potencial no Sindicato, de acordo com os critérios constantes do item 4.3. A avaliação inicial incluirá:

- Natureza do incidente
- Sistemas e dados afetados
- Impacto potencial
- Urgência da resposta necessária

Na fase de avaliação e classificação, é importante identificar a causa do incidente, atores e ações envolvidas, vulnerabilidades exploradas, com o objetivo de definir ações para as fases subsequentes.

6.3. Contenção

Uma vez que o incidente foi identificado e avaliado, medidas devem ser tomadas para conter seu impacto. Isso pode incluir:

- Isolamento de sistemas comprometidos
- Interrupção de acessos comprometidos
- Aplicação de patches ou atualizações

6.4. Erradicação

Após a contenção, o time técnico deve eliminar a causa raiz do incidente, garantindo que a vulnerabilidade ou falha seja completamente removida. Isso pode incluir:

- Remoção de malware
- Reconfiguração de sistemas
- Implementação de políticas de segurança adicionais

Devem ser adotados todos os cuidados para não impactar evidências que possam ser usadas para identificar autoria, origem e método para quebrar a segurança.

6.5. Recuperação

O passo seguinte é restaurar os sistemas afetados à operação normal, garantindo que a segurança tenha sido restabelecida:

- Restauração de dados a partir de backups seguros;
- Verificação da integridade dos sistemas restaurados;
- Monitoramento contínuo para garantir que o incidente não se repita;

Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, ou elaboração de novas rotinas processuais.

6.6. Análise Pós-Incidente

Após a resolução do incidente, o Time de Resposta a Incidentes deve realizar uma análise detalhada para determinar:

- O que causou o incidente
- A eficácia das medidas de contenção e recuperação
- Melhorias nos processos e controles para evitar futuros incidentes

6.7. Comunicação e Notificação

A comunicação adequada é fundamental durante um incidente. Dependendo da gravidade, diferentes partes interessadas serão notificadas:

- **Internamente**: O time técnico, TRI, gerência e alta administração devem ser informados imediatamente.
- **Externamente**: Caso se conclua que o incidente acarretou risco ou dano relevante aos titulares de dados pessoais, o DPO juntamente com o Jurídico deverá fazer as comunicações obrigatórias previstas na Lei. Essas comunicações podem incluir informações para os titulares de dados e imprensa, bem como comunicações formais para a ANPD. A comunicação será no prazo de três dias úteis, ressalvada a existência de prazo para comunicação previsto em legislação específica. , conforme definido pela autoridade nacional na Resolução CD/ANPD nº 15/2024, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. A ANPD poderá eventualmente solicitar o envio de Relatórios sobre os fatos ocorridos e os atos praticados que visaram a mitigar o incidente.

6.8. Documentação

O DPO deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações executadas, inclusive as da reunião de lições aprendidas. Após a neutralização da ameaça, o Encarregado de Dados (DPO) deve elaborar um relatório circunstanciado de todas as medidas que foram adotadas, apresentando todas as informações relevantes, tais como, informações sobre o incidente em si (quando foi identificado, qual sua natureza, danos ou potenciais danos causados, a extensão, a relevância e a repercussão desses danos, etc.); providências adotadas para preservação das evidências, procedimentos seguidos para a contenção da crise; medidas de correção técnicas e de Governança adotadas; questionamentos e demandas externas (requerimentos de titulares de dados, autoridades e imprensa, bem como suas respostas); deliberações do TRI.

7. Comunicação com Partes Interessadas

Durante e após um incidente, manter uma comunicação clara e precisa é essencial. As partes interessadas incluem:

- **Time Interno**: Fornecer atualizações regulares sobre o progresso da resolução do incidente.
- **Clientes**: Dependendo do tipo de incidente, os clientes podem precisar ser informados para garantir transparência e confiança.
- **Autoridades Legais/Reguladoras**: Incidentes que acarretem risco ou dano relevante aos titulares de dados podem exigir notificações formais às autoridades.
- **Mídia e Público**: Para incidentes com grande impacto público, uma comunicação coordenada com a Comunicação, Institucional e Jurídico pode ser necessária.

8. Treinamento e Simulações

Para garantir que todos os envolvidos no PRI estejam preparados para lidar com um incidente real, a Sindicato realizará regularmente:

- **Treinamentos** para o time envolvido na resposta a incidentes.
- **Simulações de incidentes** para testar a prontidão do time e a eficácia do plano.

9. Revisão e Atualização do Plano

Este plano será revisado regularmente, no mínimo anualmente, ou após qualquer incidente significativo. Além disso, revisões podem ser realizadas após mudanças tecnológicas ou organizacionais.

10. Conclusão

O Plano de Resposta a Incidentes do Sindicato é um elemento crítico para a segurança da informação e a continuidade dos negócios. Todos os colaboradores e partes interessadas devem estar cientes de suas responsabilidades e seguir os procedimentos descritos para garantir uma resposta eficiente a qualquer incidente.