	PROCEDIMENTO PARA INCIDENTE DE SEGURANÇA DA INFORMAÇÃO	Emissão:	Classificação:
Código:		Versão:	Aprovado por:

CONTEÚDO

1 Introdução

Este documento destina-se a ser usado quando ocorrer algum tipo de incidente que afete a segurança da informação de SUAPE, incluindo aqueles que, potencialmente, afetam os dados pessoais para os quais a organização é uma controladora. Destina-se a garantir uma resposta rápida, eficaz e ordenada a uma violação de segurança da informação.

Os procedimentos descritos neste documento devem ser usados apenas como orientação para resposta a um incidente. A natureza exata de um incidente e seu impacto não podem ser previstos com certezas e, portanto, é importante que o bom senso seja usado ao decidir as ações a serem tomadas.

No entanto, pretende-se que as estruturas apresentadas aqui sejam úteis para permitir que as ações corretivas sejam tomadas mais rapidamente e com base em informações precisas.

Os objetivos deste procedimento de resposta a incidentes são:

- fornecer uma visão geral e concisa de como SUAPE responderá a um incidente;
- definir quem responderá a um incidente e suas funções e responsabilidades;
- descrever as instalações que irão ajudar na gestão do incidente;
- definir como as decisões serão tomadas com relação à nossa resposta a um incidente;
- explicar como será a comunicação dentro da organização e com partes externas;
- fornecer detalhes de contato para pessoas-chave e agências externas.

Todos os membros da equipe mencionados neste documento receberão uma cópia deste que deverá ficar disponível sempre que necessário.

Os detalhes de contato serão verificados e atualizados, pelo menos, três vezes por ano. As alterações do contato ou de outros detalhes relevantes que ocorrerem devem ser comunicadas o mais breve possível.

Todas as informações pessoais coletadas como parte do procedimento de resposta a incidentes e contidas neste documento serão usadas exclusivamente para fins de gerenciamento de incidentes de segurança da informação e estão sujeitas à legislação de proteção de dados.

2 Fluxograma de Resposta a Incidentes

O fluxo do procedimento de resposta a incidentes é mostrado no diagrama abaixo.

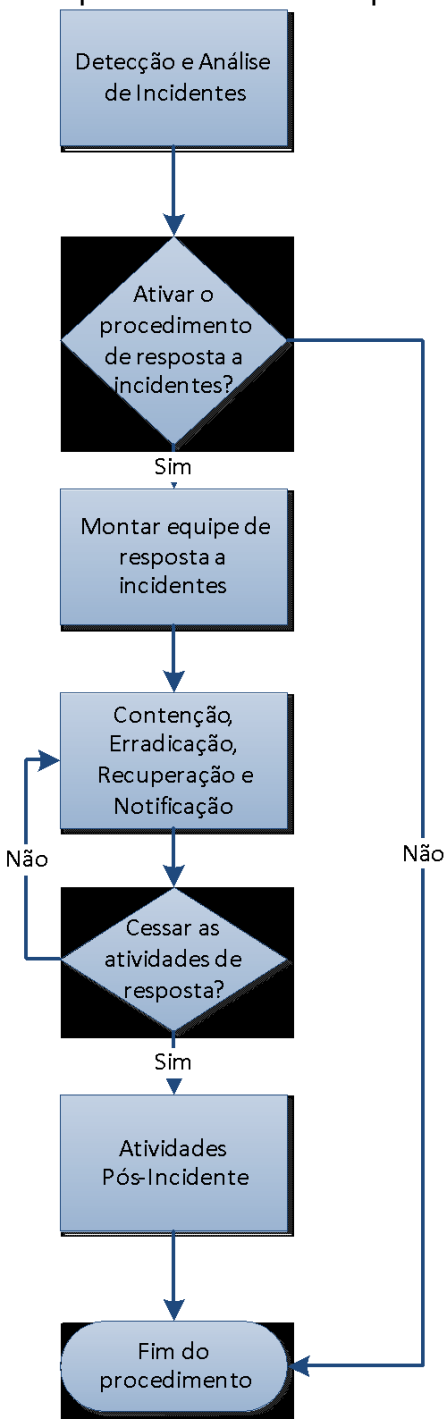

Figura 1 – Fluxograma de Resposta a Incidentes

Essas etapas são explicadas com detalhes nos próximos tópicos.

3 Identificar e Analisar o Incidente

Um incidente pode ser identificado inicialmente de várias formas e através de várias fontes diferentes, dependendo da natureza e localização do incidente. Alguns incidentes podem ser detectados automaticamente por meio de ferramentas de software usadas pela SUAPE ou por funcionários que notam atividades incomuns. Outros podem ser notificados por um terceiro, como um cliente, fornecedor ou agência de aplicação da lei que tenha conhecimento de uma violação.

É normal que haja uma demora entre a ocorrência do incidente e sua identificação real; um dos objetivos de uma abordagem proativa à segurança da informação é reduzir esse período de tempo. O fator mais importante é que o procedimento de resposta a incidentes deve ser iniciado o mais rápido possível após a identificação para que uma resposta efetiva possa ser dada.

Uma vez que o incidente tenha sido identificado, uma avaliação de impacto inicial deve ser realizada a fim de decidir a resposta apropriada.

Esta avaliação de impacto deve medir:

- A extensão do impacto na infraestrutura de TI, incluindo computadores, redes, equipamentos e acomodações;
- Os ativos de informação (incluindo dados pessoais) que podem estar em risco ou foram comprometidos;
- A duração provável do incidente, ou seja, quando pode ter começado;
- As unidades de negócio afetadas e a extensão do impacto para elas;
- Para as violações que afetam os dados pessoais, o grau de risco para os direitos e liberdades dos titulares dos dados;
- Indicação inicial da causa provável do incidente.

Essas informações devem ser documentadas para que haja um entendimento claro, disponível para uso atual ou em uma revisão posterior.

Uma lista de ativos de informação (incluindo dados pessoais), operações negociais, produtos, serviços, equipes e processos de suporte que possam ter sido afetados pelo incidente deve ser criada juntamente com uma avaliação da extensão do impacto.

Como resultado desta análise inicial, qualquer membro da equipe de gerenciamento tem autoridade para entrar em contato com o Líder da Equipe de Resposta a Incidentes a qualquer momento para solicitar que se inicie o Procedimento de Resposta a Incidentes.

4 Iniciar o Procedimento de Resposta a Incidentes

Uma vez notificado de um incidente, o Líder da Equipe deve decidir se a escala e o impacto real ou potencial do incidente justificam a ativação do Procedimento de Resposta a Incidentes e a convocação da equipe de resposta a incidentes.

As seguintes situações servem como diretrizes para determinar se uma resposta formal a um incidente deve ser iniciada:

- Existe uma perda real ou potencial, significativa, de informação, incluindo dados pessoais;
- Há uma interrupção, significativa, real ou potencial, nas operações de negócios;
- Existe um risco, significativo, para a reputação do negócio;
- Qualquer outra situação que possa causar impacto significativo para a organização.

Em caso de incerteza sobre ativar ou não uma resposta a um incidente a decisão do Líder da Equipe será a final.

Se for decidido não ativar o procedimento, um plano deve ser criado para que seja oferecida uma resposta de nível inferior pelos meios normais de gerenciamento. Isso pode envolver a invocação de outros procedimentos e outras pessoas.

Se o incidente justificar a ativação do procedimento de Resposta ao Incidente, o Líder da Equipe começará a montar a equipe.

5 Equipe de Resposta ao Incidente

Uma vez tomada a decisão de ativar o procedimento de resposta a incidentes, o Líder da Equipe (ou suplente) garantirá que todos os membros (ou seus substitutos) sejam informados sobre a natureza do incidente e o local apropriado para iniciar os procedimentos.

A exceção, será o membro da equipe que irá até o local do incidente para iniciar a coleta de informações para a avaliação do incidente que a equipe conduzirá.

5.1 Membros da Equipe de Resposta a Incidentes

A equipe de resposta a incidentes consistirá das seguintes pessoas e funções especificadas, embora a composição exata da equipe varie de acordo com a natureza do incidente.

Função/Coordenadoria	Cargo responsável da função
Líder do Time	DPO
Facilitador da Equipe	Auditor Interno
Tecnologia da Informação	Unidade de TI
Saúde e Segurança	Unidade de Saúde e Segurança
Recursos Humanos	Coordenadora de Recursos Humanos
Compliance	Unidade de integridade de gestão de riscos e controles internos
Comunicações (RP e Relações com as mídias)	Coordenadoria de comunicação
Jurídico e Regulatório	Assessoria jurídica

Tabela 1 – Membros da Equipe de Resposta a Incidentes

Os detalhes de contato das pessoas da equipe estão no *Anexo A* deste documento.

5.2 Funções e Responsabilidades

As responsabilidades das funções da equipe de resposta aos incidentes são as seguintes:

Líder do Time

- Decide se deve ou não iniciar uma resposta;
- Monta a equipe de resposta aos incidentes;
- Gerenciamento geral da equipe de resposta aos incidentes;
- Responsável pela comunicação com a diretoria e outras partes interessadas de alto nível;
- Tomador de decisão final em casos de desacordo.

Facilitador da Equipe

- Responsável pelo suporte da equipe;
- Coordena os recursos com a gerência;
- Prepara as reuniões e registra as ações e decisões;
- Mantém os resumos e status dos procedimentos atualizados;
- Facilita a comunicação via e-mail, fax, telefone ou outros métodos;

- Comparece ao local do incidente o mais rápido possível;
- Avalia a extensão e o impacto do incidente;
- Fornece as informações para a equipe;
- Fornece atualizações e respostas as perguntas necessárias para a tomada de decisões da equipe.

Tecnologia da Informação
- Fornece informações sobre questões relacionadas à tecnologia;
- Auxilia na avaliação de impacto.

Saúde e Segurança
- Avalia o risco para a vida;
- Garante que as responsabilidades legais pela saúde e segurança sejam cumpridas a todos os momentos;
- Contato com serviços de emergência, como polícia, bombeiros e médicos;
- Considera questões locais com relação ao incidente.

Recursos Humanos
- Avalia e aconselha sobre políticas de RH e questões de contrato de trabalho;
- Representa os interesses dos funcionários da organização;
- Aconselha sobre questões de capacidade.

Compliance
- Fornecer aconselhamento sobre opções de continuidade dos negócios;
- Invoca planos de continuidade dos negócios, se necessário;
- Contribui para a tomada de decisões com base no conhecimento das operações, produtos e serviços da empresa;
- Relatar aos outros membros da equipe sobre questões operacionais;
- Ajuda a avaliar o impacto provável aos clientes da organização.

Comunicações (Relações pessoais e Relações com as mídias)
- Responsável por garantir que as comunicações internas sejam eficazes;
- Decide o nível, frequência e conteúdo das comunicações com partes externas, como a mídia;
- Define a abordagem da comunicação para manter as partes afetadas informadas, por ex. clientes, acionistas;
- Monitora informações externas como notícias.

Jurídico e Regulatório
- Aconselha sobre o que deve ser feito para garantir a conformidade com as leis e estruturas regulatórias;
- Avalia as implicações legais reais e potenciais do incidente e ações subsequentes.

5.3 Gestão, Monitoramento e Comunicação de Incidentes

Uma vez que uma resposta apropriada ao incidente tenha sido identificada, a equipe precisa ser capaz de gerenciar a resposta, monitorar o status do incidente e assegurar que a comunicação efetiva esteja ocorrendo em todos os níveis.

Reuniões regulares da equipe devem ser realizadas com frequência e decidida pelo líder. Uma agenda deverá ser desenvolvida. O objetivo dessas reuniões é garantir o gerenciamento de incidentes de forma eficaz e que as decisões-chave sejam tomadas prontamente, com base em informações adequadas.

5.4 Procedimentos de Comunicação

É vital que as comunicações efetivas sejam mantidas entre todas as partes envolvidas na resposta ao incidente.

As seguintes diretrizes devem ser seguidas em todas as comunicações:

- Seja calmo e evite longas conversas;
- Aconselhe os membros da equipe interna sobre a necessidade de encaminhar solicitações de informações para a equipe;
- Se a chamada for atendida por alguém que não seja o contato:
  - Pergunte se o contato está disponível em outro local;
  - Se não puder ser localizado, deixe uma mensagem para que retorne em um determinado número;
  - Não forneça detalhes do incidente;
- Sempre documentar detalhes do tempo de chamada, respostas e ações.

Todas as comunicações devem ser registradas de forma clara e precisa, pois registros podem ser necessários como parte de uma ação legal em uma data posterior.

5.4.1 Comunicação à Autoridade Fiscalizadora de Proteção de Dados

Quando a empresa SUAPE atua como controladora, é necessário que, caso os incidentes que atinjam dados pessoais possam resultar em risco aos direitos e liberdades dos titulares de dados, sejam reportados à autoridade fiscalizadora de proteção de dados imediatamente ou dentro de 48 horas após tomar conhecimento do incidente. O Procedimento de Notificação de Violação de Dados Pessoais da SUAPE deve ser usado para essa finalidade. No caso de a meta de 48 horas não ser cumprida, as razões para o atraso devem ser reportadas.

5.4.2 Comunicação com os Titulares dos Dados Pessoais

Quando um incidente afeta dados pessoais, uma decisão deve ser tomada pelo Líder da Equipe em relação à extensão, tempo e conteúdo da comunicação com os titulares dos dados. A LGPD exige que a comunicação seja efetuada imediatamente, se a violação for suscetível de um risco elevado para os direitos e liberdades.

O Procedimento de Notificação de Violação de Dados Pessoais da SUAPE deve ser usado para essa finalidade.

5.4.3 Outra Comunicação Externa

Dependendo do incidente, pode haver uma variedade de partes externas que serão comunicadas. É importante que as informações divulgadas a terceiros sejam gerenciadas para serem oportunas e precisas.

Chamadas que não são de organismos diretamente envolvidos na resposta a incidentes (como a mídia) devem ser passadas para o membro da equipe responsável pelas comunicações.

Pode haver um número de partes externas que, embora não estejam diretamente envolvidas no incidente, podem ser afetadas e precisam ser alertadas sobre esse fato. Estes podem incluir:

- Clientes;
- Fornecedores;
- Órgãos reguladores.

O membro da equipe de Comunicação deve fazer uma lista dessas partes interessadas e definir a mensagem que deve ser dada a elas. Uma lista de externos é fornecida no *Anexo B*.

As partes interessadas que não tenham sido alertadas pela equipe podem entrar em contato para obter informações sobre o incidente e os seus efeitos. Essas chamadas devem ser registradas e passadas para o membro da comunicação.

5.4.4 Comunicação com a Mídia

Em geral, a estratégia de comunicação com relação à mídia será a emissão de atualizações via alta direção. Nenhum membro da equipe deve dar uma entrevista com a mídia, a menos que isso seja autorizado pela Direção .

A forma de comunicação com a mídia será definida pela equipe, em conjunto com a Alta Direção, escutando as orientações técnicas do membro de comunicação..

Ao redigir uma declaração para a mídia, as seguintes diretrizes devem ser observadas:

- As informações pessoais devem ser protegidas em todos os momentos;
- Atenha-se aos fatos e não especule sobre o incidente ou sua causa;
- Garantir que o aconselhamento jurídico seja obtido antes de quaisquer declarações serem emitidas;
- Tente antecipar questões que possam ser mencionadas;
- Enfatiza que uma resposta foi iniciada e que tudo está sendo feito.

Os seguintes membros serão nomeados como porta-vozes para a organização, caso sejam necessárias mais informações, por ex. conferência de imprensa:

Função	Escala de Incidentes
Coordenador de comunicação	Médio e Baixo
Diretor Executivo	Alto

Tabela 2 – Porta-vozes de Mídia

O porta-voz indicado como mais apropriado dependerá da escala do incidente e do seu efeito aos clientes, fornecedores, público e outras partes interessadas, observando-se o estabelecido na Política de Porta Vozes de Suape.

6 Contenção, Erradicação, Recuperação e Notificação de Incidentes

6.1 Contenção

O primeiro passo será tentar impedir que o incidente se agrave, ou seja, contenha-o. No caso de um surto de vírus, isso pode implicar na desconexão das partes afetadas da rede; para um ataque de hackers, pode envolver a desativação de certos perfis ou portas no firewall ou até mesmo a desconexão completa da rede interna da Internet. As ações específicas a serem executadas dependerão das circunstâncias do incidente.

Nota: se for considerado provável que seja necessário coletar provas digitais que serão posteriormente usadas, devem ser tomadas precauções para garantir que tais evidências permaneçam admissíveis. Isso significa que os dados relevantes não devem ser alterados deliberadamente ou por acidente, por ex.: abrindo um laptop.

Recomenda-se que seja obtido um aconselhamento especializado neste momento - consulte os contatos no Anexo B.

Particularmente (mas não exclusivamente) se houver suspeita de crime no incidente, registros precisos devem ser mantidos das ações tomadas e as evidências coletadas de acordo com as diretrizes forenses. Os princípios destas diretrizes são os seguintes:

Princípio 1 – Não altere nenhum dado. Se alguma coisa for feita que resulte na alteração dos dados do sistema, isso afetará qualquer processo judicial subsequente.

Princípio 2 – Acesse somente os dados originais em circunstâncias excepcionais. Um especialista treinado usará ferramentas para fazer uma cópia de qualquer dado armazenado na memória, seja em um disco rígido, memória ou cartão SIM de um telefone. Toda a análise terá local certo na cópia, e a original nunca deverá ser tocada, a menos que em circunstâncias excepcionais (por ex. o tempo é essencial, e obter informações para evitar um novo crime é mais importante do que manter a evidência admissível).

Princípio 3 – Sempre mantenha a trajetória da auditoria do que foi feita. As ferramentas forenses farão isso automaticamente, mas isso também se aplica às primeiras pessoas em cena. Tirar fotografias e vídeos é incentivado desde que nada tenha sido tocado.

Princípio 4 – A pessoa responsável deve assegurar que as diretrizes sejam seguidas.

Antes da chegada de um especialista, as informações básicas devem ser coletadas.

Isso pode incluir:

- Fotografias ou vídeos de mensagens ou informações relevantes;
- Registros manuais escritos da cronologia do incidente;
- Documentos originais, incluindo registros de quem os encontrou, onde e quando;
- Detalhes de quaisquer testemunhas.

Uma vez coletadas, as evidências serão mantidas em um local seguro, onde não pode ser adulterado.

A evidência pode ser necessária:

- Para análise posterior sobre a causa do incidente;
- Como prova para processos judiciais criminais ou civis;
- Em apoio a qualquer negociação de compensação com fornecedores de software ou serviços.

Em seguida, uma ideia clara do que aconteceu precisa ser estabelecida. A extensão do incidente e as implicações devem ser averiguadas antes que qualquer tipo de ação de contenção.

Logs de auditoria podem ser examinados para determinar a sequência de eventos; deve-se tomar cuidado para que apenas cópias seguras de registros que não foram adulterados sejam usadas.

6.2 Erradicação

Ações para corrigir os danos causados pelo incidente (ex. exclusão de malware) devem passar pelo processo de gerenciamento de alterações (salvo uma mudança de emergência, se necessário). Essas ações devem ter como objetivo corrigir a causa atual e impedir que o incidente ocorra novamente. Quaisquer vulnerabilidades que tenham sido exploradas como parte do incidente devem ser identificadas.

Dependendo do tipo de incidente, a erradicação pode, às vezes, ser desnecessária.

6.3 Recuperação

Durante a fase de recuperação, os sistemas devem ser restaurados à sua condição anterior ao incidente, embora as ações necessárias devam ser realizadas para resolver quaisquer vulnerabilidades que foram exploradas como parte do incidente. Isso pode envolver atividades como a instalação de patches, alteração de senhas, proteção de servidores e alteração de procedimentos.

6.4 Notificação

A notificação de um incidente de segurança da informação e perda de dados resultante é um assunto delicado que deve ser tratado com cuidado e com total aprovação da Diretoria . A equipe decidirá, com base em pareceres jurídicos e de outros especialistas e com uma compreensão total do impacto do incidente, a notificação necessária a ser feita.

A empresa SUAPE sempre deve cumprir integralmente os requisitos legais e regulamentares aplicáveis em relação à notificação de incidentes e avaliará cuidadosamente quaisquer ofertas a serem feitas as partes que possam ser afetadas pelo incidente.

Os registros coletados como parte da resposta a incidentes podem ser exigidos para quaisquer investigações dos órgãos reguladores e SUAPE sempre deve cooperar integralmente com tais procedimentos.

7 Atividade Pós-Incidente

O líder da equipe decidirá, com base nas informações mais recentes, o ponto em que as atividades de resposta devem cessar e a equipe deve ser desativada. Observe que a recuperação e execução de planos podem continuar além desse ponto, mas sob um controle menos formal.

Essa decisão dependerá do julgamento do líder da equipe, mas deve basear-se nos seguintes critérios:

- A situação foi totalmente resolvida ou é razoavelmente estável;
- O ritmo de mudança da situação diminuiu a um ponto em que poucas decisões são necessárias;
- A resposta apropriada está bem encaminhada e os planos de recuperação estão progredindo;
- O grau de risco para o negócio diminuiu para um ponto aceitável;
- Responsabilidades legais e regulamentares imediatas foram cumpridas.

Se a recuperação do incidente estiver em andamento, o *Líder da Equipe* deve definir as próximas ações a serem tomadas. Estes podem incluir:

- Reuniões menos frequentes da equipe, por ex. semanalmente dependendo das circunstâncias;
- Informar todas as partes envolvidas de que a equipe permanece;
- Garantir que toda a documentação do incidente está certa;
- Solicitar que todos os funcionários não envolvidos em trabalhos futuros retornem às tarefas normais.

Todas as ações tomadas devem ser registradas.

Depois que a equipe for desativada, o *Líder da Equipe* apresentará um resumo a todos os membros, idealmente, dentro de 24 horas. Os registros relevantes do incidente serão examinados pela equipe para garantir que eles estejam completos e precisos.

Quaisquer comentários imediatos ou feedback da equipe serão registrados.

Uma revisão pós-incidente mais formal será realizada em um momento a ser decidido pela alta direção de acordo com a magnitude e a natureza do incidente.

ANEXO A –Contatos Internos de Resposta Inicial

A tabela a seguir deve ser usada para registrar contato inicial com membros da Equipe de Resposta ao Incidente:

Cargo/Área	Número do telefone	Data/Hora	Resultado (Contactado / Sem Resposta / Mensagem / Inacessível)
Líder do Time	Xxx xxx xxx		
Facilitador de equipe	Xxx xxx xxx		
Tecnologia da informação	Xxx xxx xxx		
Saúde e Segurança	Xxx xxx xxx		
Recursos Humanos	Xxx xxx xxx		
Compliance	Xxx xxx xxx		
Comunicações (RP e Relações com os Mídias)	Xxx xxx xxx		
Jurídico e Regulatório	Xxx xxx xxx		

ANEXO B – Contatos Externos Úteis

A tabela a seguir mostra os detalhes de contato de terceiros que podem ser úteis dependendo da natureza do incidente:

Organização	Contato	Número de Telefone	E-mail
Autoridade de Fiscalização de Proteção de Dados			
Consultoria de Proteção de dados			
Fornecedor de software de segurança			
Grupo de resposta a incidentes regionais			
Provedor de internet			
Companhia de seguros			
Consultores de Relações com a Mídia			
Grupo de representantes do cliente			
Associações			
Órgãos Reguladores			

ANEXO C – Agenda de Reunião da Equipe de Resposta a Incidentes

Recomenda-se que a seguinte agenda seja usada para reuniões da equipe de resposta a incidentes.

AGENDA

Participantes: Todos os membros da equipe de resposta a incidentes

Localização: Sala x

Frequência:

Presidente: Líder da Equipe

Minutos: Facilitador da Equipe

1. Ações da reunião anterior
2. Atualização do status do incidente
3. Decisões requeridas
4. Atribuição de Tarefas
5. Comunicações internas
6. Comunicações externas
7. Qualquer outra situação.

Data: