

**POLÍTICA DE SEGURANÇA
DA INFORMAÇÃO
DA SECRETARIA DE EDUCAÇÃO
DE PERNAMBUCO**

**PC03 – POLÍTICA DE RESPOSTA A INCIDENTES DE SEGURANÇA
DA INFORMAÇÃO**



Faça disso um hábito!

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
15/02/17	1.0	Versão elaborada e publicada	Equipe de Elaboração
31/07/18	2.0	Versão revisada	Equipe de Elaboração

SUMÁRIO

INTRODUÇÃO	4
OBJETIVO	4
ABRANGÊNCIA	4
DIRETRIZES DA RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	5

INTRODUÇÃO

O tratamento de incidentes envolvendo a segurança da informação é fundamental no combate a eventos que possam resultar em perda, dano ou acesso não autorizado às informações. Esse tratamento corresponde a medidas planejadas e organizadas para detecção, análise e reação em situações que levem a um rompimento na tríade que configura a segurança da informação: confidencialidade, integridade e disponibilidade.

Dentre as ações que podem gerar esse rompimento, é possível destacar: negação de serviço; código malicioso; vírus; acesso não autorizado ou uso inapropriado de contas ou sistemas; instalação ou uso de softwares não autorizados; perda de arquivos essenciais às atividades; roubo ou perda de equipamentos; dano acidental ou proposital a equipamentos de tecnologia; saída não liberada de dados; divulgação não permitida de informações confidenciais ou secretas; pichação de websites, entre outros.

As respostas aos incidentes de Segurança da Informação visam assegurar o restabelecimento do nível normal do ambiente tecnológico, através do direcionamento na utilização dos recursos e procedimentos fundamentais, no intuito de garantir uma resposta efetiva após o acontecimento de um sinistro. Esta atividade compreende planejamento, identificação, resposta e vistoria.

Planejamento - Esta atividade compreende identificar, prever e descrever situações de possíveis sinistros, bem como suas respectivas ações de mitigação, responsáveis, tempos e registros, de forma que, em situações reais, as atividades já estejam previamente mapeadas e as ações já prestabelecidas.

Identificação - Esta atividade compreende realizar ações para identificação e registro dos sinistros, através dos recursos de detecção na rede, no monitoramento dos servidores e recursos de tecnologia ou através de problemas reportados pelos usuários, podendo ser identificados alertas de segurança que configurem incidentes de segurança.

Resposta – Esta atividade compreende reações aos possíveis ataques realizados. A partir de uma detecção de um incidente de segurança, é importante controlá-lo antes que uma possível extensão comprometa outros recursos. Como exemplo, tem-se uma infecção por vírus em um computador e que, se não for controlado em tempo, pode comprometer outros computadores da rede. A estratégia de resposta ao incidente de segurança da informação a ser adotada deve ser baseada no tipo (ex: vírus, perda de arquivo, incêndio, etc.) e na criticidade do incidente (ex: impacta na imagem ou na operação da SEE-PE, compromete várias áreas, entre outros).

Vistoria - A vistoria consiste em ações realizadas após a ocorrência do incidente, como auditorias e análises de vulnerabilidade, com o objetivo de identificar e fechar brechas ainda existentes no ambiente tecnológico.

OBJETIVO

Definir os critérios para a gestão de incidentes de Segurança da Informação, possibilitando uma resposta rápida e eficaz ao Incidente, minimizando os prejuízos financeiros e de imagem da organização, preservando a reputação e a imagem da SEE-PE.

ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da SEE-PE, quais sejam: funcionários servidores ou comissionados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da SEE-PE. Todos esses colaboradores serão tratados nesta política como usuários.

DIRETRIZES DA RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. Diretrizes

- a) Uma Equipe de Resposta a Incidentes multidisciplinar deve ser criada, com a competência para planejar ações, definir papéis de atuação e responsabilidades para atuar em situações de sinistro, no monitoramento, nas detecções, nas respostas, nas ações de contramedidas e nas justificativas, relativas aos incidentes de segurança.
- b) Um catálogo dos recursos tecnológicos e sistêmicos existentes no parque da SEE-PE deve ser definido e disponibilizado para a Equipe de Resposta a Incidentes, possibilitando uma atuação efetiva na resposta aos incidentes que por ventura ocorram;
- c) A Equipe de Resposta a Incidentes deve se antecipar conforme histórico e experiência de mercado para planejar contramedidas em cada tipo de incidente, definindo criticidade, respostas (ações), responsabilidade, tempo mínimo de resposta, a quem e como reportar;
- d) O planejamento de contramedidas deve considerar a autorização prévia da alta gestão para incidentes que necessitem de respostas urgentes conforme sua relevância;
- e) A Equipe de Respostas a Incidentes deverá ser acionada quando forem identificados alertas de incidentes de segurança, no sentido de tomarem as providências devidas;
- f) Alguns indícios ou situações podem configurar um evento de segurança da informação e devem ser reportadas a equipe de resposta a incidentes, por exemplo, violação da disponibilidade, confidencialidade e integridade da informação; inconformidade das políticas e/ou procedimento; alterações de sistemas sem controle; funcionamento indevido de software ou hardware e violação de acesso lógico;
- g) Eventos de segurança da informação, reportados como suspeitos, devem ser analisados e validados rapidamente pela equipe de resposta a incidentes. Uma vez confirmado o incidente, uma análise mais aprofundada deverá ser realizada, para que contramedidas sejam implementadas, prioritariamente, conforme risco apresentado;
- h) Os usuários devem relatar qualquer tipo de eventos e fragilidades, que possam causar danos à segurança da Informação. A notificação do evento ou fragilidades por parte do usuário deverá ser registrada através da Central de Serviços.
- i) Após identificação e confirmação que o incidente se trata de um evento de Segurança da Informação, deve-se:
 - I. Preservar, na medida do possível, todas as evidências, para que seja possível identificar o problema e rastrear a causa e o causador;
 - II. Verificar se existem planos de ação em que o sinistro identificado esteja previsto, no intuito de seguir o planejamento;
 - III. Agir para que os serviços afetados sejam disponibilizados em seu estado normal de funcionamento no menor tempo possível;
 - IV. Utilizar todos os recursos necessários para a implementação de uma estratégia de reação, seja permanente ou provisória;
 - V. Utilizar atividades de recuperação e atualização, tais como: restauração de backups, instalação de patches, alteração de senhas e revisão da segurança do perímetro da rede;

- j) Após a contenção, resposta e análise, todos os componentes que causaram o incidente de segurança devem ser removidos e/ou evitados, por exemplo, a exclusão de um código malicioso ou bloqueio de contas de usuários violadas.
- k) Deve-se assegurar que as atividades envolvidas nas respostas aos incidentes sejam adequadamente registradas para futuras análises, servindo de banco de conhecimento para ações futuras de resposta em incidentes semelhantes;
- l) De acordo com o incidente, uma análise mais aprofundada deve ser conduzida para identificar a origem do incidente para que o tratamento das fragilidades e/ou não conformidade encontradas contribuam para a resolução do incidente;
- m) Periodicamente, a área de tecnologia da informação deve realizar uma análise no ambiente tecnológico com o objetivo de identificar possíveis vulnerabilidades e, de forma antecipada, eliminá-las;
- n) Após a identificação das possíveis vulnerabilidades, deve ser aberta uma ocorrência na Central de Serviços e comunicada às áreas responsáveis para as devidas tratativas. Após a resolução, deve ser encerrada a ocorrência e também registradas as ações realizadas.

2. Melhores Práticas

- a) Os usuários não devem realizar implantações ou atualizações de softwares que estejam fora das especificações ou escopo da infraestrutura atual do ambiente, pois isso pode acarretar em novos incidentes de segurança;
- b) Os usuários não devem tentar provar a fragilidade do ambiente tecnológico, salvo a equipe técnica responsável e com a devida autorização;
- c) A fim de garantir a continuidade dos serviços e atividades da SEE-PE, deve ser elaborado, implementado e testado um Plano de Recuperação de Desastre (PRD) e um Plano de Continuidade do Negócio (PCN) que envolvam os ambientes e processos críticos da SEE-PE.