POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DA PROCURADORIA-GERAL DO ESTADO DO CEARÁ

NR13 - Controle de Resposta a Incidente

Setembro/2022

CEARÁ
GOVERNO DO ESTADO
PROCURADORIA-GERAL DO ESTADO

CONTROLE DE VERSÕES

Versão	Data	Responsável	Alteração principal
00	07/11/2022	Coordenadoria de TI	Elaboração inicial

SUMÁRIO

1. INTRODUÇÃO

O controle de resposta a incidentes envolvendo a segurança da informação é fundamental no combate a sinistros que possam resultar em perdas, danos ou no acesso não autorizado às informações.

2. OBJETIVO

Definir padrões que norteiam o processo de aquisição, desenvolvimento e manutenção de sistemas de informação, visando assegurar a disponibilidade dos serviços suportados por estes sistemas.

3. ABRANGÊNCIA

Estes controles se aplicam a todos os usuários internos e externos que utilizam o recurso de TIC da PGE-CE.

4. CONTROLE DE RESPOSTA A INCIDENTES

4.1. A área de TI deverá definir uma equipe de Resposta a Incidentes relacionados a Segurança da Informação;

4.2. A equipe de resposta a incidentes deverá ser acionada quando forem identificadas ocorrências de incidente, devendo adotar as medidas necessárias para investigação e resolução do problema;

4.3. Eventos reportados como suspeitos devem ser analisados e validados, e, uma vez confirmado o incidente, o mesmo deverá passar por uma análise mais profunda e contramedidas devem ser implementadas com prioridade, conforme o risco apresentado;

4.4. Os usuários deverão reportar através da Central de Serviços sobre qualquer evento e fragilidade identificado, que possa causar danos à segurança;

4.5. Ao identificar e confirmar um incidente de segurança da informação, a equipe de resposta a incidentes deverá:

I. Preservar, dentro do possível, todas as evidências para que seja possível identificar, rastrear a causa e o causador;

II. Verificar a existência de plano de ação definido para o tipo de sinistro a fim de seguir seu planejamento;

III. Adotar as medidas necessárias para restabelecer o(s) serviço(s), de forma íntegra, no menor tempo possível;
IV. Implementar uma estratégia de reação, seja ela permanente ou temporária;
V. Utilizar os meios necessários para a recuperação e mitigação do risco (restauração de backup, instalação de patches, mudança de senhas, implementação de controles internos ou de borda, dentre outros);

4.6. Após solucionado o sinistro, restabelecido o(s) serviço(s) e identificado a causa do problema, a situação deverá ser documentada em relatório e armazenada em base de conhecimento para ações futuras em eventos semelhantes;

4.7. Periodicamente, a área de tecnologia da informação deverá realizar uma análise no ambiente com o objetivo de identificar fragilidades de forma antecipada. As vulnerabilidades identificadas deverão ser catalogadas e deverá registrarum chamado na Central de Serviços para a área responsável realizar as devidas correções;

4.8. Apenas a equipe técnica responsável pela infraestrutura tecnológica poderá realizar, com a devida autorização e de forma planejada, testes de vulnerabilidades no ambiente.

CEARÁ
GOVERNO DO ESTADO
PROCURADORIA-GERAL DO ESTADO