Política de Resposta Emergencial a Incidentes

Dezembro 2006

ÍNDICE

1. OBJETIVO

A Política de Resposta Emergencial a Incidentes provê a metodologia e documentação necessária para lidar com incidentes que envolvam a estrutura computacional e de comunicação da Rede Governamental. Quando um incidente de segurança ocorre, reações e decisões devem ser tomadas rapidamente. Estas medidas têm por objetivo garantir que a SEAD continue a cumprir sua missão e preservar a imagem do Estado.

2. ABRANGÊNCIA

Esta política aplica-se a todos os equipamentos servidores e estações de trabalho operados e mantidos pela Rede Governamental. Esta política também se aplica aos usuários finais, especificamente nos cuidados quanto a procedimentos de comunicação de incidentes e de testemunho.

3. VIGÊNCIA

Esta política passa a vigorar a partir da data de sua aprovação pela Secretaria da Administração, e será revisada anualmente. A antecipação do processo de revisão poderá ocorrer em face de necessidades na reestruturação dos processos administrativos/operacionais da Rede Governamental.

4. DOCUMENTAÇÃO COMPLEMENTAR

Documentação complementar a esta Política: Manual de Relato de Incidentes de Segurança

Outras políticas e documentos referenciados nesta política: Formulário de Relato de Incidentes de Segurança.

5. POLÍTICA

5.1 Estrutura de Resposta

5.1.1 Equipe

A implementação da Política de Resposta a Incidentes de Segurança Computacional depende da formalização da Equipe de Resposta a Incidentes de Segurança Computacional (ERISC). A ERISC tem por finalidade responder aos incidentes de segurança computacional que ameacem a missão da Rede Governamental e a sua imagem. A ERISC tem a autoridade necessária para implementar medidas emergenciais.

As atribuições básicas da ERISC, quando um incidente é detectado, são:

5.1.2.1 Responder a todo e qualquer incidente;

5.1.2.2 Minimizar os impactos de todo e qualquer incidente junto a estrutura da Rede Governamental;

5.1.2.3 Coletar informações e evidências para fundamentar ações e medidas necessárias;

5.1.3 Composição da ERISC

A ERISC da Rede Governamental será composta por:

5.1.3.1 Um líder que será o Administrador de Segurança de TI da Rede Governamental, e que indicará os outros membros da equipe.

5.1.3.2 Os membros convidados poderão ser funcionários da Rede Governamental, ou de outros órgãos do Estado, e excepcionalmente, funcionários de empresas que forneçam serviços de segurança à Rede Governamental.

5.1.3 Atribuições da ERISC

5.1.3.1 A ERISC desenvolve serviços junto a Rede Governamental de resposta a incidentes, desenvolvimento e análise de políticas de segurança, testes de conformidade e

treinamento de usuários.

5.1.3.2 É de responsabilidade da ERISC desenvolver os mecanismos de comunicação necessários para a condução das atividades de resposta à incidentes.

5.1.3.3 A comunicação deve ser a mais rápida possível, e os meios e procedimentos devem ser amplamente divulgados na Rede Governamental pela ERISC.

5.1.3.4 É de responsabilidade da ERISC o treinamento dos usuários para que possam colaborar com a resposta a incidentes.

5.1.3.5 Fluxo de Informação

Todo e qualquer incidente de segurança deverá ser comunicado ao Administrador de Segurança de T.I, para que ele, respeitando o disposto na seção 5.3, convoque a ERISC. Estes incidentes poderão ter sido documentados através do Formulário de Relato de Incidentes de Segurança, ou detectados através de ferramentas de segurança operadas pela SEAD, como sistemas *IDS, firewalls* e antivírus. Caberá ao líder da ERISC a comunicação de incidentes, quando julgar necessário, aos níveis mais altos de administração da Rede Governamental e ao restante dos funcionários.

5.2 Responsabilidades

5.2.1 Líder da ERISC

É responsável por gerenciar globalmente as atividades de resposta e recuperação de todos os incidentes. O líder determinará o grau de severidade de cada incidente, e determinará quais os membros da ERISC que estarão envolvidos nas atividades de resposta e recuperação. O líder da ERISC deverá reportar-se à SUTEC sobre investimentos que tornem-se necessários durante o processo de resposta e recuperação de incidentes e sobre necessidades de apoio de outras áreas administrativas da Rede Governamental.

5.2.2 Membros da ERISC

São profissionais treinados em Segurança Computacional, oriundos de diversas áreas dos órgãos/entidades participantes, que têm a atribuição básica de executar as medidas emergenciais de resposta e recuperação de incidentes, e/ou profissionais convidados pelo líder da ERISC, provenientes de outras áreas ou empresas, que possuam domínio sobre alguma área de conhecimento necessária para executar as medidas emergenciais de resposta e recuperação de incidentes.

5.2.3 Grau de Severidade de Incidentes

Alguns incidentes de segurança, como a ocorrência isolada de *software* malicioso (vírus de computador), são facilmente endereçados por procedimentos já definidos em outras políticas cujo modelo já está implementado na SEAD e foi disponibilizado para os demais órgãos/entidades. Este tipo de incidente não justifica a convocação de toda a equipe da ERISC. Abaixo, os critérios usados para classificar a severidade de incidentes de segurança no âmbito da Rede Governamental, e que grau de severidade justifica a utilização da Política de Resposta a Incidentes de Segurança Computacional, no caso, 3, 4 e 5.

5.2.4 Incidentes envolvendo ativos de rede / ativos computacionais

5.2.4.1 Grau de Severidade Nível 1

Interferência não intencional em ativos de rede / ativos computacionais.

5.2.4.2 Grau de Severidade Nível 2

Desligamento não intencional de ativos de rede / ativos computacionais.

5.2.4.3 Grau de Severidade Nível 3

Desligamento / interferência intencional em ativos de rede / ativos computacionais.

5.2.4.4 Grau de Severidade Nível 4

Furto de ativos de rede / ativos computacionais.

5.2.4.5 Grau de Severidade Nível 5

Danificação / destruição de ativos de rede / ativos computacionais.

5.2.5 Incidentes envolvendo conexões WAN – Internet, Rede Governamental

5.2.5.1 Grau de Severidade Nível 1

Pequeno número de sondagens (*probes*) ou varreduras (*scans*) detectados em sistemas internos; infecções isoladas de vírus conhecidos, facilmente removido pelo *software* antivírus em uso na SEAD.

5.2.5.2 Grau de Severidade Nível 2

Pequeno número de sondagens (*probes*) ou varreduras (*scans*) detectados em sistemas externos; possíveis cenários em que os sistemas sobre varredura possam estar vulneráveis.

5.2.5.3 Grau de Severidade Nível 3

Grande número de sondagens ou varreduras detectados em sistemas internos e/ou externos; ataques baseados em tentativa de penetração ou DoS (Negação de Serviço – *Denial of Service*), sem impacto nas operações da Rede Governamental; grande ocorrência de vírus conhecido e facilmente removido pelo *software* antivírus em uso no núcleo da Rede Governamental; ocorrências isoladas de novo vírus de computador não removível pelo *software* antivírus em uso no núcleo da Rede Governamental.

5.2.5.4 Grau de Severidade Nível 4

Tentativas de penetração ou ataques DoS com impacto limitado nas operações; grande ocorrência de novo vírus de computador não removível pelo *software* antivírus em uso no núcleo da Rede Governamental; pequeno risco de não cumprimento da missão e de danos à imagem da Rede Governamental.

5.2.5.5 Grau de Severidade Nível 5

Penetração ou ataque DoS bem sucedido com impactos significativos na operação; risco significativo de não cumprimento da missão e de danos à imagem da Rede Governamental.

5.2.6 Incidentes envolvendo pessoal

5.3.1.1 Grau de Severidade Nível 1

Atuar como vetor não intencional de código malicioso.

5.3.1.2 Grau de Severidade Nível 2

Enviar informações internas e/ou confidenciais para fora da Rede Governamental, vítima de engenharia social.

5.3.1.3 Grau de Severidade Nível 3

Atuar como vetor intencional de código malicioso / enviar informações internas e/ou confidenciais para fora da Rede Governamental intencionalmente.

5.3.1.4 Grau de Severidade Nível 4

Participar de furto, danificação ou interferência em ativos de rede / ativos computacionais.

5.3.1.5 Grau de Severidade Nível 5

Participar de ataques envolvendo tentativas de penetração, ataques DoS, entre outros contra sistemas da Rede Governamental ou contra sistemas de terceiros através dos recursos da Rede Governamental.

6. PROPRIEDADE

6.1 Este material é de propriedade do Governo do Estado do Ceará, e mantido pelo Administrador de Segurança de T.I. da Rede Governamental.

6.2 É proibida a reprodução total ou parcial e distribuição sem a autorização prévia do Administrador de Segurança de T.I da Rede Governamental.

7. CONCORDÂNCIA

Quem violar esta política estará sujeito a ações disciplinares, que podem incluir processos administrativos, criminais e cíveis e a aplicação das penalidades previstas em lei.