POLÍTICA DE CLASSIFICAÇÃO DAS INFORMAÇÕES E SISTEMAS GOVERNAMENTAIS

Dezembro de 2006

Índice

1 Objetivo

O propósito deste documento é ser um guia para a determinação do nível de segurança necessário para cada informação ou sistema governamental(sistema corporativo, redes locais e serviços da rede governamental). Os responsáveis pelos sistemas devem usar este guia para determinar o nível de segurança adequado exigido pelas redes locais, sistemas corporativos e serviços da rede sob sua responsabilidade.

2 Designações dos níveis de Segurança

Os esforços de classificação de informações são baseados na sensibilidade da informação contida em sistemas governamentais e na criticidade operacional de disponibilidade da capacidade de processamento dos sistemas corporativos, redes locais e serviços da rede governamental. Designações dos níveis de segurança são usadas para definir as exigências destes esforços de segurança.

3 Introdução aos Níveis de Segurança

A designação do nível de segurança, dentro do Programa de Segurança de Redes locais, sistemas corporativos e serviços da rede, é baseada na:

A. Sensibilidade da informação; ou seja, na necessidade de proteção da informação contra exposição não autorizada, fraude, roubo ou abuso;

B. Criticidade Operacional da Disponibilidade de Processamento da Informação; ou seja, as conseqüências causadas pela interrupção das capacidades de processamento de informações.

Existem quatro níveis de designação de segurança para sensibilidade da informação e quatro níveis para criticidade operacional. O responsável pelo sistema deve considerar a segurança para cada sistema sob estes dois pontos de vista, e depois escolher a taxa mais elevada para o nível de segurança do sistema como um todo.

Um sistema de informação deve ser compartimentado, pois geralmente conjuntos de informações ou processos são mais sensíveis do que outros dentro de um mesmo sistema. O responsável pelo sistema deve designar o nível mais alto de qualquer conjunto de informações ou Processos dentro do sistema como a designação final do nível de segurança como um todo. Esta prática deve suportar a Confidencialidade, Integridade, e Disponibilidade necessárias para tais sistemas como descrito abaixo:

- **Confidencialidade** – O sistema contém informação que exige proteção contra exposição não autorizada.

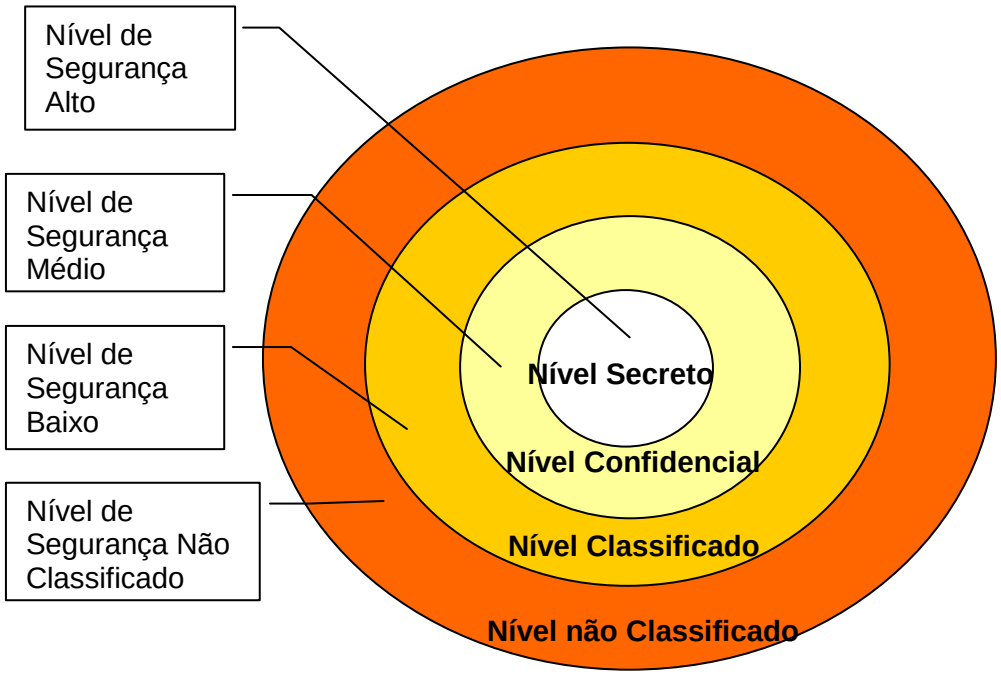
- **Integridade** - O sistema contém informação que deve ser protegida contra modificação não autorizada, intencional ou não.
- **Disponibilidade** - O sistema contém informação ou fornece serviços que devem estar disponíveis o maior tempo possível baseado nas exigências da missão ou para evitar perdas substanciais.

Os profissionais responsáveis por Redes locais, sistemas corporativos e serviços da rede devem certificar-se que as informações tratadas sejam acessadas somente por usuários autorizados que utilizem totalmente as exigências das salvaguardas do nível de segurança do sistema. Os Responsáveis por Redes locais, sistemas corporativos e serviços da rede devem tomar cuidados especiais quando especificarem o nível de segurança exigido para as redes locais, sistemas corporativos e serviços da rede, que utilizam serviços terceirizados de desenvolvimento do sistema e pessoal de suporte responsável pela manutenção dos sistemas. Ao especificarem o nível de segurança, os responsáveis por Redes locais, sistemas corporativos e serviços da rede deverão habilitar todos os registros possíveis de auditoria para que estes sejam auditados sempre que necessário.

A designação do nível de segurança de uma determinada classificação constitui a pilastra que vai possibilitar determinar as salvaguardas mínimas necessárias para proteger informações sensíveis e garantir a continuidade operacional crítica da capacidade de processamento das informações.

4 Classificação das Informações

As informações de propriedade do Governo do Estado do Ceará, mantidas nos sistemas corporativos governamentais devem ser classificadas de acordo com os níveis de segurança apresentados abaixo:



4.1 Níveis de Segurança da Informação

Os esforços de segurança de TI são baseados na sensibilidade de dados contidos nos sistemas governamentais, sejam as redes locais, os sistemas corporativos ou os serviços oferecidos pela rede governamental e na disponibilidade de processamento destes sistemas governamentais. Designações de nível de segurança são usadas para definir exigências destes esforços de segurança.

4.2 Categoria de Informação

Os órgãos ou entidades da rede pública estadual tratam diversas informações, que vão desde informações sensíveis para o Governo até informações necessárias para o seu desenvolvimento como entidades. As informações devem ser avaliadas de acordo com o critério de seleção descrito na tabela abaixo e devem ser associadas com o nível mínimo de segurança exigido.

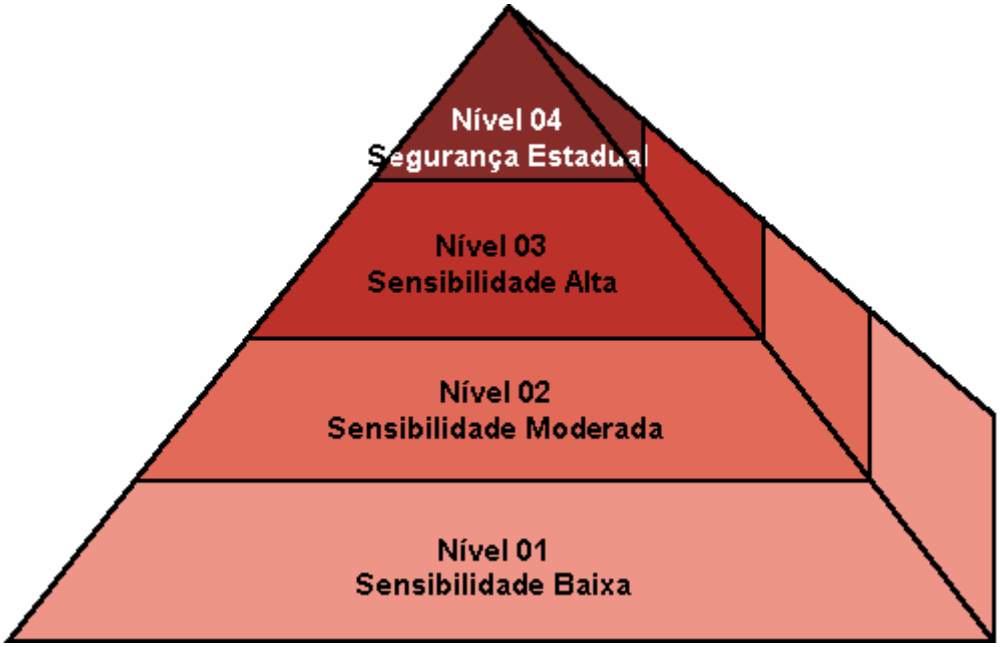
Categoria	Explicação e exemplos	Nível de Segurança		
		B	**M**	**A**
(1) Informação Pública	Qualquer informação que seja declarada para consumo dos órgão ou entidade da rede pública estaduais e entidades públicas por autoridades oficiais, tais como informações do diário Oficial. Também inclui Informações colocadas na Internet.	**B**		
(2) Informação sobre indivíduos	Informação de pessoal, médica, e dados similares. Inclui todas as informações cobertas pela lei de privacidade tais como: salários, identificadores de usuários (ID's), perfil pessoal (endereço de casa e número telefônico), histórico médico, histórico do empregado e histórico de investigação (criminal/prisão).		**M**	
(3) Informações Financeiras, orçamentárias, comerciais e proprietárias.	Informações e aplicações financeiras, comerciais recebidas em confidência, ou segredos comerciais (proprietário, informação de ordem de contratos, informação sensível sobre patentes, e informações protegidas legalmente). Informação sobre pagamento, tomada de decisão automatizada, aquisições, inventario, outras financeiras relacionadas a sistemas, e operação do lugar e despesas com segurança.		**M**	
(4) Administração interna	Informação da administração interna do órgão ou entidade da rede pública estadual, tais como regras pessoais, posições de compras e negociação, e informações sobre ações judiciais.		**M**	

		Nível de Segurança		
(5) Informações de outros órgão ou entidade da rede pública estaduals e entidades	A proteção da Informação que é exigida por estatuto, ou que é recebida de um outro órgão ou entidade da rede pública estadual Federal e exige aprovação pelo órgão ou entidade da rede pública estadual emissor para liberação.		M	
(6) Tecnologia nova ou controlada cientificamente	Informação relacionada à nova tecnologia, Informação cientifica que é proibida de exposição para certos Governos estrangeiros ou que podem exigir uma licença de exportação do departamento de Estado.		M	
(8) Informação Operacional	Informação que exige proteção durante operações; geralmente informação crítica ao tempo.		M	
(9) Informação sobre gerenciamento de configuração de sistemas	Qualquer informação pertencente a operações da rede ou sistema computacional interno, tais como endereços de dispositivos de rede; esquemas de endereçamento de sistemas e protocolos implementados no órgão ou entidade da rede pública estadual; protocolos de informação de gerenciamento de rede, string de comunidade SNMP, pacotes de informação da rede, etc.; senhas de dispositivos e sistemas; informação de configuração de dispositivos e sistemas.		M	
(10) Informação de Investigação, a segurança estadual	Informação de Investigação por lei para propósitos de coerção; Informação relacionada à Inteligência que não pode ser classificada, mas está sujeita a confidencialidade e controles extras de segurança, tais como planos de segurança, de contingência, de operações emergenciais, relatórios de incidentes, relatórios de investigações, de verificação e certificação de riscos.			A
(11) Informação de missão crítica	Informação qualificada como crítica para a missão do órgão ou entidade da rede pública estadual ou para o Estado, incluindo informações de estatísticas vitais para operações de emergência.			A
(12) Informação vital	Informação crítica para a vida útil de sistemas tais como, informações onde a incerteza, perda, ou alterações da informação pode resultar em perda de vida.			A
(13) Patrimônios dos cidadãos	Informações sobre patrimônios dos cidadãos tais como veículos, registro de imóveis, poupança, ações nominais, dentro outros.			A

Legenda: B-Baixo, M- Média, A- Alta.

5 Níveis de Sensibilidade para Informações

Níveis de Sensibilidade classificam informações de acordo com o tipo de informação armazenada na base de dados e exigência de leis especificas governando a proteção ou exposição da informação armazenada.



A designação de nível 01 é usada para informações com o menor grau de sensibilidade e a designação de nível 04 é usada para informações com a maior sensibilidade relativa.

5.1 Nível 01: Sensibilidade Baixa

Esta categoria classifica informações que exigem proteção mínima. Ameaças para estas informações são consideradas mínimas, e somente as precauções mínimas do ambiente do usuário precisam ser tomadas para proteger a informação. Alteração não intencional ou destruição são as principais preocupações para esta classe de informação.

Esta categoria é constituída por informações de registros submetidos à lei de privacidade, virtualmente de domínio público, tais como arquivos de informações limitadas sobre funcionários, de forma que sua exposição não autorizada não afete o funcionário.

5.2 Nível 02: Sensibilidade Moderada

Esta categoria classifica informações que possuem alguma importância para o órgão ou entidade da rede pública estadual e entidade da administração estadual ou para o Estado e que devem ser protegidas contra atos destrutivos e maliciosos. Como estes tipos de informações

são geralmente usados para propósitos analíticos, problemas de exposição não são tão significantes.

Esta categoria inclui:

a. Informação gerencial sobre carga de trabalho, nomeação, e informações similares, geralmente em forma estatística, usadas para gerar relatórios que refletem o status de algum órgão ou entidade da rede pública estadual. Acessos para estas informações precisam ser restritos somente para uma classe de usuários limitada. As informações são protegidas por causa do seu valor para o Estado ou algum órgão ou entidade da rede pública estadual entidade da administração estadual.

b. Informações de domínio não público sujeitas à lei de privacidade, que sua exposição não autorizada poderia causar problemas indeterminados para um cidadão.

c. Informações de e-mails e documentos que devem ser protegidos contra alteração ou exposição não autorizada. Estes tipos de informações incluem todas as correspondências, memorandos, e outros documentos que seu lançamento ou distribuição para fora do governo estadual precise ser controlado.

5.3 Nível 03: Sensibilidade Alta

Esta categoria classifica as informações mais sensíveis para o Estado. A informação nesta categoria exige o maior nível de proteção, salvaguarda e ambiente de usuário mais restrito.

Esta categoria inclui:

a. Informação sobre pagamentos e informação usada para autorizar ou fazer pagamentos para pessoas ou organizações. Estas informações são geralmente armazenadas em redes locais, sistemas corporativos e serviços da rede em produção, e constituem informações privilegiadas, tais como a folha de pagamento.

b. Informação Proprietária que possui valor para o Estado e que deve ser protegida de exposição não autorizada.

c. Informações em e-mails e documentos considerados altamente sensíveis para o Estado e algum órgão ou entidade da rede pública estadual, cuja informação deva ser protegida de alteração não autorizada e/ou exposição antes do tempo, tais como licitações.

d. Informações de registros de redes locais, sistemas corporativos e serviços da rede submetidos à lei de Privacidade, em que a exposição não autorizada constitua uma invasão de privacidade pessoal trazendo conseqüências para um cidadão em termos financeiros, médicos, psicológicos, ou posição social.

5.4 Nível 04: Sensibilidade Muito Alta

Esta categoria classifica todas as informações classificadas como segurança estadual ou nacional, onde a falta ou uso inadequado desta informação pode afetar a segurança estadual.

6 Classificação de Redes Locais, Sistemas Corporativos e Serviços da Rede Governamental

Se a classificação de um sistema governamental (rede local, sistema corporativo ou serviço da rede governamental) for classificado baseado no tipo de informação governamental que ele(a) manipula, tal sistema deve encaixar-se em uma das categorias abaixo:

Tipo de Informação	Descrição
Alta Confidencialidade	Sistemas que manipulam informações governamentais, cujo acesso indevido pode trazer: prejuízo financeiro para o Estado ou terceiros, impactos negativos à imagem do Estado, danos a certos indivíduos em benefícios de outros e insegurança para alguns indivíduos.
Alta Integridade	Sistemas que manipulam informações governamentais cuja manipulação indevida pode acarretar em danos ao Estado ou a indivíduos que confiam em tais sistemas tais como: resultados de aprovações, meteorológicas, indicadores econômicos e sociais, informações privadas.
Alta disponibilidade	Serviços, tais como comunicação de rede, Internet, correio eletrônico, banco de dados de sistemas críticos, cuja paralisação pode trazer danos ao Estado como perda de arrecadação, de negócios, dentre outros.

6.1 Níveis de Criticidade para Redes Locais, Sistemas Corporativos e Serviços da rede

Níveis de criticidade classificam redes locais, sistemas corporativos e serviços da rede de acordo com o nível de informações que eles suportam e sua disponibilidade de processamento para o Estado. Uma designação de nível 01 é usada por uma rede local, sistema corporativo ou serviço da rede contendo processamento de informação de menor sensibilidade relativa para o Estado ou que requeira baixa disponibilidade. Uma designação de nível 04 é usada por uma rede local, sistema corporativo e serviço da rede com processamento de informação com a mais alta sensibilidade relativa ou que requeira alta disponibilidade para o Estado.

6.2 Nível 01: Criticidade Baixa

Esta categoria classifica redes locais, sistemas corporativos e serviços da rede com capacidade de processamento de informação que exigem proteção mínima. No caso de alteração ou falha, estas redes locais, sistemas corporativos e serviços da rede devem afetar minimamente o Estado ou o órgão/entidade da rede pública estadual relacionada, podendo ficar indisponível e ainda assim representar um impacto mínimo de tempo, custo e pessoal. Esta categoria também inclui redes locais, sistemas corporativos e serviços da rede que geram, armazenam, processam, transferem, ou comunicam informações que são consideradas de baixa ou nenhuma sensibilidade (Nível 01 de Sensibilidade).

Caso uma ameaça a esta categoria de informações se realize, ocasionará um Impacto notável na missão do órgão/entidade da rede pública estadual ou entidade governamental, funções, imagem, ou reputação. Uma brecha deste nível de segurança pode gerar um resultado negativo, causando danos, exigindo reparos a um patrimônio ou recurso.

6.3 Nível 02: Criticidade Moderada

Esta categoria classifica redes locais, sistemas corporativos e serviços da rede com disponibilidade de processamento de média criticidade e sensibilidade de informações que são considerados importantes, mas não criticas para o gerenciamento interno do Estado como um todo. Esta categoria inclui:

a. Redes locais, sistemas corporativos e serviços da rede em que falhas no seu funcionamento por um longo período de tempo não devem causar um impacto ao Estado ou aos órgãos e entidades da administração pública estadual que elas suportam.

b. Redes locais, sistemas corporativos e serviços da rede que geram, armazenam, processam, transferem, ou comunicam informações consideradas de sensibilidade moderada (Nível 02 de Sensibilidade).

Caso uma ameaça a esta categoria de informações se realize, ocasionará uma falha grave para missão do órgão ou entidade da rede pública estadual, funções, imagem, ou reputação que deve colocar o órgão ou entidade da rede pública estadual em desvantagem significativa ou poderia resultar em danos maiores, exigindo reparos extensivos para patrimônios ou recursos.

6.4 Nível 03: Criticidade Alta

Esta categoria classifica redes locais, sistemas corporativos e serviços da rede com disponibilidade crítica de processamento e sensibilidade de informação considerada sensível para o Estado ou órgãos e entidades da administração pública estadual que elas suportam.

Esta categoria inclui:

a. Redes locais, sistemas corporativos e serviços da rede em que falhas no seu funcionamento por um certo período de tempo causem um impacto grave para o Estado ou para órgão e entidades da administração pública estadual que elas suportam.

b. Redes locais, sistemas corporativos e serviços da rede que tratam informações que são consideradas de alta potencialidade para fraude, destruição, ou abuso.

c. Redes locais, sistemas corporativos e serviços da rede que geram, armazenam, processam, transferem, ou comunicam informações consideradas de sensibilidade alta (Nível 03 de sensibilidade).

Caso uma ameaça a esta categoria de informações se realize, ocasionará uma perda total da capacidade de desempenho da missão do órgão ou entidade da administração pública estadual por um longo período de tempo, ou resultar em perda dos principais patrimônios e recursos, podendo chegar a colocar vidas humanas em risco.

6.5 Nível 04: Criticidade Muito Alta

Esta categoria classifica todos as redes locais, sistemas corporativos e serviços da rede com disponibilidade de processamento crítico e sensibilidade de informação considerada sensível para o bem do Estado e da população.

7 Responsabilidades

7.1 Administrador de Segurança Governamental

a. Garantir que as designações de Nível de Segurança (4, 3, 2, ou 1) sejam associadas para todos os sistemas corporativos e serviços da rede governamental e infra-estrutura respectiva do sistema.

b. Coordenar o processo de classificação de sensibilidade das informações;

c. Coordenar o processo de classificação de criticidade dos sistemas governamentais.

7.2 Auditor de Segurança

a. Auditar as determinações dos níveis de segurança das informações governamentais baseado na sensibilidade de tais informações;

b. Auditar as associações de criticidade dos serviços, dos sistemas corporativos, redes locais e serviços da rede governamental.

7.3 Administrador de Rede, sistema ou serviço

a. Determinação da designação do Nível de Segurança para os sistemas corporativos e serviços da rede governamental sob sua gerência e bases de dados associadas.

b. Notificação do Auditor de Segurança de TI Estadual e usuários dos níveis de segurança exigidos pela informação e capacidade de processamento da informação dos sistemas corporativos e serviços da rede governamental sob sua gerência.

8 Política

- Todas informações do Estado do Ceará tratadas por órgãos/entidades da rede pública estadual devem ser classificadas quanto a sensibilidade de tais informações de acordo com a planilha de classificação de sistemas e serviços em anexo neste documento;
- Todos os sistemas corporativos, serviços da rede governamental, de dominio público devem ser classificados quanto a criticidade de suas operações de acordo com a planilha de classificação de sistemas e serviços em anexo neste documento.

ANEXOS

ANEXO A - PLANILHA DE CLASSIFICAÇÃO DE SISTEMAS E SERVIÇOS

Nome do Sistema Governamental:			
Tipo do Sistema:	☐ Rede local - ☐ Sistema Corporativo - ☐ Serviço da Rede		
Órgão ou entidade responsável:			
Profissional responsável pelo sistema:			
Missão do sistema / serviço			
Objetivos do sistema / serviço			
Classificação das informações			
Informação manipulada	Nível de classificação	Justificativa	
Nível de classificação do sistema			
Sensibilidade		Criticidade	
Observações:			

Aprovação

Auditor de Segurança Estadual	Administrador de Segurança de TI Estadual
Responsável pelo Sistema	Responsável pelo órgão

ANEXO B - ACORDO PARA SALVAGUARDAR INFORMAÇÕES SENSÍVEIS

Governo do Estado do Ceará

Eu, _____, reconheço que tenho acesso a informações sensíveis mantidas pelo governo do Estado do Ceará na intranet da rede governamental.

Eu aceito que obterei, usarei ou revelarei tais informações somente na conexão da execução das obrigações da minha posição para propósitos autorizados.

Eu aceito manter a confidencialidade da informação em conformidade com as leis estaduais.

Eu entendo que falhas na salvaguarda de informações sensíveis podem resultar em imposição de penalidades, incluindo afastamento do cargo, demissão do Estado até processos judiciais.

Se eu observo quaisquer condições que causariam a exposição da informação de qualquer maneira, eu entendo que é minha responsabilidade tomar ações para salvaguardar o governo do Estado do Ceará e informar o incidente para meu superior.

Eu aceito que minha obrigação para salvaguardar a confidencialidade dos dados do governo deve sobreviver o termino do meu emprego ou contrato com o governo do Estado do Ceará

RECONHECIMENTO E ASSINATURA:

_____

_____

(Empregado/contratado) (Data)

_____

_____

(Supervisor/Assinatura) (Data)