Política de Sistemas Corporativos e Serviços da Rede Governamental

Dezembro de 2006

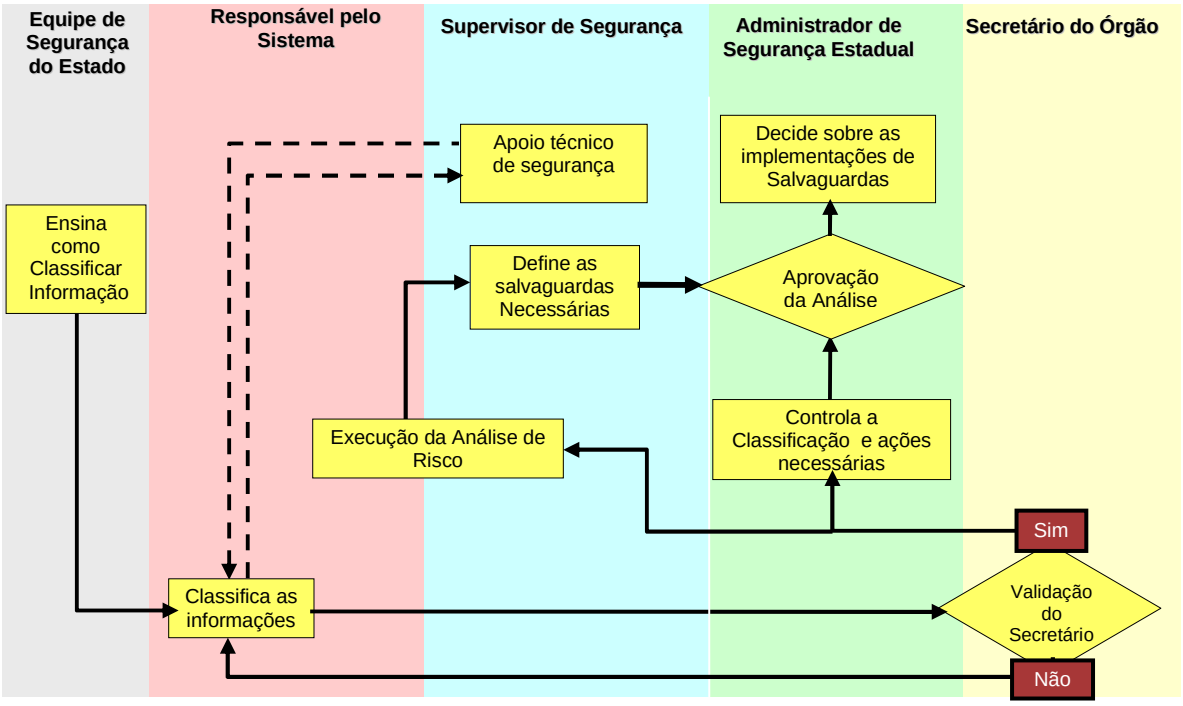
Índice

1 Objetivo

Esta política estabelece normas, procedimentos, e responsabilidades para a implementação e administração da segurança de sistemas corporativos, serviços da Rede Governamental e redes locais doravante chamados sistemas governamentais.

Para ajudar na implementação desta política, este documento contém alguns guias e exemplos dos processos necessários para o desenvolvimento do programa.

Fluxograma da Política



2 Abrangência

2.1 A quem se destina

Esta política aplica-se a todos os funcionários, incluindo contratados, dos órgãos/entidades da administração pública estadual direta ou indireta e outras entidades de interesse do governo do Estado do Ceará. Aplica-se a todos os sistemas governamentais, infra-estrutura de sistemas corporativos e serviços, incluindo todos os itens que compõem a Rede Governamental.

3 Considerações Gerais

O Governo do Estado do Ceará implementará uma política de segurança de sistemas governamentais para garantir que cada Sistema Governamental, contendo informações necessárias ao funcionamento global do Estado, tenha um nível de segurança comensurável com o risco e a magnitude do dano resultante de perda, uso indevido, exposição ou modificação da informação tratada pelo sistema.

a. Cada Sistema Governamental deve ter as salvaguardas técnicas, pessoais, administrativas e ambientais adequadas;

b. A segurança do Sistema Governamental deve ser baseada em custo efetivo;

c. Um Sistema Governamental que suporta funções críticas do Estado deve ter um plano de contingência ou recuperação de desastre para fornecer continuidade de operação;

d. Profissionais de tecnologia de informação dos órgãos/entidades da administração pública estadual devem ser formalmente alocados para administrar os sistemas governamentais sob sua responsabilidade de acordo com as recomendações deste programa.

4 Exigências de Segurança para sistemas governamentais

As exigências de segurança aplicam-se para todos os sistemas governamentais e infra-estrutura de Tecnologia da Informação sobre a responsabilidade direta ou indireta do Estado, incluindo aqueles que são operados pelos órgãos/entidades da administração pública estadual e por empresas terceirizadas.

Quanto mais alta a designação do Nível de Segurança de um Sistema Governamental, mais restritas são suas exigências de segurança. Sistemas governamentais com designação de Nível de Segurança mais baixo geralmente exigem somente precauções de segurança comuns; isto é, proteção por salvaguardas que são consideradas como boa prática de administração de sistemas. Em todos os casos, as exigências mínimas de segurança de sistemas governamentais devem ser iguais ou maiores do que o nível mais alto de criticidade do Sistema Governamental ou serviço da Rede Governamental.

4.1 Exigências dos Níveis de Segurança

- **Exigência do Nível 01**

  Os controles exigidos para salvaguardar adequadamente um Sistema Governamental com criticidade classificada com nível 01 são aqueles que

normalmente deveriam ser considerados como boa prática de administração e gerenciamento de sistemas, incluindo:

a. Um programa de treinamento e conscientização da segurança do Sistema Governamental;

b. Controles de acesso Físico;

c. Um conjunto completo de documentação do Sistema Governamental.

- **Exigências do Nível 02**

  Os controles exigidos para salvaguardar adequadamente um Sistema Governamental com criticidade classificada com nível 02 constituem todas as exigências para o nível 01, com a adição das seguintes exigências:

  a. Um Programa de Gerenciamento de Riscos detalhado.

  b. Um Plano de Segurança para cada Sistema Governamental.

  c. Uma lista controlada de usuários autorizados.

  d. Procedimentos de revisão e certificação de Segurança.

  e. Registro de investigações exigido para todos os funcionários e pessoal contratado.

  f. Um Plano de Contingência formal.

  g. Uma Análise de Risco formal.

  h. Uma Auditoria Automatizada.

  i. Procedimentos de controle de acesso autorizados.

  j. Um programa de emergência de energia.

- **Exigências do Nível 03**

  Os controles exigidos para salvaguardar um Sistema Governamental com criticidade classificada com nível 03 adequadamente contemplam todas as exigências para os níveis 1 e 2, com a adição das exigências de inventario de *hardware* e *software*.

- **Exigências do Nível 04**

  Os controles exigidos para salvaguardar adequadamente um Sistema Governamental nível 04, incluem todas as exigências para os níveis 1, 2, e 3, com adição de procedimentos de segurança especificados pelos órgãos/entidades da administração pública estadual que fornecem a informação ou sistemas classificados.

5 Administração da Segurança dos Sistemas governamentais

As exigências para a administração do Programa de Segurança de sistemas governamentais estão relacionadas com:

- A coordenação das atividades de segurança de tais sistemas e serviços;
- Informação do status dos programas para o Administrador de Segurança de TI Estadual;
- Coordenação dos procedimentos para relatar brechas de segurança;
- Condução de investigações periódicas de segurança.

5.1 Responsabilidades

- **Administrador de Segurança de TI Estadual**

  a. Coordenar atividades de treinamento em recursos de segurança da informação para responsáveis e usuários de sistemas governamentais.

  b. Garantir que os planos de segurança sejam desenvolvidos, revisados, e implementados quando necessário.

  c. Desenvolver e implementar os procedimentos de relato de brechas de segurança.

  d. Garantir que Políticas de Segurança adicionais sejam desenvolvidas e implementadas como exigida pela informação, pessoal e infra-estrutura do Sistema Governamental.

  e. Garantir que todos os Responsáveis por sistemas governamentais e usuários da infra-estrutura de TI sejam conhecedores do nível de segurança do serviço oferecido (i.e., designação de segurança).

  f. Manter um inventário dos sistemas governamentais, que foram designados com um Nível de Segurança 04 ou 03. A manutenção do inventário dos níveis 2 e 1 são opcionais. Sistemas nível 02 que exigem Planos de Segurança de sistemas governamentais devem ser inventariados.

- **Responsabilidades do Supervisor de Segurança de TI Estadual**

  O Supervisor de Segurança de TI Estadual é responsável pela avaliação e fornecimento de informação sobre o programa da Rede Governamental e pela comunicação do Programa de Segurança de sistemas governamentais, das exigências e preocupações do Estado do Ceará, sendo responsável por:

  a. Relatar informação sobre brechas de segurança dos recursos.

  b. Fornecer avisos e assistência aos profissionais responsáveis por sistemas governamentais, administradores de sistemas, e outros

membros da rede estadual preocupados com a segurança destes sistemas e serviços.

c. Colaborar com os responsáveis por sistemas governamentais para a criação do plano de segurança de cada sistema, fornecendo todos os subsídios técnicos necessários.

d. Certificar o plano de segurança desenvolvido.

e. Especificar, implementar, e revisar procedimentos usados para proteger a Integridade da infra-estrutura de TI e sistemas operacionais, incluindo o desenvolvimento da análise de risco e a determinação de exigências mínimas de segurança e salvaguardas.

f. Garantir que a segurança necessária da infra-estrutura de TI está sendo identificada, as brechas monitoradas e as ações corretivas estão sendo tomadas.

g. Realizar o inventário dos sistemas governamentais, que foram designados com um Nível de Segurança 04 ou 03. A manutenção do inventário dos níveis 2 e 1 são opcionais. Sistemas nível 02 que exigem Planos de Segurança de sistemas governamentais devem ser inventariados.

- **Responsabilidades do Administrador do Sistema Governamental**

O responsável de cada Sistema Governamental deve desenvolver, implementar, manter, e revisar o Programa de Segurança de sistemas governamentais referente ao sistema/ serviço sob sua responsabilidade, sendo também responsável por:

a. Integrar o programa de Segurança de sistemas governamentais do órgão/ entidade da rede estadual com outros programas e exigências de segurança;

b. Fornecer subsídios sobre o programa de Segurança de Sistemas governamentais para o Supervisor de Segurança de TI Estadual da Rede Governamental.

c. Garantir que as exigências de segurança da informação e a capacidade de processamento da informação dos sistemas governamentais sob sua gerência estejam de acordo com as exigências desta política.

d. Garantir que os sistemas governamentais sob sua gerência e bases de dados respectivas, somente sejam executados nas instalações e infra-estrutura com a designação do Nível de Segurança igual ou maior do que as designações dos sistemas governamentais.

e. Periodicamente revisar e verificar se todos os usuários dos sistemas governamentais estão autorizados e usando as salvaguardas de segurança exigidas.

5.2 Investigação de Segurança

É exigido que o Supervisor de Segurança de TI Estadual conduza revisões periódicas e avaliações dos sistemas governamentais do Estado com o propósito de re-certificação das salvaguardas de segurança da Rede Governamental para tais sistemas.

Três tipos de investigação de segurança são exigidas:

a. Uma **Re-certificação** deve ser conduzida pelo menos uma vez a cada ano para cada Sistema Governamental ou sempre que for detectada a necessidade.

b. Uma **Análise de risco** deve ser conduzida pelo menos uma vez a cada dois anos para cada Sistema Governamental ou sempre que for detectada a necessidade.

c. Uma **Revisão de Controles Internos do Programa de Segurança de Sistemas governamentais** para o Sistema Governamental deve ser conduzida pelo menos uma vez a cada dois anos ou sempre que for detectada a necessidade.

Cada órgão/entidade da administração pública estadual proprietário do sistema é responsável por garantir que estes três tipos de investigações sejam planejadas e conduzidas de maneira a permitir que prioridades consistentes sejam estabelecidas, minimizando a duplicação do esforço, e protegendo a Integridade do Programa de Segurança de sistemas governamentais da Rede Governamental.

5.3 Manutenção e Execução de Atividade de Auditoria

É necessário manter uma revisão periódica do programa de Segurança de sistemas governamentais. Deve ser exigido que uma empresa de consultoria externa conduza revisões periódicas e avaliações ao programa de Segurança de sistemas governamentais com o propósito de certificação dos procedimentos, salvaguardas, ferramentas de auditoria e se os mecanismos utilizados estão seguindo padrões internacionais de segurança.

6 Política

Esta seção apresenta a política de segurança de sistemas governamentais baseado na criticidade operacional de sistemas governamentais. Os órgãos/entidades da administração pública estadual devem usar este guia para garantir a segurança dos sistemas governamentais classificados como nível 03 e 04.

Sabendo-se que nenhuma informação e nem todo Sistema Governamental são de mesmo valor ou sensibilidade para o Estado, as informações precisam ser agrupadas e protegidas diferentemente. Sistemas governamentais que são classificadas com Nível de Segurança Alto (03) exigem designações de salvaguardas de segurança mais aprofundadas do que aquelas designações com Nível de Segurança baixo. Sistemas governamentais que são classificados com nível mais baixo geralmente exigem somente precauções mínimas.

6.1 Responsabilidades

6.1.1. Administrador de Segurança de TI Estadual

a. Garantir que os sistemas governamentais com um Nível de Segurança designado como nível 04 ou 03 possuam um administrador nomeado responsável pela segurança do sistema ou serviço.

b. Garantir que as exigências de segurança computacionais estejam consideradas no desenvolvimento dos sistemas governamentais.

c. Garantir que as salvaguardas de segurança exigidas estejam colocadas para todos os sistemas governamentais, como descrito no quadro 01- **Matriz de salvaguardas de Segurança Mínima**.

d. Garantir que um Plano de Segurança de sistemas governamentais seja desenvolvido para cada Sistema Governamental que contenha informação sensível.

e. Garantir que cada Sistema Governamental sob sua responsabilidade tenha associado um status de segurança certificado. (Veja Quadro IX-B, "Certificação do Sistema Governamental Segurança")

f. Garantir que a argumentação lógica para as exigências ou recomendações de segurança citadas na verificação de risco e/ou Plano de Segurança de sistemas governamentais estejam documentadas.

g. Certificar que os administradores da rede dos órgãos/entidades onde os sistemas governamentais estão sendo executados fornecem os recursos exigidos na infra-estrutura e sistemas operacionais adequadamente para proteger o Sistema Governamental dentro de sua responsabilidade, proporcionado nível de risco aceitável.

6.1.2 Administradores de sistemas e Serviços da Rede Governamental

Administradores responsáveis por sistemas governamentais devem desenvolver, implementar e revisar os procedimentos para proteger a Integridade dos sistemas governamentais sob sua gerência. O responsável pelo Sistema Governamental é também responsável por:

a. Notificar o Supervisor de Segurança de TI Estadual e usuários sobre o nível de segurança exigido pelo Sistema Governamental.

b. Certificar que as exigências de segurança dos sistemas governamentais estão implantadas.

c. Documentar e prover uma explanação observando exigências individuais de segurança ou verificação de risco e recomendações que não podem ser satisfeitas.

d. Semestralmente, rever e verificar que todos os usuários dos sistemas governamentais sob sua gerência são autorizados e estão usando as salvaguardas de segurança exigidas.

e. Garantir que os sistemas corporativos e serviços corporativos sob seu domínio estão sendo executados somente na infra-estrutura do Sistema Governamental e que a infra-estrutura é também certificada no nível de segurança igual ou maior do que o nível de segurança designado para o sistema corporativo ou serviço de Rede Governamental.

f. O Administrador da rede ao qual o sistema corporativo ou serviço governamental responde pela especificação, implementação e revisão de procedimentos usados para proteger os sistemas operacionais dos sistemas e serviços sob sua responsabilidade, incluindo a execução da análise de risco e a determinação de exigências e salvaguardas mínimas de segurança.

6.1.3. Supervisor de Segurança de TI Estadual

a. Garantir que a infra-estrutura do Sistema Governamental que executa os sistemas governamentais, classificados no nível de segurança, é igual ou maior do que o nível de segurança designado para seus sistemas e serviços.

b. Realizar o inventário de sistemas e infra-estrutura respectiva do Sistema Governamental que foram designados com um nível de segurança 04 ou 03. A realização de inventário dos níveis 02 e 01 são opcionais.

6.2 Gerenciamento de Sistemas e Informação de Aplicação

6.2.2. Designações de Nível de Segurança para o Sistema Governamental

Responsáveis por sistemas governamentais devem associar a designação do Nível de Segurança para os sistemas e serviços usando as definições fornecidas na seção “Designações do Nível de Segurança”. As designações de Nível de Segurança determinam as salvaguardas de segurança mínimas exigidas para proteger os sistemas e serviços corporativos. Se um Sistema Governamental é compartimentado, da mesma forma que quando um conjunto de processos ou informações é mais sensível do que outros, o responsável pelo Sistema Governamental deve associar a designação do Nível de Segurança mais alto de qualquer conjunto de processos ou informações para o sistema ou serviço como um todo.

É importante enfatizar que um Sistema Governamental só deve ser executado em uma infra-estrutura que seja certificada em um nível de segurança igual ou maior do que o sistema e que o administrador seja responsável por garantir que todos os usuários do sistema corporativo e serviço da Rede Governamental satisfazem as salvaguardas exigidas para o sistema ou serviço em questão.

6.2.3. Integração de Segurança Computacional dentro do Desenvolvimento do Ciclo Vida do Sistema

Um Processo de controle deve ser estabelecido para garantir que os mecanismos de salvaguardas adequados sejam incorporados dentro de todas as novas funcionalidades e modificações significantes atuais do sistema. No mínimo, para cada sistema corporativo crítico, o responsável pelo sistema responde pela:

a. Definição e aprovação das especificações de segurança antes da programação.

b. Condução e aprovação das revisões do projeto e testes das características de segurança antes do lançamento do sistema para total operação.

6.3 Planos de Segurança de sistemas governamentais

Quando um Sistema Governamental é classificado como crítico (se associado uma designação de Nível de Segurança 04 ou 03), um Plano de Segurança de Sistema Governamental deve ser preparado. Ele deve incluir, no mínimo, quatro seções básicas:

6.3.1. Identificação do Sistema - Inclui a organização responsável, o nome do sistema ou assunto, o grupo (aplicação principal), o status do sistema operacional, uma descrição da função e propósito do sistema, uma descrição do ambiente do sistema ou serviço, e a pessoa de contato.

6.3.2. Sensibilidade de Informação Manipulada - Inclui leis aplicáveis e regulamentações, uma descrição da sensibilidade da informação em termos de tipo (confidencialidade, Integridade, disponibilidade) e importância relativa (alta, média, baixa) de proteção necessária.

6.3.3. Medida do Sistema de Segurança - Inclui uma verificação de risco, guia aplicável, medidas de controle de segurança exigidas, e status para cada medida de controle.

6.4 Certificação de Sistema Governamental

Para novos sistemas governamentais, o processo de certificação deve iniciar durante o estágio de desenvolvimento do sistema. Sistemas governamentais sensíveis devem ser re-certificados pelo menos uma vez a cada ano. Todo Sistema Governamental sensível deve ser re-certificado se a exigência da salvaguarda mudar, se o sistema for violado, ou o sistema submeter-se a uma modificação significante.

No mínimo, o Supervisor de Segurança de TI estadual, responsável pela certificação, deve revisar os seguintes documentos durante um processo de certificação para um Sistema Governamental sensível:

- Plano de Segurança do Sistema
- Resultados e testes de especificações de Segurança
- Plano de contingência
- Outros documentos pertinentes (análise de risco, registro de auditoria)

Quando o profissional responsável pela certificação estiver satisfeito com as salvaguardas colocadas para o Sistema Governamental e que a informação Processada pelo Sistema Governamental estiverem seguras, o procedimento adotado deve ser:

1. O profissional responsável pela certificação preenche o Quadro 02, "Certificação da Segurança do Sistema Governamental", para documentar o procedimento de certificação.

2. O Responsável pelo sistema fica com uma cópia do formulário de certificação da segurança e envia uma segunda cópia do formulário para o Administrador de Segurança de TI Estadual. A terceira cópia pode ser mantida como arquivo central.

3. Sistemas governamentais que não atendem as exigência de segurança substantiva e procedural não devem ser certificados. De qualquer forma, o quadro IX-C “Adiamento de Certificação” deve ser completado. A determinação de adiamento inclui uma lista de deficiências que devem ser remediadas. Quando um adiamento de certificação é executado, o sistema deve ser reportado como uma fragilidade de segurança sobre o processo de relatório.

6.5 Proteção do Núcleo de Facilidades e Infra-estrutura dos Sistemas governamentais

De acordo com esta política, todos os órgãos/entidades da rede estadual gerentes de sistemas governamentais devem implementar a segurança física e salvaguardas na sua infra-estrutura de TI para proteger estes patrimônios de uso não autorizado ou fraudulento, manipulação ou destruição.

As políticas e guias a serem criadas serão usadas para proteção da infra-estrutura, dos sistemas governamentais e sistemas operacionais da organização. O objetivo é proteger e preservar a informação, propriedade física, patrimônios humanos, e sistemas operacionais através da redução da exposição de vulnerabilidades que podem interromper ou cortar operações de sistemas governamentais.

6.6 Sistemas Operacionais

6.6.1. Exigências do Sistema Operacional

As exigências para proteção da infra-estrutura dos sistemas operacionais de sistemas governamentais são:

a. O Supervisor de Segurança de TI Estadual deve garantir que o sistema operacional em execução esteja usando as características que garantam a Integridade e previna o uso não autorizado das interfaces do Sistema Governamental.

b. O Supervisor de Segurança de TI Estadual deve garantir que o sistema operacional controla o acesso para a base de dados e programas de *softwares* armazenados no Sistema Governamental.

c. O Supervisor de Segurança de TI Estadual deve garantir que o sistema operacional registra e informa atividades fora de rotina que possam ser indicadas como uma violação de segurança.

d. O Supervisor de Segurança de TI Estadual deve garantir ainda que o sistema operacional:

(1) Forneça as salvaguardas para proteger o status operacional e a Integridade subseqüente durante e depois da re-inicialização do computador do Sistema Governamental.

(2) Inclua documentação completa e atualizada que permita a realização de auditorias para o propósito de triagem de atividades fora da rotina.

6.6.2. Procedimentos de Salvaguardas

a. Existem muitos métodos possíveis para manipulação de sistemas e os Responsáveis por Sistemas governamentais devem investigar os sistemas sob sua gerência para encontrar vulnerabilidades e garantir que salvaguardas estejam funcionando como deveriam.

b. O Responsável pelo Sistema Governamental deve instituir os procedimentos para a separação adequada de obrigações dentro da infra-estrutura do Sistema Governamental sob seu domínio.

c. O Responsável pelo Sistema Governamental deve estabelecer procedimentos que exigem validação de sistemas operacionais antes da instalação do mesmo. A validação deve ser executada tanto nos novos sistemas quanto nos sistemas modificados. O propósito da validação é garantir a inclusão de salvaguardas de segurança antes da Instalação do mesmo.

6.7 Determinações da Política de Segurança de Sistemas e Serviços da Rede Governamental

6.7.1. **Existência de controle de sistemas.** O controle de sistema para cada Sistema Governamental deve garantir que salvaguardas adequadas foram incorporadas a ele, testadas antes da implementação, e testadas anualmente após a implementação.

6.7.2. **Um plano de sistemas qüinqüenal deve ser desenvolvido.** Cada órgão/entidade da administração pública estadual deve desenvolver um plano, incluindo marcos específicos com obrigações e estimativas de despesas, para cada Sistema Governamental no órgão/entidade da administração pública estadual. Estas exigências cobrem os sistemas governamentais existentes e sistemas em desenvolvimento.

6.7.3. **Existência de um plano de contingência/ recuperação de desastre.** Os órgãos/entidades da administração pública estadual devem desenvolver, manter, e testar recuperação de desastre e planos de continuidade de operações para garantir que seus sistemas corporativos fornecerem uma continuidade de suporte razoável do processamento dos sistemas e serviços se as operações normais forem impedidas.

6.7.4. **Condução de verificação de vulnerabilidades.** A Administração central de segurança deve revisar a susceptibilidade de seus programas ou funções contra danos, perdas, uso não autorizado ou uso indevido através da condução de verificações de vulnerabilidade ou estudos equivalentes tais como auditorias.

6.7.5. **Existência de análise Custo-Benefício.** Os órgãos/entidades da administração pública estadual devem determinar e comparar os benefícios de propostas de sistemas ou controles contra o custo de desenvolver e operar estes sistemas ou controles. Somente propostas em que os benefícios excedam as estimativas de custo em 10% devem ser consideradas para desenvolvimento, a menos que seja especificamente exigida por lei.

6.7.6. **Garantias razoáveis são aplicadas.** Garantia razoável é igual a um nível satisfatório de confidencialidade, baseado no julgamento pelo Supervisor de Segurança de TI Estadual, Administrador de Segurança de TI Estadual e responsáveis pela área de TI do órgão/entidade, se for o caso, dos controles de custo/ benefício versus riscos reconhecidos. É reconhecido que esta garantia não é 100% efetiva. Cada órgão/entidade da administração pública estadual deve fornecer uma garantia razoável.

6.7.7. **Controles objetivos estão definidos.** Os órgãos/entidades da administração pública estadual devem estabelecer os objetivos para endereçar vulnerabilidades conhecidas, ou para promover a segurança dos sistemas governamentais.

6.7.8. **Técnicas de controle são selecionadas.** Os órgãos/entidades da administração pública estadual devem desenvolver métodos, satisfazer as exigências de controles prevenindo, detectando, e/ou corrigindo eventos indesejáveis.

6.7.9. **Adequações às exigências de segurança estão determinadas.** Os órgãos/entidades da administração pública estadual devem garantir que requisitos adequados de segurança no âmbito técnico, administrativo, físico, e pessoal estejam inclusos nas especificações para a aquisição ou operação da infra-estrutura de sistemas governamentais, equipamentos ou *software*.

6.7.10. **Existência de especificações de Segurança.** Controles internos e exigências de segurança devem estar declaradas com designado nas especificações e aprovado pelo Administrador de Segurança de TI Estadual antes que comece o desenvolvimento do Sistema Governamental.

6.7.11. **Determinação da adequação das especificações de segurança.** Os órgãos/entidades da administração pública estadual devem apresentar provas para o Administrador de Segurança de TI Estadual de que planejou especificações satisfazendo as exigências de controle para autorizar o desenvolvimento e/ou modificação dos programas computacionais dos sistemas governamentais.

6.7.12. **Aprovação do Plano de sistema.** Antes do desenvolvimento de um Sistema Governamental ser autorizado, a Administrador de Segurança de TI Estadual deve ter certeza de que o projeto do sistema satisfaz as exigências do usuário e incorpora as exigências de controle adequadas.

O plano de revisão deve ser documentado e deve estar disponível para avaliação.

6.7.13. **Documentação dos Controles.** Controles internos de sistemas, incluindo todas as transações e eventos significantes, devem estar claramente documentados e prontamente disponíveis para avaliação.

6.7.14. **Existência de documentação de sistemas.** A documentação deve refletir o estado atual de um Sistema Governamental assim que ele começa a operar. A documentação deve ser suficiente para garantir operações efetivas por usuários e manutenção de sistemas por programadores.

6.7.15. **Existência de um plano de contingência de sistemas.** Planos devem ser desenvolvidos, documentados, e órgão/entidade para assegurar que os usuários de sistemas governamentais possam continuar a executar suas funções essenciais no caso da capacidade de processamento ser interrompida. O plano deve também ser consistente com a recuperação de toda a abrangência do órgão/entidade da administração pública estadual em caso de desastre.

6.7.16. **Teste de Controles** Antes de um Sistema Governamental, novo ou modificado, ser colocado em estado de produção, seus controles devem ser testados para provar que eles operam como desejado. Os resultados dos testes devem ser documentados e enviados para o Administrador de Segurança de TI Estadual findando aprovação antes da implementação do sistema.

6.7.17. **Condução de testes sistemas.** Antes da implementação de um Sistema Governamental ser autorizada, evidências de que o sistema opera como desejado devem ser apresentadas ao Administrador de Segurança de TI Estadual. Estas evidências devem também incluir os resultados dos testes de controle. Os resultados dos testes devem estar documentados e disponíveis para avaliação.

6.7.18. **Documentação dos resultados dos testes.** A documentação deve demonstrar que as exigências de controle e de funcionalidade de sistemas governamentais operam como esperadas.

6.7.19. **Certificação do sistema antes da implementação.** Antes de um Sistema Governamental poder ser implantado, o Administrador de Segurança de TI Estadual juntamente com o Supervisor de Segurança de TI Estadual deve certificar que o sistema atende a todas políticas estaduais aplicáveis, regulamentações, e padrões, e que os resultados dos testes demonstram que os controles instalados são adequados para o sistema.

6.7.20. **Revisão dos controles executados.** Periodicamente, cada Sistema Governamental deve ser testado para determinar se suas funções de controle ainda funcionam como esperado. Os resultados dos testes devem estar documentados e disponíveis para avaliação.

6.7.21. **Condução de revisões periódicas e re-certificações.** Pelo menos uma vez a cada ano, os órgãos/entidades da administração pública estadual que possuem sistemas governamentais com nível de criticidade 04 ou 03 devem revisar tais sistemas e recertificá-los quanto a adequação de suas salvaguardas. As re-certificações devem ser documentadas e devem estar disponíveis para revisão.

6.7.22. **Condução periódica de verificações de risco.** Os órgãos/entidades da administração pública estadual devem conduzir verificações periódicas de risco na infra-estrutura dos sistemas governamentais sob sua gerência para fornecer a medida de suas relativas vulnerabilidades e ameaças à infra-estrutura para que os recursos de segurança possam ser efetivamente distribuídos para minimizar perdas potenciais.

6.7.23. **Uma ação corretiva é tomada, os resultados de auditoria são resolvidos imediatamente.** Os administradores devem avaliar imediatamente os resultados de auditoria e recomendações, determinar apropriadamente as ações corretivas a serem tomadas, e completar essas ações.

6.7.24. **Preparação de um relatório anual de controle interno.** Cada órgão/entidade da administração pública estadual deve anualmente determinar se os sistemas de controle interno estão de acordo com os padrões gerais de controle.

6.7.25. **Preparação de um relatório anual de controle de contabilização.** Cada administrador de redes e sistema em cada órgão/entidade da administração pública responsável pelo sistema corporativo em questão e serviço da Rede Governamental estadual deve verificar anualmente se a contabilização de seus sistemas estão de acordo com os padrões gerais de controle.

6.7.26. **Envio de relatórios anuais para o Administrador de Segurança de TI Estadual.** O responsável por cada sistema deve assinar um relatório anual e transmiti-lo anualmente para o Administrador de Segurança de TI Estadual.

ANEXOS

7 Gerenciamento de Risco

De acordo com as exigências do Programa de Segurança de sistemas governamentais, todos os órgãos/entidades da administração pública estadual responsáveis pelos sistemas governamentais devem desenvolver, implementar, e manter um programa de Gerenciamento de Risco para garantir que as medidas de salvaguardas adequadas sejam tomadas a fim de proteger todas as informações sensíveis e capacidade de processamento da informação ou serviço.

O propósito desta sessão é descrever os elementos básicos de um Programa de Gerenciamento de Risco de sucesso em nível governamental. As características peculiares de cada Programa de Gerenciamento de Risco podem variar, mas os princípios gerais e métodos de Gerenciamento de Risco permanecem o mesmo. Todo Programa de Gerenciamento de Riscos consiste de uma análise de risco seguida pela seleção e Implementação de salvaguardas.

7.1 Responsabilidades

A. Administrador de Segurança de TI Estadual

O Administrador de Segurança de TI Estadual é responsável por garantir que um Programa de Gerenciamento de Riscos adequado seja desenvolvido, implementado, e mantido para todos os sistemas governamentais e infra-estrutura dos sistemas governamentais de designação de nível 02 ou superior.

B. Supervisor de Segurança de TI Estadual

O Supervisor de Segurança de TI Estadual é responsável por:

- Coordenar o Programa de Gerenciamento de Riscos na Rede Governamental para garantir que todos os Programas de Gerenciamento de Riscos estejam integrados entre si.
- Desenvolver, direcionar e suportar o Programa de Gerenciamento de Riscos para cada Sistema Governamental e monitorar todas as fases destes programas a fim de garantir que as fases sejam conduzidas de forma adequada e eficiente.

C. Responsáveis por Sistemas governamentais

Os profissionais responsáveis por sistemas governamentais devem conduzir análises de risco para os sistemas governamentais e infra-estrutura do Sistema Governamental sob sua responsabilidade a fim de determinar o custo efetivo e as salvaguardas de segurança necessárias.

7.2 Programa de Gerenciamento de Risco

Cada órgão/entidade da rede estadual responsável por Sistema Governamental deve desenvolver um programa de Gerenciamento de Risco. É quase impossível eliminar o risco completamente, mas os responsáveis pelos sistemas precisam estar cientes dos riscos potenciais e vulnerabilidades das informações que ameaçam a segurança dos sistemas governamentais e da infra-estrutura do Sistema Governamental. Uma vez ciente dos problemas e das opções de salvaguardas, os responsáveis pelos sistemas podem tomar decisões fundamentadas na preocupação da necessidade e custo beneficio das várias opções de salvaguardas e alternativas de segurança aos sistemas governamentais.

É necessário que uma análise de riscos de sistemas governamentais seja realizada periodicamente a cada dois anos.

A infra-estrutura do sistema deve ser revisada a cada dois anos. Revisões adicionais são exigidas quando acontecerem modificações significantes no sistema ou na infra-estrutura do sistema.

Se a análise de risco apresentar falta de conformidade com as exigências de segurança, as razões pelos quais as exigências de segurança não podem ser satisfeitas devem ser documentadas e tal documento deve ficar disponível para auditoria.

Se possível, a análise de risco inicial deve ser executada em conjunto com o desenvolvimento do sistema. Uma análise de risco de alto nível deve ser conduzida na fase de inicio do ciclo de vida do sistema. Riscos adicionais podem ser identificados durante o progresso do desenvolvimento desde as exigências de definição, projeto, codificação, e testes.

O programa de Gerenciamento de Risco consiste dos seguintes Processos:

7.3 Análise de risco

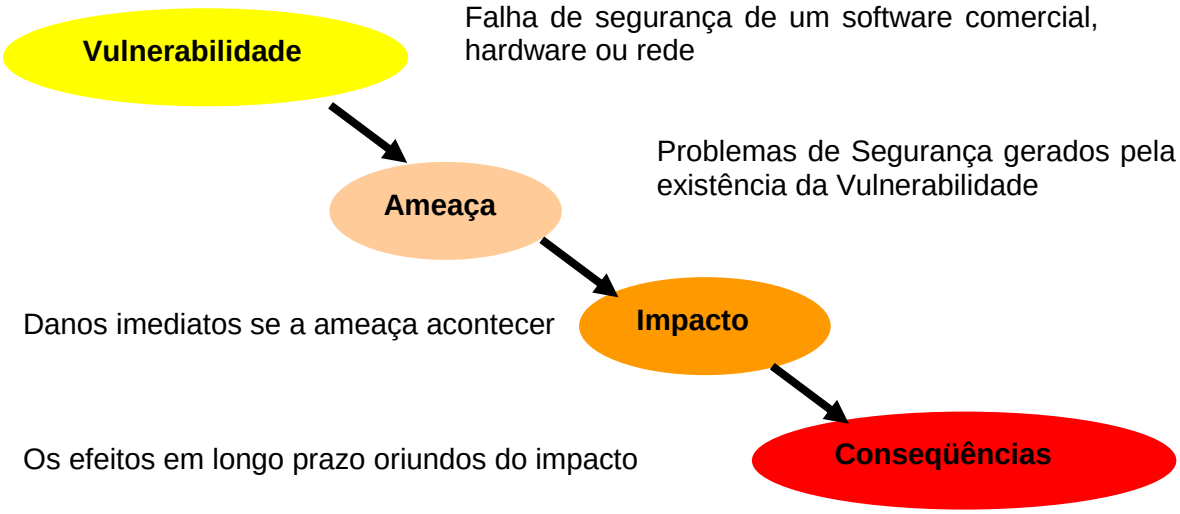
a. Passo 01- Determinação da Ameaça
b. Passo 02- Identificação das Vulnerabilidades
c. Passo 03- Associação das Medidas de Probabilidade
d. Passo 04- Estimativa das perdas Potenciais
e. Passo 05- Análise de Salvaguardas
f. Passo 06- Análise do Custo Beneficio
g. Passo 07- Desenvolvimento do Relatório Final
h. Passo 08- Criação do Arquivo de sumário de verificação de Risco

Seleção e Implementação das Salvaguardas

a. Decisões Gerenciais

b. Implementação

7.4 Processo da Análise de Risco



O objetivo de uma análise de risco formal é determinar o status atual da segurança de um Sistema Governamental e da infra-estrutura do Sistema Governamental.

Na primeira fase, as ameaças e vulnerabilidades especificas são identificadas e analisadas.

Depois, as salvaguardas potenciais são avaliadas para selecionar aqueles que são de melhor custo efetivo no tratamento das ameaças e eliminação ou redução das vulnerabilidades para um nível aceitável.

Por último é preparado um relatório final que sumarize os resultados e apresente um conjunto de recomendações agrupadas por prioridade. O relatório final de várias análises de risco sobre um órgão/entidade da rede estadual pode tornar-se a base para um arquivo de Sumário de Verificação de Risco, conduzindo a uma possível mudança na política desenvolvimento.

Descrição:

Termo	Descrição	Exemplo
Ameaças/probabilidade	Ameaças qual a probabilidade de sua ocorrência	Acesso pela Internet / Probabilidade = Alta
Impactos	Danos imediatos se a ameaça acontecer	Roubo, modificação
Conseqüências	Os efeitos em longo prazo se a ameaça acontecer	Diminuição do PIB
Controles	Medidas de segurança efetivas para diminuir a probabilidade	Serviços e mecanismos de segurança
Risco	O Risco permanecente, depois da implantação dos controles	Seqüestrar um usuário chave e descobrir a senha dele.

Os sistemas governamentais devem ser avaliados de acordo com o impacto do acontecimento da ameaça e conseqüência para o Estado, caso a mesma aconteça.

a. Determinação da Ameaça

A determinação da Ameaça exige a identificação e verificação das ameaças potenciais para um Sistema Governamental ou sua infra-estrutura. Ameaças Potenciais incluem desastres naturais e pessoas que podem interromper operações ou dependem de tempo de serviços ou podem causar perdas aos patrimônios físicos, perda de Integridade no sistema ou prejuízos para o Estado. Cada análise de risco resulta em um sumário com uma lista de ameaças para todo aspecto de Sistema Governamental e infra-estrutura do Sistema Governamental.

O resultado deste processo deve constituir de uma forte indicação das ações adversas que devem causar danos ao sistema, a probabilidade que estas ações devem ocorrer e a fragilidade do sistema que pode ser explorada para causar as ações adversas. Para conseguir atingir este resultado, as ameaças e vulnerabilidades precisam ser identificadas, bem como a probabilidade da ocorrência das mesmas.

b. Identificação da Vulnerabilidade

Identificação de Vulnerabilidade envolve a determinação de fragilidades ou falhas que existem em um Sistema Governamental ou na sua infra-estrutura, e que permitiriam afetar o sistema de segurança. A identificação de vulnerabilidades deve ser realizada nos sistemas governamentais e na

infra-estrutura dos sistemas governamentais novos, existentes e modificados recentemente.

Os controles de segurança existentes devem ser analisados para determinar se eles estão atualmente provendo alguma proteção às ameaças identificadas.

Se um controle não estiver provendo segurança, ele deve ser considerado como uma vulnerabilidade.

Uma análise de alto nível consegue determinar a amplitude do risco decorrente da perda de confidencialidade de determinados dados, através da revelação da informação.

Um sumário contendo a lista de vulnerabilidades identificadas deve ser preparado para cada Sistema Governamental e sua infra-estrutura sendo analisada. A seguinte área de Vulnerabilidade deve ser verificada:

(1) Oportunidade para entrada de informações erradas ou falsificadas.
(2) Oportunidade para acesso não autorizado.
(3) Controles administrativos não efetivos.
(4) Controles ineficientes dentro do programa do sistema.

C. Associação de Medidas de Probabilidade

A probabilidade de ocorrência de uma ameaça pode ser normalizada como um valor que varia entre 01 e 03 na seguinte forma:

03 = Alta

02 = Moderada

01 = Baixa

Associar o par Ameaça/vulnerabilidade com a probabilidade de realização da ameaça.

Ex: Qual a probabilidade de uma ameaça ser realizada, se uma vulnerabilidade for explorada?

Patrimônio	Ameaça	Criticid.	Vulnerabilidade	Prob.
Planos estratégicos	Roubo	03	Armazenados em um servidor sem proteção e senha fraca com acesso à Internet e IP válido	03

d. Estimativa de Perdas Potenciais

Depois das ameaças e vulnerabilidades terem sido determinadas, o valor (em dinheiro ou outro peso de medida) das perdas potenciais, incluindo todos os custos, deve ser quantificado.

Por exemplo, no caso de perda de informação ou roubo de arquivos de programas específicos, a perda potencial é o custo para reconstruir os arquivos, tanto das cópias de *backup* ou dos documentos origem, e possivelmente o custo de espera de processamento para o usuário. Quando perdas de tempo são mais criticas que perda de dinheiro, tais como um sistema de suporte médico ou a geração de arrecadação, então a medida de perda de tempo torna-se mais adequada do que a medida de custo para a condução da análise de riscos.

O valor do Sistema Governamental pode ser representado em termos de perda potencial. Esta perda pode ser baseada no valor substituído, o impacto imediato da perda e a conseqüência. Esta técnica de avaliação indicará o *ranking*.

03 = Alta;

02 = Moderada;

01 = Baixa.

O valor de um sistema também pode ser calculado através do somatório de todos os gastos (pessoal técnico e digitadores, valor do sistema, manutenção, energia) que o Estado teve desde sua concepção até os dias atuais para que este sistema estivesse neste estágio de desenvolvimento manipulando as informações atuais.

e. Análise de Salvaguarda

A fase seguinte inclui a identificação e verificação de possíveis medidas de salvaguardas e seus custos relacionados. As salvaguardas identificadas devem preencher as exigências de segurança mínima grifadas no Quadro-01, "Matriz de Salvaguardas de Segurança Mínima".

Na tabela abaixo temos um exemplo para determinar mecanismos necessários para proteger os sistemas contra Ameaças.

Ameaça	Vulnerabilidade	Risco	Salvaguarda	
			Serviço	Mecanismo
Acesso a informaçõe s pessoais	Senha fraca	03	Mudança da forma de criação das Senhas	Gerador de senha ou sistema Baseado em Tokens.

f. Análise Custo Beneficio

Durante esta fase, uma prioridade é associada para cada ameaça ou Vulnerabilidade (e.g., essencial, importante, marginal). Os custos das possíveis salvaguardas são comparados com os custos de perdas estimados que devem ser esperados no caso das salvaguardas não serem implementadas. Situações, onde o custo de se salvaguardar pesar mais do que o beneficio de sua Implementação, devem ser documentadas.

Calculando a medida do custo das salvaguardas

O custo pode ser normalizado com valores da mesma maneira como está sendo usado para perdas potencias.

03= Custo Alto

02=Custo Médio

01= Custo Baixo

g. Relatório Final

Quando a análise de risco estiver completa, um relatório final deve ser preparado. O relatório deve possuir no mínimo as seguintes seções:

(1) Lista de ameaças e vulnerabilidades.

(2) Lista de salvaguardas, incluindo as alternativas, sempre que existirem mais do que uma possível salvaguarda.

(3) Análise do Custo beneficio para cada ameaça ou Vulnerabilidade e as salvaguardas potenciais.

(4) Salvaguardas recomendadas baseadas na análise de Custo beneficio.

Calculando Riscos

O resultado deste processo deve indicar para a organização o grau de risco associado com os patrimônios analisados.

RISCO = Magnitude de Perda X Freqüência da perda

Considere os componentes adicionais:

Confiabilidade,

Proteção,

Performance.

Sistema Governamental	Prob.	Perda	Cálculo	Risco
Sistema Financeiro	02	01	2X1=	02
E-mails	02	03	3X2=	06
Aplicação Web	03	03	3X3=	09

Tabela de Riscos

Valor	Risco
01	Baixo
02	Baixo
03	Moderado
04	Moderado
06	Alto
07	Alto
08	Alto
09	Alto

A Comparação das medidas de risco deve resultar na criticidade dos componentes usados para determinar a medida de risco.

Comparando Riscos e Custos

Para calcular o relacionamento Custo/beneficio use a medida de risco associado com cada relacionamento Ameaça/mecanismo e crie uma taxa de risco para o custo. Se a taxa for < 1, indicará que o custo do mecanismo é maior do que o risco associado com a ameaça. Isto geralmente não é uma situação aceitável e pode ser difícil justificar, mas não deve ser automaticamente desconsiderada. Considere que o valor do risco é uma função de ambos as medidas de perda e probabilidade. Um ou ambos podem representar algo tão crítico sobre o patrimônio tal que o mecanismo de custo seja justificado.

h. Arquivo Sumário da Verificação de Risco

Um arquivo Sumário da Verificação de Risco, que acumule informações de saída de várias análises de riscos, fornecerá o conhecimento necessário sobre as falhas e defeitos comuns e o desenvolvimento da política para o Administrador de Segurança de TI Estadual, o Supervisor de Segurança de TI Estadual e responsável por sistemas.

O Administrador de Segurança de TI Estadual é responsável por garantir a criação de uma agenda para condução de análises de risco dentro dos órgãos/entidades da administração pública estadual.

Os responsáveis pelos sistemas devem conduzir análises de risco a uma freqüência comensurável com a sensibilidade dos sistemas governamentais ou da informação que eles processam. Eles também devem conduzir análises de risco sempre que grandes mudanças acontecerem em um Sistema Governamental sensível ou infra-estrutura de um Sistema Governamental. Responsáveis pelos sistemas devem manter todos os relatórios de análise de risco e documentação por pelo menos 05 anos.

7.5 Seleção e Implementação das Salvaguardas

a. Decisões de Gerenciamento

Baseado no relatório de análise de risco e com apoio do Supervisor de Segurança de TI Estadual, Responsáveis por Sistemas governamentais devem selecionar salvaguardas de segurança especificas que permitam uma notável redução na exposição da informação baseado no menor custo de implantação. Como parte deste processo, administradores de segurança devem identificar salvaguardas que possam proteger múltiplos sistemas e infra-estrutura de sistemas.

b. Implementação

Responsáveis por sistemas governamentais e administradores da infra-estrutura em conjunto com o Supervisor de Segurança de TI Estadual, devem determinar uma agenda para implementar as salvaguardas selecionadas. A agenda deve considerar prioridades para o Estado e constrangimentos de verba, bem como a urgência associada com a proteção dos sistemas governamentais.

O responsável pelo sistema também deve desenvolver um plano para monitorar a Implementação das salvaguardas. O Supervisor de Segurança de TI Estadual deve revisar e aprovar todos os planos de Implementação baseado na adequação do mesmo ao Programa de Segurança de sistemas governamentais como um todo.

8 Plano de Contingência

Cada órgão/entidade da administração pública estadual responsável pela gerência de um Sistema Governamental deve desenvolver e testar um plano de contingência formal para cada Sistema Governamental classificado entre os níveis 04 ou 03. O nível 02 é opcional.

O plano a ser desenvolvido deve detalhar como o Sistema Governamental deve continuar sua missão e fornecer continuidade de processamento de informação se a operação do sistema, serviço ou rede for interrompida por um longo período de tempo, tal como falha de energia. O plano deve ser documentado e uma cópia deve ser enviada para a administração central de segurança governamental.

O Processo de desenvolvimento do plano de contingência de cada Sistema Governamental deve incluir desenvolvimento, manutenção, teste e implementação.

O Administrador de Segurança de TI Estadual da Rede Governamental deve exigir que cada administrador responsável por Sistema Governamental, seja um sistema corporativo, rede local, ou serviço da Rede Governamental realize uma análise de riscos para identificar ameaças potenciais para os sistemas e infra-estrutura do sistema. Em conjunto com esta análise de risco, cada administrador responsável pelo sistema deve determinar a extensão das salvaguardas a serem fornecidas em uma ação de resposta a incidentes de segurança. É recomendado que uma avaliação seja feita no ambiente do sistema para reduzir a ocorrência de incidentes de segurança e responder efetivamente aos incidentes quando eles ocorrerem.

8.1 Responsabilidades

8.1.1. Administrador de Segurança de TI Estadual

Deve garantir o desenvolvimento adequado e teste do plano de contingência para os sistemas governamentais devidos, assim como a manutenção deste dentro da Rede Governamental.

8.1.2. Supervisor de Segurança de TI Estadual.

O Supervisor de Segurança de TI Estadual da Rede Governamental é responsável por apoiar os administradores dos sistemas governamentais no desenvolvimento das políticas e procedimentos para garantir que o plano de contingência esteja corretamente desenvolvido.

8.1.3. Responsáveis por sistemas governamentais

Respondem pelo desenvolvimento e manutenção do plano de contingência, incluindo a designação de pessoal responsável por operações de *backup* no caso de grandes interrupções.

8.2 Introdução ao Processo de desenvolvimento do Plano de Contingência

Um plano de contingência deve ser desenvolvido para cada sistema corporativo governamental classificado com nível de criticidade 04 ou 03. Existem grandes diferenças no nível de detalhe exigido para um Sistema Governamental grande (baseado na sua arquitetura e plataforma). Esta Política tratará de planos de contingência para ambientes de computação distribuída.

Cada órgão/entidade da administração pública estadual responsável pelo Sistema Governamental deve fazer todo esforço para administrar o processo do plano de contingência de maneira integrada sobre todos os seus sistemas, ambientes e redes, alocando recursos eqüitativos, descobrindo e endereçando pontos da interface entre todas as partes envolvidas.

A seguinte lista apresenta passos chaves no Processo de plano de contingência:

a. Identificar os sub-sistemas mais críticos.
b. Classificar os sub-sistemas de acordo com a prioridade para recuperação.
c. Definir uma interrupção máxima permissível (i.e., interrupção de serviço, uso, ou acesso) para cada sistema, em conjunto com o Administrador de Segurança de TI Estadual.
d. Fazer *backup* regularmente dos sistemas críticos, informações, *softwares* operacionais, e base de dados.
e. Explorar possibilidades alternativas de processamento de sistemas governamentais dentro da Rede Governamental.
f. Selecionar um local alternativo, baseado em ajuda mútua, construindo, alugando, ou fazendo acordos com outros órgãos/entidades da administração pública estadual.
g. Desenvolver procedimentos de operação em locais alternativos.
h. Implementar testes no local alternativo usando informação de *backup*.
i. Continuar os testes regularmente.
j. Atualizar o plano de contingência baseado nos resultados dos testes.

9 Matriz de Salvaguardas de Segurança Mínima

A Matriz de Salvaguardas de Segurança Mínima identifica as salvaguardas de segurança que são exigidas para proteger todos os tipos de sistemas governamentais ordenados por nível de segurança. Um “X”na matriz significa que a salvaguarda é uma exigência para o Sistema Governamental ou para a designação do nível de segurança, e um “O” na matriz significa que a salvaguarda é opcional.

Justificativas para não Implementação destas salvaguardas devem ser baseadas nos resultados de uma análise de risco formal.

QUADRO 01- Matriz de Salvaguardas de Segurança Mínima

	Nível de Segurança			
	Nível 04	**Nível 03**	**Nível 02**	**Nível 01**
1. Garantir que exista uma documentação completa e atualizada para todos os sistemas em operação.	**X**	**X**	**X**	**X**
2. Exigir o uso de usuários e senhas baseado na política de senhas do Estado para proteção da informação sensível dos sistemas governamentais contra acessos não autorizados.	**X**	**X**	**X**	**O**
3. Estabelecer procedimentos para registrar e proteger o segredo de senhas e nomes de usuários.	**X**	**X**	**X**	**O**
4. Limitar o número de tentativas de acesso fracassadas a um sistema corporativo ou serviço da rede.	**X**	**X**	**X**	**O**
5. Desenvolver mecanismos por onde a autorização do usuário possa ser determinada.	**X**	**X**	**X**	**O**
6. Estabelecer auditoria automatizada com capacidade para registrar atividades do usuário.	**X**	**X**	**X**	**O**
7. Implementar métodos, que possa incluir o desenvolvimento de criptografia, para assegurar a informação sendo transferida entre dois pontos.	**X**	**X**	**O**	**O**
8. Garantir que o sistema operacional contenha controles para prevenir o acesso não autorizado para os *softwares* de sistema, tais como o SGBD.	**X**	**X**	**X**	**O**
9. Garantir que o sistema operacional contenha controles que separem o usuário e os modos de	**X**	**X**	**X**	**O**

operação de administrador.				
10. Registrar ocorrências de atividade de usuário ou operador fora de rotina e relatar tais atividades para o Supervisor de Segurança de TI Estadual.	**X**	**X**	**O**	**O**
11. Garantir que o sistema operacional forneça métodos para proteger o status operacional e a Integridade subseqüente durante e depois de uma parada/ inicialização.	**X**	**X**	**O**	**O**
13. Garantir que o sistema operacional contenha controles para garantir a transferência de informação entre todos os pontos de comunicação e dispositivos da rede.	**X**	**O**	**O**	**O**
17. Preparar e manter listas de pessoas autorizadas para acessar localizações e sistemas governamentais processando sistemas e serviços críticos.	**X**	**X**	**X**	**O**
18. Estabelecer procedimentos para controlar o acesso a localizações dos sistemas governamentais críticos.	**X**	**X**	**X**	**X**
19. Determinar todos os critérios de segurança física da localidade onde o Sistema Governamental está armazenado.	**X**	**X**	**O**	**O**
27. Garantir a segurança dos meios de comunicação utilizados na transferência da informação.	**X**	**X**	**X**	**O**
28. Conduzir testes de intrusão periódica ao sistema operacional.	**X**	**O**	**O**	**O**
30. Estabelecer um programa detalhado de Gerenciamento de Risco.	**X**	**X**	**X**	**O**
31. Estabelecer Planos de Segurança de Sistemas governamentais para sistemas e serviços críticos.	**X**	**X**	**X**	**O**
32. Conduzir análises de risco formais.	**X**	**X**	**X**	**O**
33. Estabelecer programas de conscientização e treinamento de segurança para os funcionários.	**X**	**X**	**X**	**X**
34. Manter inventário de todo o *hardware* e *software.*	**X**	**X**	**X**	**X**
35. Estabelecer programa de revisão e certificação de segurança.	**X**	**X**	**X**	**O**
36. Estabelecer plano de contingência.	**X**	**X**	**X**	**O**

38. Conduzir revisões periódicas do Nível de Segurança designado.	**X**	**X**	**X**	**O**
39. Garantir que todas as pessoas, incluindo contratados, receberam investigações.	**X**	**X**	**X**	**O**
40. Manter uma lista de todas as pessoas, incluindo contratados, que foram aprovados para utilização do sistema.	**X**	**X**	**O**	**O**

Quadro 02: Certificação da Segurança do Sistema Governamental

Eu revisei cuidadosamente o plano de segurança do sistema/ serviço computacional anexado e acompanhei o veredicto de recomendações de uma investigação de riscos documentada; análise de ameaças, vulnerabilidades, e salvaguardas; ou avaliação de segurança executada dentro de um ano Baseado na minha autoridade e julgamento e observando as exigências operacionais eu autorizo a operação continuada do (nome do Sistema Governamental) com as seguintes restrições:

(restrições, se alguma)

Além disso, eu autorizo o início das seguintes ações corretivas, a serem completadas dentro do próximo calendário anual:

(ações corretivas)

_____

Assinatura

Quadro 03: Adiamento de Certificação

Baseado na revisão do plano de segurança do sistema em anexo, as exigências de segurança do (nome do Sistema Governamental), esta aplicação não pode ser certificada neste momento. As razões para o adiamento incluem:

[ ] Uma análise de ameaças, vulnerabilidades, e salvaguardas não foi executada dentro do último ano.

[ ] Não existe especificações de segurança documentadas.

[ ] Especificações documentadas do teste de segurança não foram realizadas dentro do último ano.

[ ] Existem Vulnerabilidades (especificar) _____

[ ] Treinamento de conscientização de segurança não foi realizado.

[ ] Outro (especificar) _____

Eu autorizo o início das seguintes ações corretivas, a serem completadas dentro do próximo calendário anual:

(ações corretivas)

_____
Assinatura

Quadro 04: Matriz de Salvaguardas de Segurança do Sistema corporativo e serviço da Rede Governamental

Esta matriz fornece um guia para identificação das salvaguardas de segurança mínimas exigidas para sistemas governamentais.

Localize a designação do Nível de Segurança do sistema corporativo e serviço da Rede Governamental na coluna da esquerda. Um "X" para o lado direito da designação do Nível de Segurança significa que a salvaguarda de segurança listada acima é exigida, e um "O" significa que a salvaguarda de segurança é opcional.

Salvaguardas de Segurança						
Nível de Criticidade	Controles de Acesso	Criptografia	Cópias de *Backup*	Auditoria	Análise/ Revisão de Risco Periódico	Segurança Física
04	**X**	**X**	**X**	**X**	**X**	**X**
03	**X**	**O**	**X**	**X**	**X**	**X**
02	**X**	**O**	**X**	**O**	**X**	**X**
01	**O**	**O**	**O**	**O**	**O**	**O**

Quadro 05: *Checklist* de Segurança de Sistema Governamental

Explicação: As seguintes questões destacam as exigências de segurança dos sistemas governamentais. Para cada resposta "NÃO", forneça uma explicação por escrito para ser enviada ao Responsável pelo Sistema Governamental.

EXIGÊNCIAS	SIM	NÃO
1. É mantido um inventário preciso, incluindo o valor de *hardware* e *software*?		
2. Os relatórios e mídias removíveis estão adequadamente armazenados em um local seguro quando não estão sendo utilizados?		
3. É mantida uma lista atualizada de usuários autorizados?		
4. Os usuários autorizados foram treinados em operação e uso de microcomputadores, bem como nas exigências de segurança do Sistema Governamental?		
5. As senhas de acesso aos sistemas governamentais estão disponíveis somente para usuários autorizados?		
6. As senhas são trocadas quando usuários deixam o governo do Estado?		
7. Quando mudanças são realizadas (por exemplo, novas aplicações, rodízio de pessoal), os riscos são reexaminados?		
8. Cópias de segurança dos arquivos e base de dados são feitas periodicamente? Se afirmativo, registrar com que freqüência.		
9. A documentação de *software* e usuário é mantida atualizada e salvaguardada?		
10. Quando autorizado, uma cópia de segurança do *software* é feita e o original é mantido em segurança?		
11. Existe reavaliação da segurança trimestralmente?		
12. Os dispositivos de segurança instalados e os procedimentos empregados, diminuem o risco de roubo ou de acesso não autorizado ao microcomputador?		
14. Planos de contingências estão implantados para microcomputadores que executam aplicações com designações de Nível de Segurança de nível 04 ou 03?		
15. Os dados armazenados ou processados no microcomputador são sensíveis? (Se a resposta for "não", prossiga para a questão 17.)		
16. Existe pessoal em posição sensível relacionada aos		

computadores, que envolve seu, submetido a averiguações adequadas de dados pessoais?		
17. Existe capacidade de se implementar senhas para proteger sistemas governamentais? E para proteger informações?		
18. As informações sensíveis armazenadas estão protegidas de visualização ou uso não autorizado durante a transmissão e armazenamento?		
19. Os registros e disquetes estão rotulados e controlados?		
20. Registros sensíveis não mais necessários são destruídos e arquivos desnecessários são sobrescritos?		

OBS: Profissionais que conduzirem revisões de segurança em sistemas governamentais podem solicitar documentação especifica para apoio às suas respostas. Em adição, os resultados do *checklist* devem ser usados para determinar se a informação sensível é processada e/ou o plano de segurança de sistemas precisa ser desenvolvido (ou atualizado).

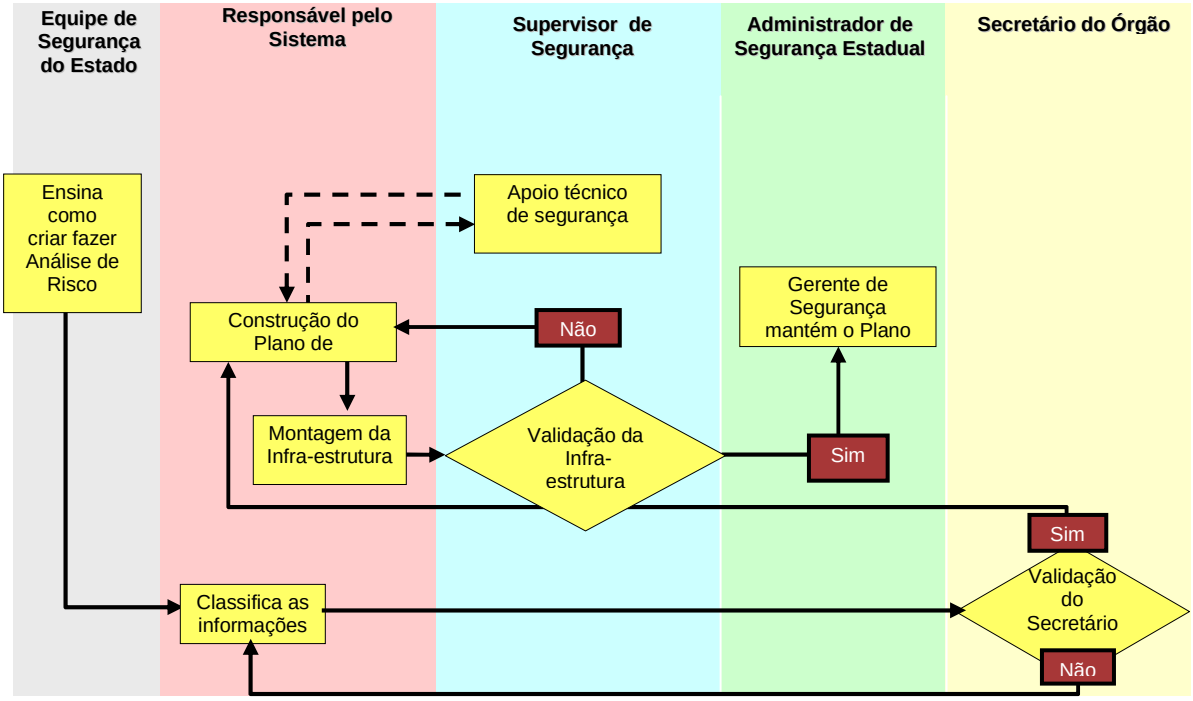
_____
_____
(Assinatura do Responsável pelo Sistema Governamental /Data)

_____ _____
(Assinatura pelo responsável do órgão/entidade da administração pública estadual /Data)

Quadro 06: Plano de Segurança de Sistema Governamental

10 PLANO DO SISTEMA

Fluxograma de Execução do Plano do Sistema



Modelo do Plano do Sistema

A. IDENTIFICAÇÃO DO SISTEMA

1- Categoria do Sistema	
Tipo:	☐ Serviço, ☐ Sistema Corporativo ☐ Rede local ☐ Outro.
Ameaça com Atenção Especial:	
Nome/ Título do Sistema Governamental	
Órgão ou Instituição Responsável pelo Sistema	
Informação do(s) Contato(s)	
Responsável pelo sistema	
Nome	
Cargo	
Endereço	
Telefone	
Nº do Fax	
Endereço de *E-mail*	
Status Operacional do Sistema Governamental	
☐ Operação ☐ Em Desenvolvimento ☐ Sendo modificado	
Descrição e Propósito Geral	
Função	
Fluxo de processamento do sistema da entrada até a saída	
Informação processada	

Ambiente do Sistema Governamental	
Descrição técnica do sistema	
Fatores ambientais ou técnicos	
Plataforma de computação	
Componentes principais do sistema	
Softwares de segurança	
Localização física	

Interconexão do Sistema e Compartilhamento de Informação

Leis Aplicáveis Afetando o Sistema

Sensibilidade da Informação e Verificação da Criticidade				
Informação tratada pelo sistema	Tipo	Necessidade de proteção	Sensibilidade	Salvaguarda

B. CONTROLES DE GERÊNCIA

Verificação e Gerência de Risco	
Relatório da verificação de risco.	
Grupo/ data	
Cronograma	

Revisão de Controles de Segurança					
Revisão	Tipo de Avaliação	Responsável	Propósito	Resultado	Ações

Regras de Comportamento	
Usuário	**Regra**

Planejamento de Segurança em um Ciclo de vida de Sistema	
FASE	**Tratamento de Segurança**
Iniciação	
Desenvolvimento /Aquisição	
Implementação	
Operação /Manutenção	
Finalização	

Autorização para Processamento

C. CONTROLES OPERACIONAIS

C.1 Segurança Pessoal

- Todos os cargos foram revisados quanto ao nível de sensibilidade?

- O acesso do usuário é restrito para o mínimo necessário para a execução da sua função?

- Existe um processo para solicitação, determinação, emissão, e encerramento de conta de usuário?

- As funções críticas são divididas entre pessoas diferentes com separação de obrigações?

- Quais mecanismos estão implementados para manter usuários responsáveis para suas ações?

- Quais são os procedimentos de encerramento de contratação de funcionários?

C.2 Controles de Produção, Entrada e Saída

- Existe um *help desk* ou grupo que forneça avisos e possa responder a incidentes de segurança em de forma imediata?

- Existem procedimentos implementados e documentados de forma a reconhecer, tratar, reportar, e corrigir incidentes e/ ou problemas?

- Existem procedimentos para garantir que pessoas não autorizadas não possam ler, escrever, copiar, alterar, ou roubar informação impressa ou eletrônica?

- Existem procedimentos para garantir que somente usuários autorizados acessam, recebem, ou entregam informações e mídias de entrada e saída?

- Existem auditorias para recebimento de entradas e saídas sensíveis?

- Existem procedimentos para restrição de acesso para saída de produtos?

- Existem auditorias para gerência de inventário?

- Existem procedimentos para armazenamentos controlados, tratamento, ou destruição de mídia que não pode ser reusada?

- Existem procedimentos para compartilhamentos ou outras medidas destrutivas para mídia não mais necessárias?

C.3 Planejamento de Contingência

- Acordos de processamento de *backup*.

- Procedimentos de *backup* documentados incluindo e escopo (*full*, incremental, e diferencial).

- Localização de *backups* e geração de *backups* armazenada.

- Os planos de contingência e recuperação de desastres implementados foram testados? Como eles foram testados?

- Todos os empregados chaves foram treinados sobre regras e responsabilidades relativas para a emergência, desastres e planos de contingência?

- Cobertura de procedimentos de *backup*?

C.4 Controles de *Hardware* e *Software* para Manutenção do Sistema

- Existem restrições quanto às pessoas que executam manutenção em *hardware* e *software*?

- Existem procedimentos especiais para realização de reparos e manutenção de emergência?

- Existem procedimentos usados para controlar serviços remotos de manutenção em casos em que procedimentos ou manutenção são realizados à distância?

- O *software* foi desenvolvido localmente ou através de contrato?

- O governo é o dono do *software*? Ele foi recebido de outro órgão/entidade da administração estadual?

- O *software* está licenciado adequadamente e existem cópias suficientes para o funcionamento do sistema?

- Existem políticas organizacionais contra uso ilegal de *software* e "*sharewares*" protegidos por direito de cópia?

- Auditorias periódicas são realizadas em computadores de usuários para garantir que somente cópias de *software* legalizadas estão instaladas?

- Quais procedimentos estão sendo usados para proteger a organização contra uso de *software* ilegal?

- Descreva qualquer mudança formal nos processos de controles implementados.

- Todas as mudanças para o *software* do sistema ou componentes do sistema estão documentadas?

- Existem análises de impacto para determinar um efeito de mudanças propostas em medidas de segurança existentes incluindo necessidade de treinamento para as comunidades técnica e de usuário associadas com uma mudança em *hardware* ou *software*?

- Existem procedimentos de identificação, aprovação, e documentação de mudanças?

- Existem procedimentos para certificar que planos de contingência e outras documentações associadas estão atualizados para refletir mudanças no sistema?

- Existe um processo que obriga todas as mudanças para um sistema de *software* ser testado e aprovado antes do *software* ser colocado em produção?

- Existem procedimentos para teste e ou aprovação de componentes do sistema antes de ser colocado em produção?

- Planos de testes fazem referência para as necessidades originais de segurança?

- Os resultados dos testes são documentados?

C.5 Controles de Integridade e Validação de Dados

- Existe sistemas de detecção de vírus e eliminação de *software* instalados? Caso positivo, existem procedimentos para atualização de arquivos de assinatura de vírus, procura automática e/ou manual de vírus, e eliminação e relatório de vírus?

- Existem rotinas usadas pelo sistema, tais como, *checksums*, *hash*, contagem de registros? Inclua descrição das ações tomadas para resolver quaisquer discrepâncias.

- Programas de verificação de integridade estão sendo usados pelo sistema para procurar por evidencia de informações com erros e omissões de informações?

- Uma ferramenta de detecção de intrusos está instalada para monitorar o sistema?

- Existem procedimentos implementados para tratar e resolver incidentes de segurança?

- Outros pacotes de *software* de segurança de rede são usados? Quais?

- O sistema de monitoramento e performance é usado para análise de logs em tempo real a procura de problemas de disponibilidade, incluindo ataques ativos?

- Teste de penetração foi realizado no sistema? Em caso positivo, quais os procedimentos que estão implementados para garantir que estes testes foram realizados adequadamente?

- A autenticação da mensagem usada em um sistema para garantir que o emissor da mensagem é conhecido e que a mensagem não foi alterada durante a transmissão?

C.6 Documentação

Sistema	Lista de Documentação	Procedimento para atualização	Localização Física

D. CONTROLES TÉCNICOS

D.1 Identificação e Autenticação

- Descreva os mecanismos de controle de autenticação do usuário ao sistema

---

- Indique a freqüência de mudanças de senhas, descreva como as mudanças são reforçadas e identifique quem faz a mudança das senhas (o usuário, o administrador do sistema, ou a sistema).

- Verifique se os requisitos abaixo são usados no sistema de senha:

  ☐ Tamanho de senha (mínimo, máximo);

  ☐ Conjuntos de caractere usados;

  ☐ Espaço de tempo para troca de senha;

  ☐ Número de geração de senhas expiradas não permitidas para uso;

  ☐ procedimentos para mudanças de senha (depois da expiração e esquecida, perdida);

  ☐ procedimentos para tratamento de comprometimento de senha;

  procedimentos para treinamento de usuários.

- Descreva o mecanismo de controle de acesso (rede, operação de sistema, e sistema *software*).

- Descreva como o mecanismo de controle de acesso suporta controle individual e auditoria (e.g., senhas associadas com um ID de usuário que é associado para uma única pessoa).

- Descreva as técnicas de auto proteção para o mecanismo de autenticação do usuário (exemplo: senhas criptografadas enquanto são transmitidas pela rede).

- Determine o número de tentativas de acessos inválidos que podem ocorrer para um dado usuário ID ou acesso localização (terminal ou porta)

- Descreva os procedimentos para verificação e mudança de todas senhas padrão do usuário administrador de todos os sistemas.

- Descreva os procedimentos para limitação de *scripts* de acesso senhas embutidas.

- Descreva quaisquer políticas de exigência de autenticação de usuário, tais como tecnologia *single-sign-on* (e.g., computador a computador, servidores de autenticação, identificadores de usuário, e grupo usuário identificadores) e qualquer outro controle.

- Descreva qualquer uso de assinatura digital ou eletrônica e os padrões usados. Discuta os procedimentos gerenciais para geração de chaves, distribuição, armazenamento, e finalização.

D.2 Controles de Acesso Lógicos

- Como os direitos de acesso estão sendo concedidos? Os privilégios estão sendo concedidos baseados na função ou cargo de trabalho?

- Descreva a capacidade do sistema para estabelecer uma ACL.

- Descreva controles para detectar tentativas de transação não autorizada pelo sistema e /ou tentativas de acesso de usuários não autorizado.

- Descreva qualquer restrição para prevenir usuários de acessar o sistema fora do horário normal de trabalho ou em finais de semana.

- Indique a quantidade de tempo de inatividade de usuário para o sistema exigir que o usuário entre com sua senha para reconectá-lo ao sistema?

- Indicar se algum mecanismo de criptografia está sendo usado para prevenir acesso a arquivos sensíveis como parte do procedimento de controle acesso do sistema.

D.3 Controles de Acesso Públicos

- Quais controles adicionais estão sendo usados na interconexão deste sistema dentro da Rede Governamental para proteger a confidencia do sistema?

- Descreva os controles adicionais que estão sendo usados na conexão deste sistema na Internet.

- Tais controles incluem:

  ☐ Alguns formulários de identificação e autenticação?

  ☐ Controles de Acesso para limitar quais usuários podem ler, escrever, modificar ou apagar

  ☐ Controles de Assinatura Digital para prevenir usuários de modificar informação em um sistema público.

  ☐ Cópias de informação para acesso publico disponível em um sistema separado.

  ☐ Controles para proibir acesso público em bases de dados.

  ☐ Verificação de vírus em informação distribuída para o público.

  ☐ Auditoria do Sistema e disponibilidade da informação.