PLANO DIRETOR
DE
SEGURANÇA

Dezembro de 2006

Índice

Apresentação

Este documento condensa o “Plano diretor de comunicação e disponibilização de dados governamentais localizados na SEAD” e as “Necessidades Atuais e Futuras de segurança da SEAD” referente a seção 4.1.2.1 – Análise Abrangente do edital da segurança da Rede Governamental.

O Plano Diretor para segurança da Rede Governamental é um trabalho, que reúne o esforço de todos os gestores de TI do governo do Estado do Ceará e da Secretaria da Administração, como gestora deste plano, e que serve como instrumento norteador das ações e medidas de segurança que o Estado deve realizar na construção de um modelo seguro de gestão dos negócios e recursos de Tecnologia da Informação.

1. Introdução

Entende-se por Rede Governamental a interligação física e lógica de todos os órgãos/entidades da administração pública estadual direta ou indireta e outras entidades de interesse do governo do Estado do Ceará, delimitada pelo perímetro da rede local de cada uma destas e a conexão à Internet, localizada na Secretaria da Administração. O grau de informatização de cada órgão/entidade participante da Rede Governamental é heterogêneo, tornando a estrutura funcional complexa no aspecto de segurança. Entretanto, o uso dos sistemas corporativos de gestão estadual é comum a todos da administração pública estadual.

A Rede Governamental permite a comunicação entre órgãos/entidades da rede estadual na troca de informações entre si ou no acesso a sistemas corporativos e no acesso desses à Internet, devendo estas estarem protegidas contra ameaças internas e externas de segurança. Atualmente, as ameaças de segurança, tais como vírus, acesso e uso indevido de dados podem ser originadas a partir da Internet ou a partir de órgãos/entidades interligados através da Rede Governamental.

Por causa da complexidade e heterogeneidade das partes integrantes desta Rede, faz-se necessária a definição de diretrizes e normas de segurança, para as informações armazenadas em formato digital, a serem cumpridas por todos os órgãos/entidades no que diz respeito à conexão com a Internet e interligação com outras redes, para que os sistemas de informação do governo estejam protegidos contra ameaças existentes.

Abrangência

Toda administração pública estadual direta e indireta e outras entidades de interesse do Governo do Estado do Ceará que possuam conexão com a Rede Governamental, através de dirigentes e técnicos, deverão estar cientes do Plano Diretor de Segurança e colaborar para a consecução dos seus objetivos. A conscientização e a participação do Corpo de especialistas em informática responsáveis pela administração da infra-estrutura de TI, dos colaboradores técnicos contratados e demais usuários de informática que atuam nos órgãos/entidades conectados à Rede Governamental é fundamental para implantação e manutenção de um nível de segurança aceitável.

Finalidade

Este documento tem por finalidade de estabelecer a metodologia do processo de segurança de TI, determinando diretrizes básicas que nortearão as atividades relacionadas com a segurança da rede corporativa do Governo Estado do Ceará.

Relação deste Plano com outros Documentos

DOCUMENTOS DE SAÍDA

DOCUMENTOS DE ENTRADA

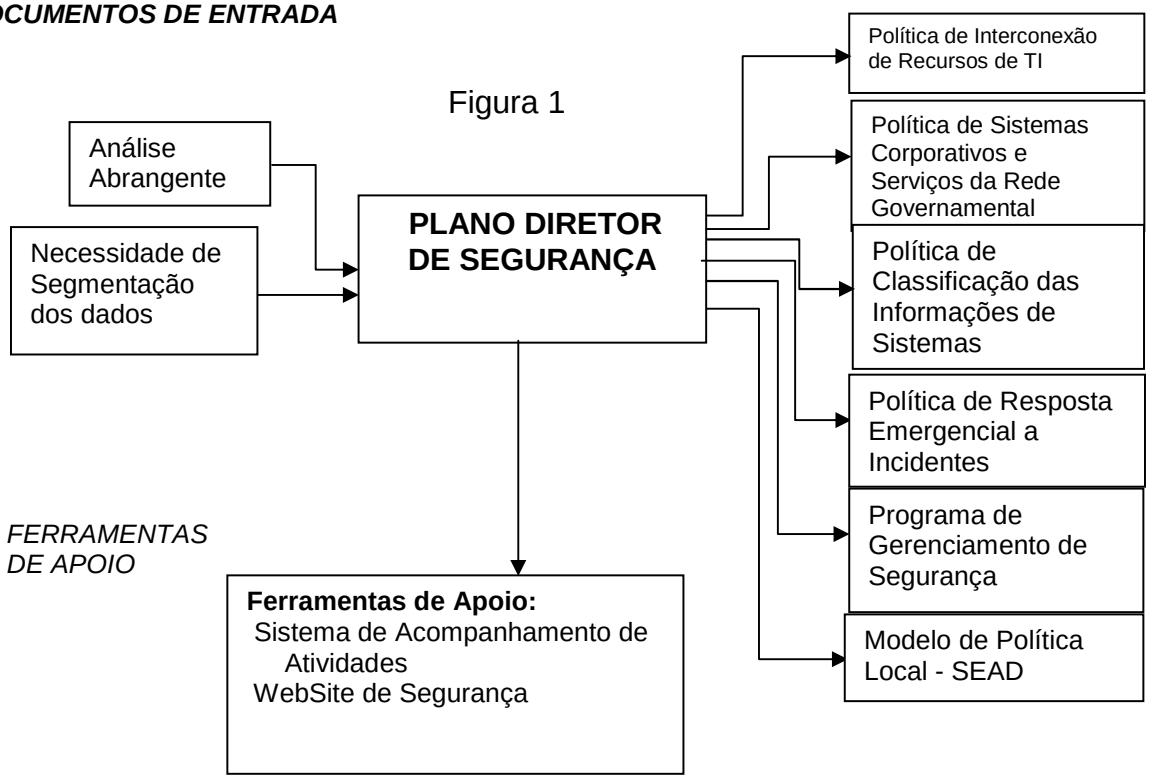


Figura 1

Os documentos de “Análise Abrangente” e “Necessidade de Segmentação dos Dados" fornecem os subsídios necessários para a elaboração deste plano e a criação das políticas e programa de gerenciamento de segurança.

NECESSIDADES DE SEGURANÇA DA REDE GOVERNAMENTAL

2. Análise de Segurança

De acordo com a análise abrangente das informações realizada pela consultoria em segurança nos órgãos da rede estadual, constatou-se que:

- Os dispositivos da Rede Governamental não garantem, por si só, a segurança necessária para proteger as informações que nela trafegam, pois existem muitas vulnerabilidades que podem comprometer a segurança da Rede Governamental;
- Cada órgão/entidade da administração pública estadual possui necessidades de segurança diferentes baseadas na sua missão, na sua forma de trabalho, na sensibilidade de suas informações e no grau de complexidade de sua infraestrutura tecnológica;
- As informações e infra-estrutura de TI dos diversos órgãos/entidades da administração pública estadual estão vulneráveis a ameaças originadas em outros órgãos/entidades conectados à Rede Governamental;
- As comunicações dentro da Rede Governamental acontecem sem planejamento, criando um ambiente inseguro e propício ao descontrole;
- Os sistemas de informação da gestão estadual em plataforma baixa, em geral, não possuem planejamento das necessidades específicas de segurança;
- Não existem políticas de segurança que regulamentem as atividades e ações envolvendo troca de informações na Rede Governamental;
- Os serviços da Rede Governamental possuem um nível de segurança razoável, mas necessitam de um planejamento de segurança mais elaborado;
- A Rede Governamental é composta por uma estrutura de sistemas (redes locais dos órgãos/entidades da administração pública, sistemas corporativos e serviços da rede) heterogênea e complexa, dificultando um modelo único de segurança para todas as partes da mesma;
- A forma como alguns órgãos/entidades utilizam os serviços de Internet pode comprometer a segurança da Rede Governamental.

Documentos Relacionados

O resultado da Análise encontra-se, na integra no documento intitulado: “ANÁLISE GLOBAL DE SEGURANÇA DA REDE GOVERNAMENTAL E NECESSIDADE DE SEGMENTAÇÃO DE DADOS E SERVIÇOS”.

3. Domínios de Segurança

Para assegurar a proteção das informações e obter uma melhor visão das necessidades de segurança para a Rede Governamental, é necessário mapear os locais onde as mesmas são processadas, tratadas, armazenadas, transmitidas e acessadas. Para efeito de análise, a Rede Governamental será subdividida em domínios de segurança, que são partes integrantes desta e interagem fortemente entre si.

Cada domínio possui vulnerabilidades peculiares e deve possuir um tratamento diferenciado. Este plano especifica a segurança de todos estes domínios e a integração entre eles.

No aspecto da segurança, a Rede Governamental é composta pelos seguintes domínios.

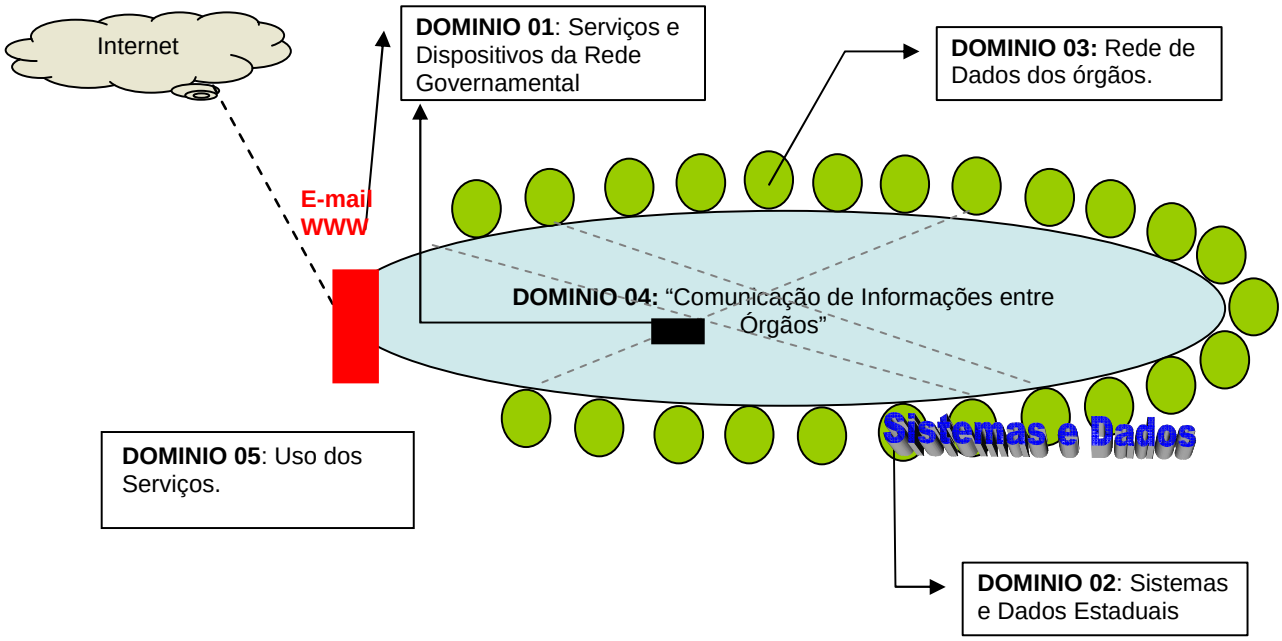


Figura 2

- **<u>DOMINIO 01:</u> Serviços e Dispositivos da Rede Governamental**

  Os serviços da rede, tais como acesso à Internet, *Proxy* (Cache de Páginas), DNS (Resolução de Nomes), Segurança de Internet, Intranet, dentre outros são administrados pela SEAD e utilizados por todos os órgãos/entidades estaduais.

  Os dispositivos, geralmente roteadores, são implantados e mantidos pelo provedor da Rede Governamental e são utilizados para realizar a troca de informações nesta.

- **DOMINIO 02: Sistemas de Informação e dados sensíveis**

  Sistemas de Informação estaduais são os sistemas que tratam informações necessárias para a administração pública estadual, tais como sistemas de Arrecadação, sistema de Orçamento, sistemas de Planejamento, dentre outros.

  Sistemas de Informações Públicas Sensíveis são aqueles que tratam informações sensíveis de cidadãos tais como Identidade Civil, licenciamento de veículos, contas de água e outros.

- **DOMINIO 03: Redes de Dados de Órgãos e seus Sistemas Internos**

  São as redes de dados locais dos órgãos/entidades conectados à Rede Governamental que tem seu perímetro delimitado pelo dispositivo de acesso a esta.

- **DOMINIO 04: Comunicação de informações entre entidades e órgãos dentro da Rede Governamental**

  É o serviço que permite aos órgãos/entidades trocar informações entre si com a Internet utilizando-se da infra-estrutura da Rede Governamental.

- **DOMINIO 05: Uso dos Serviços da Rede Governamental**

  É a forma como os usuários estão usando os serviços da Rede Governamental, tais como uso de E-mail, Internet, entre outros.

MECANISMOS DE PROTEÇÃO DA REDE GOVERNAMENTAL

4. Premissas

Com a responsabilidade de prover segurança aos serviços corporativos localizados na SEAD, a comunicação entre órgãos/entidades e aos dispositivos da Rede Governamental, o provedor de serviço elaborou um projeto denominado “Projeto de Segurança da Rede Governamental” a fim de garantir que a Rede Governamental estará devidamente protegida.

5. Prerrogativa

O modelo de segurança da Rede Governamental é baseado em classificação dos componentes de cada domínio descrito anteriormente, onde todo componente, seja ele uma rede local, serviço, informação ou infra-estrutura deve receber designação do nível de segurança baseado na sua criticidade e ou sensibilidade no contexto da Rede Governamental.

A seção necessidade de segmentação de dados e serviços do documento "ANÁLISE GLOBAL DE SEGURANÇA DA REDE GOVERNAMENTAL E NECESSIDADE DE SEGMENTAÇÃO DE DADOS E SERVIÇOS", contém a categoria das informações estaduais associada com a sensibilidade de cada informação em uma tabela contendo os campos:

Categoria	Explicação e exemplos	Nível de Segurança		
		B	**M**	**A**
(1) **Informação Pública**	Qualquer informação que seja declarada para consumo dos órgãos/entidades públicos por autoridades oficiais, tais como informações do diário Oficial. Também inclui Informações colocadas na Internet.	**B**		

O documento deve ser atualizado semestralmente para contemplar os novos componentes e eliminar os componentes não mais existentes.

- **Classificação das Informações dos Sistemas Governamentais**

  O governo presume que todas as informações corporativas coletadas, mantidas e processadas pelo Estado possuem algum valor. Como nenhuma das informações, serviços ou sistemas possuem valor ou sensibilidade de mesmo peso para o Estado, eles precisam estar agrupados e protegidos em níveis diferentes de segurança. Cada nível de segurança, classificado como Alto, Médio e Baixo deve proteger a confidencialidade, integridade e disponibilidade das informações tratadas pelos diversos sistemas e serviços computacionais do Estado.

  O passo inicial é o mapeamento das exigências de segurança de todos os sistemas governamentais, em âmbito estadual, tratados nos diversos órgãos/entidades do governo, dando ênfase nas informações de maior importância. Este mapeamento deve ser atualizado periodicamente.

  Todas as informações agrupadas em bases de dados, redes locais, serviços críticos, sistemas corporativos dos órgãos/entidades da rede pública estadual devem ser agrupados com nível de segurança proporcional ao risco e a magnitude do dano resultante da perda, mau uso, exposição, ou modificação da informação contida em tais sistemas governamentais.

  Sistemas de informação, serviços, redes locais ou base de dados agrupados com nível de sensibilidade Alto devem possuir designação de salvaguarda mais precisa. Sistemas governamentais agrupados no nível mais baixo geralmente exigem somente as precauções mínimas de segurança.

  Sistemas integrados possuindo informações com níveis de sensibilidade diferentes devem ser tratados considerando-se o maior nível de segurança exigido.

Documentos Relacionados

- ANÁLISE GLOBAL DE SEGURANÇA DA REDE GOVERNAMENTAL E NECESSIDADE DE SEGMENTAÇÃO DE DADOS E SERVIÇOS.
- Política de Classificação das Informações e Sistemas Governamental.

6. Proteção dos Domínios de Segurança (Necessidade Atual de Segurança)

DOMINIO 01: Proteção dos Serviços e Dispositivos da Rede Governamental

O "Projeto de Segurança da Rede Governamental" é a principal ferramenta para definir e implantar a segurança necessária para cada um dos serviços e dos dispositivos. Após a aprovação, deve-se garantir que esse projeto será implementado sem falhas.

Cada serviço ou dispositivo pertencente à Rede Governamental deverá estar formalmente associado a um administrador do órgão/entidade, do provedor de serviço ou de empresa terceirizada com obrigações administrativas sobre este.

A medida em que novos serviços ou dispositivos forem incluídos na rede, os administradores responsáveis por tais componentes devem receber treinamento adequado de manutenção antes da instalação.

Ferramentas de investigação serão usadas periodicamente por profissionais designados pela Administração de Segurança de TI Estadual, com base no programa de gerenciamento, para determinar se novas vulnerabilidades estão presentes nos dispositivos e serviços da rede, e os relatórios serão enviados para os administradores dos dispositivos ou serviços específicos para que ações corretivas sejam tomadas.

Todos os serviços e dispositivos na Rede Governamental ser classificados e associados ao grau de criticidade "Baixo, Médio ou Alto". Os serviços mais sensíveis devem seguir as recomendações da Política de Sistemas Governamentais e os dispositivos mais críticos devem seguir as recomendações de segurança dos fabricantes.

- **Políticas e Recomendações de Segurança**

  A Política de Sistemas Governamentais da Rede Governamental deve informar a periodicidade de verificação de vulnerabilidades dos dispositivos e de correção das mesmas.

  Toda a metodologia de trabalho e as ferramentas utilizadas devem estar descritas na política de Sistemas Governamentais, que conterá todas as ações, responsabilidades e cronograma de atividades a serem implementadas e executadas metodicamente para garantir o nível de

segurança aceitável para cada serviço e dispositivo da Rede Governamental.

Cada dispositivo, sistema operacional ou serviço utilizado na Rede Governamental deve seguir orientações de verificação e correções de segurança dos fabricantes.

DOMINIO 02: Proteção das Redes de Dados dos Órgãos e Entidades

Independente de sua classificação, toda rede de dados de órgãos/entidades conectados à Rede Governamental necessariamente devem seguir a determinação abaixo.

- **Determinação básica de Segurança para todos os órgãos/entidades conectados à Rede Governamental**

Todos os órgãos/entidades conectados à Rede Governamental, que utilizam a estrutura do Núcleo de Facilidades, devem seguir as linhas básicas de segurança que estabelecem:

1- Um *Firewall* deverá ser implementado (Instalação do sistema e configuração de regras que permitam a passagem somente dos protocolos/serviços necessários para as necessidades de cada órgão/entidade) e mantido em todos os segmentos de redes não controladas diretamente pela gerência da Rede Governamental, atualmente representada pela SEAD.

2- Toda rede deverá possuir um sistema de Detecção de Intrusos (IDS) implementado e mantido no ambiente protegido por cada *Firewall*. O sistema deve ser capaz de emitir alertas sobre tentativas de intrusão 24 horas por dia, 7 dias por semana, para os devidos responsáveis e reportados para o Administrador de Segurança de TI Estadual, caso ocorra algum incidente de segurança que envolva outro órgão/entidade.

3- Toda rede deverá ter configurado um dispositivo para controle de acesso aos usuários (*proxy*), baseado em autenticação e capacidade básica de filtrar conteúdo, além da capacidade de emitir relatórios de utilização que auxiliem os administradores a coibir abusos.

4- Toda rede deverá possuir um sistema de antivírus instalado e atualizado constantemente para prevenir que códigos maliciosos se espalhem no interior da rede e para as demais redes do governo.

Esta determinação deve ser seguida pelos órgãos/entidades e unidades remotas destes que possuem um número de máquinas maior ou igual a X (determinar esse número) ou que contenha dados críticos (rede de dados classificada como nível médio ou alto). Para o caso de unidades remotas com um número inferior ao especificado nessa determinação e que sua rede de dados esteja classificada como nível baixo, o órgão/entidade deverá prover a segurança necessária. Caso ocorra algum incidente que afete a Rede Governamental, o órgão/entidade será responsabilizado.

- **Redes de Dados classificadas com o nível Alto**

  As redes de dados classificadas com nível Alto devem manter especialistas em segurança da informação para desenvolver projetos na área de segurança, com objetivos de criar uma Política de Segurança projetada e implantada especificamente para o ambiente singular de cada órgão/entidade, corrigir todas as vulnerabilidades de serviços, sistemas e dispositivos internos e implementar mecanismos de segurança para a proteção das informações dos respectivos órgãos/entidades podendo seguir o modelo do projeto realizado na rede interna da SEAD.

- **Redes de Dados classificadas com nível Médio e Baixo**

  As redes de dados classificadas com nível Médio e Baixo devem pelo menos seguir as recomendações básicas de segurança determinada como recomendação de segurança aos órgãos/entidades.

- **Política de Segurança Local**

  Cada órgão/entidade precisa definir sua política de segurança local. A SEAD definiu políticas de segurança locais que poderão servir de modelo e serem adaptados para a realidade de segurança local de cada órgão/entidade. Fica sob responsabilidade dos órgãos/entidades a adaptação das Políticas de Segurança.

- **Documentos Relacionados**

  Políticas Locais da SEAD;

  Fases de um projeto de Segurança.

DOMINIO 03: Proteção da Comunicação de Informações na Rede Governamental

- **Política de Interconexão de Recursos de TI**

  A segurança de toda e qualquer comunicação de informações dentro da Rede Governamental precisa ser previamente analisada e a determinação da segurança necessária para tal comunicação deve ser formalizada e implantada para que seus objetivos sejam cumpridos com o nível de segurança mínimo aceitável, de forma a não comprometer serviços e troca de dados dependentes de tais comunicações.

  Todas as regras e ações neste contexto devem seguir padrões de segurança cuidadosamente analisados, planejados e documentados de acordo com a Política de Interconexão de Recursos de TI.

  Um Memorando de Entendimento (ME) e um Acordo de Segurança da Interconexão (ASI) deverão ser desenvolvidos para todas as interconexões que prevejam troca de informações com nível de classificação Alto, que deverá ser assinado pelo dirigente de cada instituição proprietária da rede que faz parte do grupo de entidades que irão comunicar-se através da Rede Governamental. O ME detalhará as razões pelo qual a interconexão está sendo implementada, e o ASI registrará os riscos associados e os controles necessários para atenuação dos riscos, assim como as condições pelas quais aquela interconexão poderá deixar de existir.

  O ME será criado pelos administradores da rede do órgão/entidade estadual com o apoio das partes interessadas na comunicação, que deverão validar em conjunto o conteúdo do ME e certificar a implantação.

  A finalização deste processo é marcada pela implantação dos mecanismos determinados e registro sobre a comunicação de dados, do ME e do ASI em meio eletrônico.

- **Documento Relacionado**

  Política de Interconexão de Recursos de TI.

DOMINIO 04: Proteção dos Sistemas de Informação Estadual e de Informações Públicas Sensíveis

- **Plano de Segurança do Sistema**

  Todas as salvaguardas de segurança necessárias devem ser designadas para proteger cada sistema e estar devidamente documentadas no Plano de Segurança do Sistema.

Para que seja possível determinar as salvaguardas necessárias para cada sistema, é necessário que sejam realizados: (1) um plano de segurança de sistemas, (2) acompanhado de uma análise de riscos efetiva, (3) seguida de certificação da implementação das salvaguardas de segurança exigidas.

Reformular esse parágrafo e colocar o plano de segurança no de baixo eliminando este.

- **Política de Segurança de Sistemas Corporativos**

  Deve ser criada uma política de segurança que contenha as designações de salvaguardas para os sistemas corporativos capaz de determinar as ações, responsabilidades e tarefas a serem executadas metodicamente, a fim de garantir o nível de segurança designado para cada sistema corporativo.

  O plano de Segurança de cada sistema deve ser desenvolvido pelo administrador ou responsável pelo sistema com o apoio do supervisor de segurança. Ao final do processo, o administrador de Segurança de TI estadual deve certificar o plano criado e registrá-lo em meio magnético para que possa ser auditado futuramente.

- **Documento Relacionado**

  Política de Sistemas Governamentais.

<u>DOMINIO 05:</u> Proteção do Uso Adequado dos Serviços da rede Governamental

- **Política de uso Aceitável dos Serviços da Rede Governamental**

  Esta Política definirá como os serviços oferecidos pela Rede Governamental devem ser utilizados, especificando quais serviços e ações são permitidas dentro dos seus limites.

- **Documento Relacionado**

  Política de Uso Aceitável dos Serviços da Rede.

ADMINISTRAÇÃO DE SEGURANÇA DA REDE GOVERNAMENTAL

7. Modelo de Administração

Cada órgão/entidade possuirá o seu próprio modelo de administração de segurança, que deve definir como a segurança da rede local, dos sistemas, das informações e infra-estrutura do órgão/entidade será administrada. Cada setorial colaborará diretamente com a Administração de Segurança de TI Estadual.

A segurança da Rede Governamental, dos sistemas de informação de maior interesse estadual e da infra-estrutura corporativa da rede será administrada em um ponto central localizado na Secretaria da Administração do Estado do Ceará, como apresentado na figura 3.

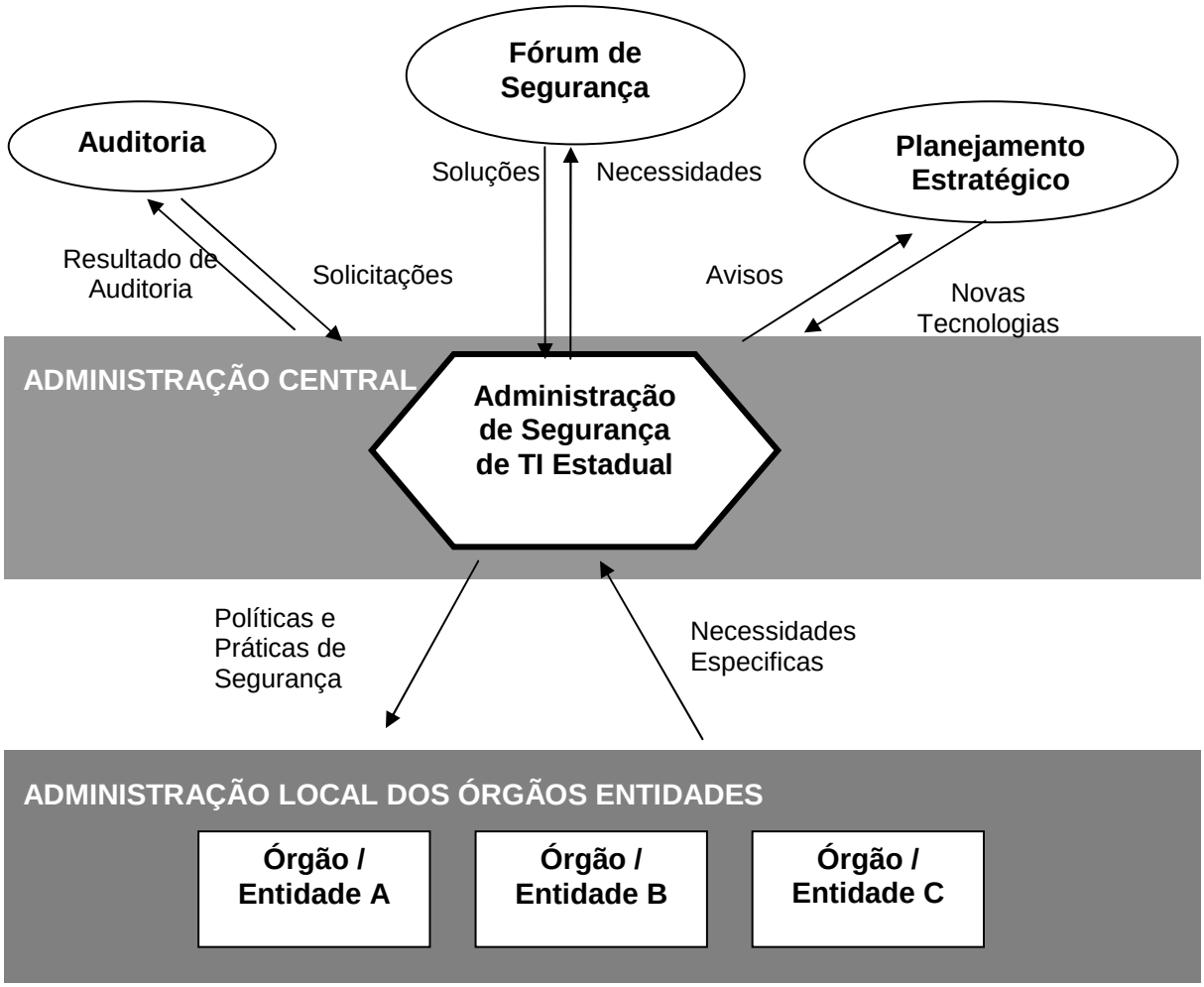


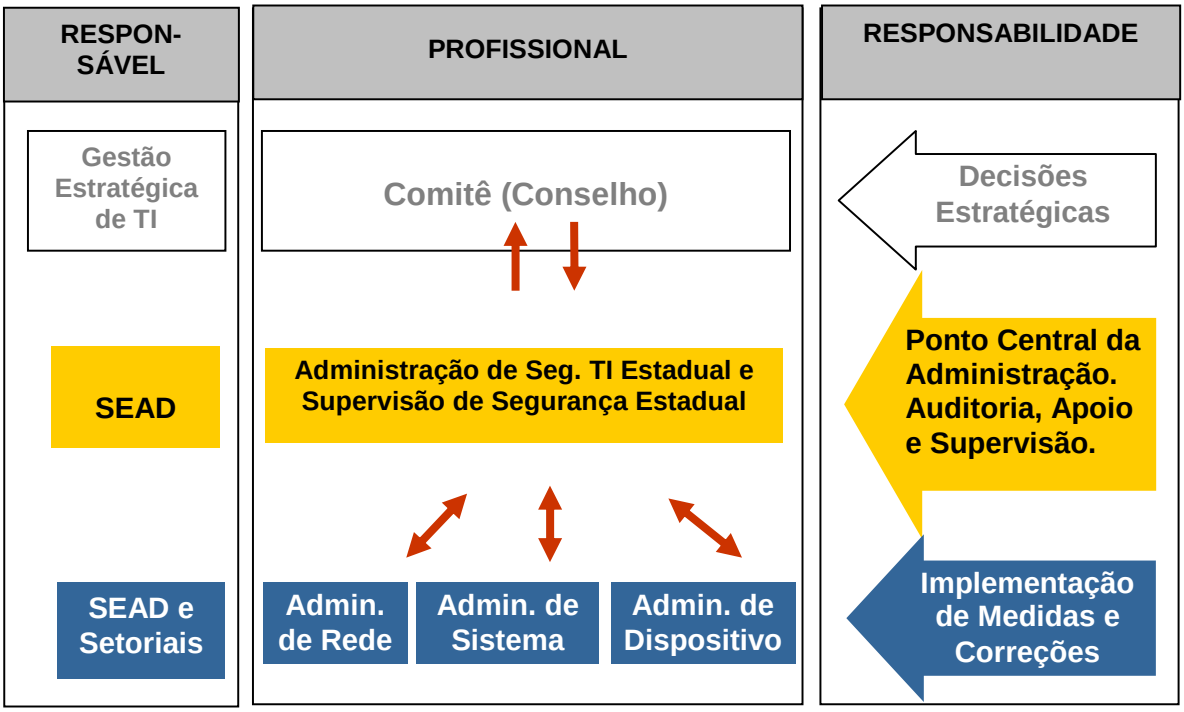
Figura 3

A Administração de Segurança de TI Estadual deverá responsabilizar-se pela coordenação das medidas e normas necessárias relacionadas com a segurança da Rede Governamental, interagindo e ajudando os órgãos/entidades na implantação de suas políticas locais, integração e concordância com a Política da Rede Governamental.

8. Infra-estrutura da Administração Central da Segurança da Rede Governamental

8.1 Estrutura de Pessoal

A estrutura da Administração de Segurança de TI Estadual é fortemente dependente dos profissionais envolvidos com a execução das tarefas previamente planejadas e descritas, por isso o Governo do Estado do Ceará deverá instituir uma entidade ou departamento, no órgão responsável pela administração da Rede Governamental que irá exercer gestão, acompanhamento, auditoria e gerência sobre a certificação e reconhecimento do atendimento pelos órgãos/entidades governamentais dos padrões de segurança definidos na política de segurança para a Rede Governamental e possuirá a seguinte estrutura:



- **Administrador de rede e dispositivo:** Profissional com responsabilidade de administrar determinados dispositivos e serviços da rede. O administrador de redes e dispositivos será responsável por instalar, administrar e garantir a manutenção adequada do dispositivo ou rede de dados sob sua responsabilidade, assim como instalar e configurar *softwares* residentes nestes componentes.

- **Supervisor de segurança:** Um profissional responsável pela garantia e implementação da política de segurança da informação. Será responsável por desenvolver todas as atividades relacionadas à

auditoria, acompanhamento e revisão de segurança, incluindo a configuração dos componentes de auditoria, execução e análise.

- **Administrador de Segurança de Tecnologia da Informação Estadual:** Profissional responsável pela conformidade corporativa com a política de segurança, incluindo o apoio de suporte executivo e do Comitê de Segurança de TI Estadual para o programa de gerenciamento de riscos de sistemas de informação.

- **Comitê de Segurança de TI Estadual:** A Administração de Segurança de TI Estadual deverá construir um comitê de segurança. Este comitê deverá incluir um representante sênior de todos os órgãos/entidades usuários ou não da Rede Governamental. A Comissão irá informar o Comitê de Segurança de TI Estadual sobre assuntos relacionados ao gerenciamento de riscos da política e irá aprovar e projetar modificações na política para serem adotados pelo Estado do Ceará.

A separação de obrigações e responsabilidades das pessoas envolvidas é um conceito muito importante no gerenciamento da segurança da Rede Governamental. Em geral, quanto maior a organização, maior deve ser a formalidade desta separação. O objetivo é impor responsabilidade de ações em indivíduos chaves e minimizar a função individual no programa como um todo.

Todos os profissionais serão formalmente nomeados para desempenhar as atividades que eles serão responsáveis.

8.2 Ambiente de Trabalho

Para garantir o funcionamento adequado deste modelo de segurança, é necessário que exista um ambiente de produtividade específico para esta finalidade de forma a garantir a exigüidade do modelo.

Este ambiente deve:

- Ser exclusivo para o desenvolvimento desta atividade (dos profissionais envolvidos com a segurança de Rede Governamental – Administrador de segurança, supervisor, etc.),
- Possuir recursos computacionais com as ferramentas de apoio e *softwares* de gerenciamento, supervisão e controle de segurança.
- Os participantes deste ambiente deverão executar as tarefas de gerenciamento da segurança da rede, auditoria de segurança, resposta a incidentes, elaboração e manutenção do plano de contingência, notificação de incidentes, verificação do cumprimento

das políticas estabelecidas por parte dos órgãos/entidades que se interconectam através da Rede Governamental, dentre outras.

8.3. Ferramentas de Apoio

Através das ferramentas abaixo listadas, a administração central de segurança vai fazer a gerência da comunicação entre os profissionais participantes do projeto.

- **Website de Segurança**

  É um site restrito apenas aos órgãos/entidades conectados à Rede Governamental para comunicação das políticas, soluções, normas e avisos da administração Central da Segurança estadual, contendo fórum para discussão das questões técnicas.

- **Sistema de Acompanhamento de Segurança**

  É um sistema restrito apenas aos profissionais integrantes da administração central da Rede Governamental que faz a gerência de comunicação de todas as atividades relacionadas à segurança desta e dos chamados solicitados pelos administradores de rede dos órgãos/entidades.

  Todos os documentos de soluções adotadas que forem de caráter restrito serão mantidos neste sistema, por causa do sistema de controle de usuários do mesmo.

9. Capacitação do Pessoal Envolvido

A Capacitação dos participantes da estrutura organizacional da administração central de segurança responsável pela execução da política é um fator preponderante para o sucesso desta política, onde cada membro desta administração deverá receber treinamento sobre o funcionamento da política de segurança global e sobre a realização de suas tarefas especificas.

Para isto, deve ser elaborado um plano de capacitação contemplando atualização periódica de todos os envolvidos. A capacitação periódica dos participantes da estrutura organizacional da administração de segurança deverá envolver cursos e treinamentos nas áreas de segurança de rede, segurança de banco de dados, criptografia, segurança de sistemas operacionais, segurança de aplicações web além de participação em fóruns e listas de discussões para que os profissionais possam se manter sempre atualizados.

10. Estrutura para Resposta a Incidentes de Segurança

A administração de Segurança de TI Estadual tem a responsabilidade de desenvolver e implementar procedimentos de relato de incidentes de segurança, através de um *checklist* de todos os procedimentos necessários para manter a Rede Governamental segura. Também deverá manter uma equipe sempre preparada para atender aos incidentes de segurança que possam vir a ocorrer, realizando atividades tais como:

1. Investigação de anomalias quando necessário;
2. Investigação, coordenação, relatos e *follow-up* (acompanhamento) de possíveis incidentes de segurança.

- **Procedimentos**

  Procedimentos de resposta a incidentes de segurança serão definidos e publicados a todos os administradores de sistemas e redes para os domínios de comunicação de redes, sistemas corporativos e serviços críticos. O escopo e funcionamento de tais procedimentos serão tratados em treinamentos de segurança específicos.

- **Equipe de Resposta**

  Uma equipe governamental de resposta a incidentes deve ser constituída por membros da consultoria em segurança e membros da estrutura da Rede Governamental preparados para iniciar uma investigação imediatamente no momento de uma suspeita de segurança.

Tempo de Resposta

Atendimento	Descrição	Resposta
Suporte Crítico:	Chamados oriundos de problemas afetando a segurança, suspeita de invasões à rede ou parada da rede ocasionadas por mecanismos de segurança, tais como, *Firewall* e outros.	Até 02hs
Suporte não Crítico:	Chamados oriundos de problemas que não ocasionam a parada das atividades da rede nem comprometem a integridade e segurança dos dados.	Até 08hs
Apoio a Decisões:	Chamados para apoio a tomada de decisões da Administração de Segurança de TI Estadual, envolvendo a rede e segurança dos dados.	Até 24hs

- **Criação da Política de Resposta Emergencial a Incidentes**

  Os procedimentos de resposta a incidentes deverão ser desenvolvidos ao final da fase de implantação do Projeto de Segurança inicial, através de técnicas publicadas e aprovadas por instituições de contingência de segurança, para atender as medidas de contingência. Tais procedimentos deverão estar descritos na política de contingência, devidamente documentados e constantemente atualizados mediante modificação desta Política.

11. Administração das Necessidades Futuras de Segurança

As necessidades futuras de segurança da Rede Governamental estão relacionadas à atualização dos procedimentos de segurança e à aplicação e atualização das políticas de segurança.

11.1 Manter a Segurança da Rede Governamental

Manter a segurança da Rede Governamental depende de um processo de conscientização dos administradores de rede e usuários de sistemas corporativos, da implantação e revisão contínua das políticas de segurança estabelecidas com a possível introdução de novas regras a serem seguidas e do acompanhamento contínuo deste plano diretor e seus documentos relacionados.

- **Segurança dos Serviços e Dispositivos da Rede**

  Depois de certificado, todo sistema de segurança necessita de vigilância dobrada pela grande quantidade de vulnerabilidades que surgem para seus componentes em curto espaço de tempo. Tal vigilância será conseguida através do acompanhamento e do monitoramento das vulnerabilidades da rede.

- **Segurança das Redes de Dados dos Órgãos/Entidades**

  Todo órgão/entidade deve responsabilizar-se pela manutenção dos seus sistemas de proteção de rede, seja através de consultoria especializada para esta finalidade ou através da equipe de informática interna de cada órgão/entidade.

  As auditorias e revisões irão verificar a existência de possíveis falhas nestes ambientes que devem ser corrigidas com prazo pré-determinado mediante a gravidade do problema.

- **Segurança do Serviço de Comunicação de Informações entre Entidades**

  Todo ME deve ser revisado, reavaliado e recertificado periodicamente (verificar na Política de Interconexão) para garantir que todas as interconexões estabelecidas mantém-se seguras e com ME atualizados. O supervisor de segurança deve ser responsável por esta revisão periódica com apoio dos administradores de rede e com a utilização das ferramentas disponíveis.

- **Segurança dos Sistemas Corporativos e Serviços da Rede Governamental**

  Periodicamente, o plano de segurança destes sistemas e serviços serão auditados e as recomendações de segurança serão enviadas para que os administradores de sistemas providenciem as correções no prazo pré-estabelecido de acordo com o grau do risco da vulnerabilidade encontrada.

- **Capacitação de todo pessoal envolvido**

  O Administrador de Segurança de TI Estadual deve estabelecer um programa de treinamento pró-ativo específico para todos os membros da administração de segurança que pertence à Rede Governamental.

  A consultoria especializada em segurança será responsável por manter toda a equipe atualizada em relação a novos procedimentos

de administração de segurança, reciclagem dos profissionais e transferência tecnológica.

O treinamento de todo pessoal será acompanhado e reportado para o Administrador de Segurança Estadual a fim de manter a conformidade da política de segurança estadual.

11.2 Garantir a Segurança do Governo Eletrônico

Futuramente, com o crescimento da visão estadual de compartilhamento de informações entre órgãos/entidades e consultas centrais e distribuídas em todos os órgãos/entidades, será necessário proteger as transações entre os diversos bancos de dados mantidos pelos órgãos/entidades estaduais com a devida garantia de confidencialidade, integridade e não repúdio de tais transações dentro do perímetro de segurança ao qual estas entidades participam e disponibilizar o resultado de tais consultas, que originaram a transação, com a segurança adequada ao solicitante. Para que seja possível tal implementação, primeiramente é necessário que os propósitos atuais de segurança da Rede Governamental estejam devidamente implantados.

ANEXO I

PLANO DE AÇÕES DA REDE GOVERNAMENTAL

Todas as ações relacionadas a implantação deste plano estão devidamente listadas no quadro abaixo: