Segurança da Informação

Fundamentos do Modelo de Segurança da Informação

MINISTÉRIO DO PLANEJAMENTO

GOVERNO FEDERAL
Trabalhando em todo o Brasil

A Segurança da Informação no Governo Federal

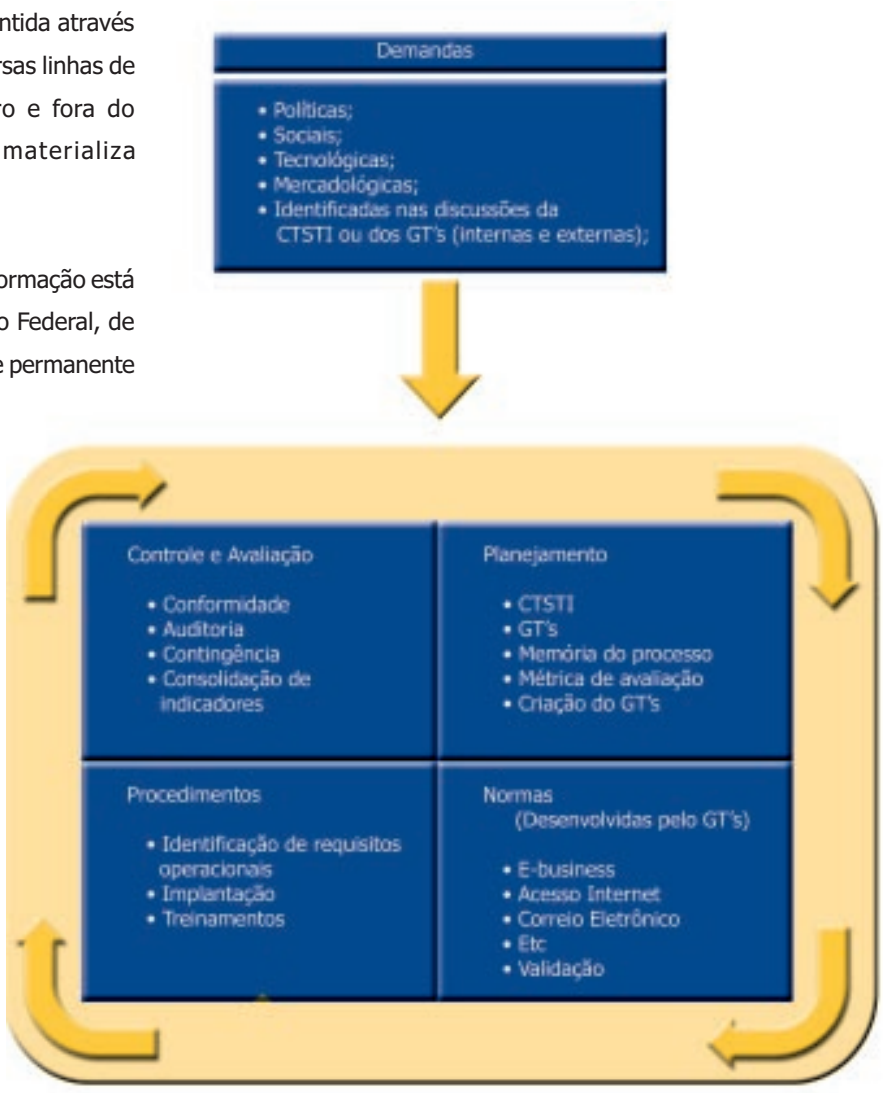
O Governo Federal, em diversas oportunidades, tem se manifestado no sentido de assegurar a proteção da informação sob sua guarda e aquelas de interesse do cidadão. É fundamental garantir o direito dos cidadãos à privacidade, além do direito à consulta sobre os dados coletados nos sistemas governamentais, previstos na Constituição. Os websites públicos devem comprometer-se a garantir a confiabilidade das informações de caráter pessoal que são armazenadas em suas bases de dados, sejam elas relativas aos usuários ou pessoas que compõem a administração pública.

A distribuição da massa informacional garantida através de mecanismos de segurança para as diversas linhas de aplicação e suporte às atividades dentro e fora do governo, é uma diretriz que se materializa gradativamente.

Desta forma, a questão da segurança da informação está sendo reposicionada no âmbito do Governo Federal, de modo a receber um tratamento destacado e permanente por meio do estabelecimento da "Política de Segurança da Informação nos órgãos do Poder Executivo Federal – PSIPE".

Caberá à Secretaria-Executiva do Conselho de Defesa Nacional - SECDN, órgão vinculado ao Gabinete de Segurança Institucional da Presidência da República, assessorada pelo Comitê Gestor da Segurança da Informação – CGSI, propor as diretrizes para a implementação da Política no contexto do Poder Executivo Federal. O Governo Federal desenvolverá a PSIPE de acordo com as diretrizes do Comitê e contará com o apoio técnico/operacional da Câmara Técnica de Segurança da Tecnologia da Informação – CT-STI/SISP.

Por sua vez, a Secretaria de Logística e Tecnologia da Informação – SLTI do Ministério do Planejamento, Orçamento e Gestão, exercerá um papel preponderante na implementação da PSIPE, considerando que a mesma tem entre as suas atribuições a competência de coordenar as atividades do Sistema de Administração de Recursos de Informação e Informática – SISP, propondo políticas, diretrizes e normas de Informação e Informática, no âmbito da Administração Pública Federa direta, autárquica e fundacional. A dinâmica operacional da Câmara Técnica será cíclica conforme detalhamento da figura abaixo:



O Modelo de Segurança da Informação - MSI

Existe uma complexidade no estabelecimento de parâmetros que sirvam de subsídio para a afirmação de que um ambiente de informação é seguro. É importante a identificação das conseqüências relacionadas às vulnerabilidades do tratamento da informação, da compreensão dos diversos ambientes de contexto governamental e da adoção de um modelo de segurança que possa minimizar tais conseqüências.

Considerando estes aspectos, as ameaças à segurança da informação se concentram em dois pontos: as vulnerabilidades existentes nos ambientes onde a informação é processada, armazenada ou transmitida e as ameaças externas e internas à segurança da informação nestes ambientes, incluindo vulnerabilidades de aplicações, banco de dados, rede, sistemas operacionais e serviços.

A modelagem da segurança, nas suas diversas formas, é um dos componente que influi na credibilidade de um sistema de computadores, conectado ou não em rede. Esta, sob um contexto mais amplo, propõe um maior controle sobre os ativos de informação, assim como sobre os serviços disponibilizados pelas diversas áreas do Governo. Torna mais tangível a avaliação da qualidade dos serviços e a responsabilização sobre o uso indevido ou a má administração de tais recursos.

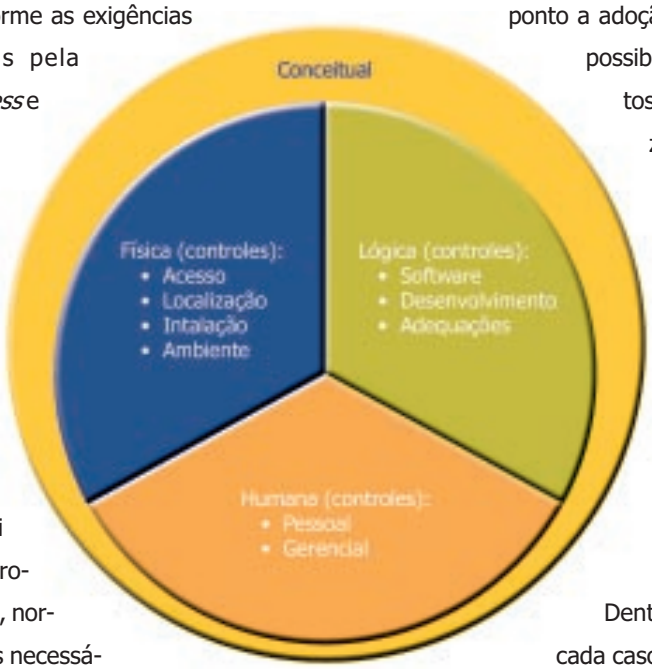
O modelo inclui as fases de avaliação, projeto, implementação, gerenciamento, suporte, treinamento e conscientização em segurança da informação, nos seus processos e produtos.

É possível perceber questões fundamentais a serem solucionadas no desenvolvimento do modelo de segurança. Entre estas pode-se identificar a maximização do uso coerente e seguro dos recursos e a proteção dos ativos de informação contra roubo, vandalismo e de políticas

Nesta metodologia, usada no processo de modelagem, a segurança é considerada sob os seguintes aspectos:

- **Ataques à segurança**
  Qualquer ação que comprometa a segurança da informação governamental;
- **Mecanismos de segurança**
  Qualquer mecanismo utilizado para a detecção, prevenção ou recuperação de danos causados pelos ataques à segurança;
- **Serviços de segurança**
  Qualquer serviço que garanta a segurança dos sistemas de processamento de dados e as informação que trafegam nas redes. O objetivo dos serviços de segurança é a contenção dos ataques à segurança. A implantação destes serviços pode ocorrer a partir da implementação de um ou mais mecanismos de segurança.

para tratamento de ataques, visando a manutenção da segurança. As fases deste ciclo serão avaliadas e revistas periodicamente, considerando as normas e procedimento envolvidos, conforme as exigências tecnológicas impostas pela estruturação do *e-business* e do *e-commerce*, ou qualquer outro tipo de transação envolvendo interações eletrônicas.



O modelo de segurança da informação ultrapassa os limites da segurança das redes de computadores. Ele inclui um amplo conjunto de procedimentos, mecanismos, normas, diretrizes e políticas necessárias a salvaguarda da informação governamental, incluindo assim, todas as informações em processamento, em trafego nas redes de computadores, armazenadas em meios magnéticos, e aquelas sob guarda do Governo. Cada área considerada pelo modelo será tratada sob os aspectos conceituais, físicos, lógicos e de recursos humanos.

O dimensionamento e a satisfação das necessidades de segurança de cada órgão ou entidade, convergem para a avaliação de processos e produtos relacionados. Nesta ponto a adoção de uma metodologia que possibilita a definição dos requisitos de segurança e a caracterização das ações a serem tomadas na implantação ou adequação de processos e produtos é fundamental. Nesta fase são identificadas as correlações de fatores para a implantação dos elementos de segurança mais adequados a cada ambiente.

Dentro do dimensionamento de cada caso específico, o MSI considera o balanceamento de três fatores críticos:

- A probabilidade de sucesso dos ataques às vulnerabilidades do ambiente;
- O custo envolvido em um ataque, incluindo a recuperação dos processos organizacionais e dos serviços envolvidos;
- E o custo de prevenção contra possíveis ataques.

Princípios

Os serviços de segurança podem ser caracterizados segundo os seguintes princípios:

• Disponibilidade

Uma grande variedade de ataques pode resultar na perda ou redução da disponibilidade da informação. Alguns desses ataques são compensados através de medidas automatizadas, como a autenticação e a criptografia, ao passo que já outros requerem algum tipo de ação física para a prevenção ou recuperação das perdas de disponibilidade de elementos de um sistema distribuído.

• Integridade

O serviço de integridade, pode ser aplicado a todo um fluxo de mensagens de uma conexão, a uma única mensagem ou a determinados campos desta mensagem. Uma conexão que tenha este princípio implantado garante que as mensagens serão recebidas como foram enviadas, sem duplicação, inserção indevida, modificação, sem reordenação ou repetições. A destruição de dados

também é tratada neste serviço. Sob outro foco, este serviço trata tanto da modificação da mensagem como da negação de serviços. É possível fazer uma distinção entre o serviço com e sem recuperação. Porque o serviço de integridade trata de **ataques ativos**, a atenção se concentra na detecção ao invés da prevenção. Caso uma violação de integridade seja detectada, então o serviço pode simplesmente informar esta violação, de forma que uma outra parte do *software* ou algum tipo de intervenção humana seja necessária para a recuperação de tal violação. De forma alternativa, existem mecanismos disponíveis para a recuperação de perda de integridade de dados. Esta última alternativa é a mais atraente.

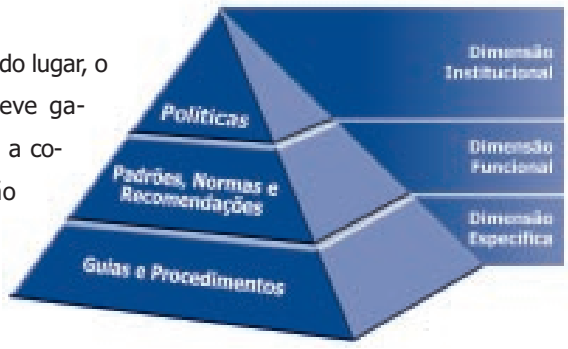
• Confidencialidade

A confidencialidade é a proteção da informações contra **ataques passivos** e análise de mensagens, quando em trânsito nas redes ou contra a divulgação indevida da informação, quando sob guarda. Com respeito à utilização indevida de conteúdos de mensagens, pode-se identificar diversos níveis de proteção para cada tipo de informação identificado. Podem ser definidos diversas formas para este serviços, incluindo a proteção de mensagens individuais ou até mesmo de campos dentro desta mensagem. Este processo de identificação e refinamento daquilo que realmente deve ser protegido é bastante complexo e se reflete em toda a estrutura de segurança adotada.

• Autenticidade

O serviço de autenticação se relaciona com a garantia de que a comunicação é autentica. No caso de uma simples mensagem, como é o caso de um sinal de alarme, a função da autenticação é garantir ao receptor que a mensagem é realmente originária da fonte informada. No caso de uma interação em tempo real, como a conexão de um computador com outro, pode-se considerar dois aspectos, o primeiro no momento da inicialização da conexão, este serviço deve garantir que as duas entidades são autenticas, ou seja que são quem alegam ser.

A divisão básica do MSI considera as dimensões institucional, funcional e específica.



Em segundo lugar, o serviço deve garantir que a comunicação deve ocorrer de forma que não seja possível a uma terceira parte se disfarçar e se passar por uma das partes já autenticadas na inicialização da conexão para conseguir transmitir e receber mensagens de forma autorizada.

Outros Serviços

Como serviços derivados dos princípios de segurança anteriormente citados , podemos identificar:

• Não Repúdio

Este serviço previne tanto o emissor contra o receptor, quanto previne contra a negação de uma mensagem transmitida. Desta forma, quando uma mensagem é enviada, o receptor pode provar que de fato a mensagem foi enviada pelo emissor em questão. De forma similar, quando uma mensagem é recebida, o emissor pode provar que a mensagem foi realmente recebida pelo receptor em questão.

• Controle de Acesso

No contexto de segurança de rede, o controle de acesso é a habilidade de limitar ou controlar o acesso aos computadores hospedeiros ou aplicações através dos enlaces de comunicação e do controle de acesso físico. Para tal, cada entidade que precisa obter acesso ao recurso, deve primeiramente ser identificada, ou autenticada e de forma a que os direitos e permissões de acesso sejam atribuídos ao usuário.

Estratégias Operacionais

Estratégia de Segurança da Informação - SISP *

- **Acesso Livre**
- **Modelagem dos Processos de Segurança**
- **Avaliação e Conformidade de Produtos de Segurança**

Modelagem dos processos de segurança

- Modelo de segurança e seu objetivo
- Modelagem da segurança física
- Modelagem da segurança lógica
- Modelagem da segurança humana
- Modelagem do fluxo de informação
- Políticas de classificação da informação
- Definição de níveis de segurança
- Identificação do conteúdo do modelo de segurança
- Apresentação do modelo para avaliação e implantação
- Modelagem da integração
- Políticas e objetivos
- Modelo de Plano de Contingência
- Modelo de Auditoria

Dimensão

Institucional
Funcional
Específica

Dimensionamento Organizacional

- Análise Orçamentária
- Análise de Risco
- Análise de Vulnerabilidade
- Políticas de Utilização do Ambiente
- Estratégia de Autenticação
- Estratégia de Serviços Confiáveis (Creditação)
- Estratégia de Confidencialidade (Privacidade)
- Estratégia de Segurança nas Transações de Negócios/e-business
- Requisitos de Segurança na Rede de Defesa
- Detalhamentos para Implementação
- Procedimentos de Auditoria

(*) Ainda em discussão na Câmara Técnica, o MSI deve orientar-se por este detalhamento.

Ministro do Planejamento, Orçamento e Gestão
Martus Antônio Rodrigues Tavares

Secretário-Executivo
Guilherme Gomes Dias

Secretário de Logística e Tecnologia da Informação
Solon Lemos Pinto

Diretor do Departamento de Serviços de Rede
Alexandre Machado Santana

Elaboração:

Pedro Paulo Lemos Machado
Ernandes Lopes Bezerra
José Ney de Oliveira Lima

Edição:

Marden Elias

Programação Visual:

Kenia Ribeiro e Ricardo Wagner

Para obter outras informações, entre em contato com:

Ministério do Planejamento, Orçamento e Gestão
Secretaria de Logística e Tecnologia da Informação - SLTI
Câmara Técnica de Segurança da Tecnologia da Informação - CT - STI
Tel.: (61) 313-1433 / 313-1400
Fax.: (61) 322-1393

Gerência de Projetos de Segurança da Informação
Tel.: (61) 313-1216
Fax.: (61) 322-3622

site: www.redegoverno.gov.br
e-mail: ctsti@planejamento.gov.br

Agosto de 2000
Brasília - Distrito Federal


e-gov
edições