Ministério do Planejamento Orçamento e Gestão
Secretaria de Logística e Tecnologia da Informação
Departamento de Serviços de Rede
Coordenação de Segurança da Informação

Guia de Referencia para a Segurança da Informação

Usuário Final

Introdução

O presente guia tem como objetivo a criação de um instrumento de referência para a implantação de um ambiente informacional mais seguro nos órgão e instituições públicas, facilitando desta forma os processos de gestão e controle. A segurança da informação tende a se tornar um tema permanente na agenda de atividades do Fórum de CGMIs, instituído pelo Decreto Nº 1048/94 que estabelece o sistema de informação e informática, no qual questões estratégicas da área de Tecnologia da Informação – TI, são tratadas e discutidas de maneira a aprimorar os mecanismos de gestão governamental, visando a melhoria continua da qualidade dos processos internos e serviços prestados ao cidadão.

Questões relacionadas com segurança da informação devem ser tratadas como tema sensível nas organizações governamentais.

Observa-se atualmente um grande desnível cultural e tecnológico entre os órgãos que formam a Administração Pública Federal – APF.

Com o objetivo de promover e motivar a criação de uma cultura de segurança da informação, na dimensão de usuário final é proposto o presente guia de referencia. De maneira complementar serão desenvolvidos dois guias adicionais cuja abrangência será a dimensão técnica e a gerencial.

O objetivo deste guia, é que ele sirva como referencia, na área de segurança da informação, para as unidades responsáveis pela gestão de TI, nos órgãos e instituições publicas que formam a APF. A dimensão considerada é a de usuário final. Estas entidades públicas poderão desenvolver guias de melhores práticas, considerando o seu contexto de atuação e observando sempre o disposto na legislação vigente, bem como nos padrões de interoperabilidade do Governo Eletrônico e-PING.

Como é um guia relacionado com uma área tecnológica bem definida, segurança da informação, é importante que o mesmo seja revisto anualmente, sob a coordenação

do MPOG/SLTI/DSR/Coordenação de Segurança da Informação, com vista a sua atualização, adequação tecnológica e legal.

Utilizando a idéia da criação de uma ampla rede de colaboradores, torna-se possível a criação, dentro deste ambiente cooperativo, de grupos técnicos temáticos na área de segurança, sob demanda, com total envolvimento institucional. Estes grupos poderão interagir com outras ações em andamento na APF, evitando o re-trabalho e promovendo a racionalização de gastos nesta área.

1. Fundamentos e Conceitos de Política de Segurança

Para a implementação de controles de segurança faz-se necessária a criação de um processo de gestão da segurança da informação. Este processo deve considerar o incentivo à definição de políticas de segurança, cujos escopos devem abarcar o gerenciamento de riscos baseado em analise quantitativa e qualitativa, como analises de custo benefício e programas de conscientização.

A gestão da segurança da informação inicia-se com a definição de políticas, procedimentos, guias e padrões.

As políticas podem ser consideradas como o mais alto nível de documentação da segurança da informação, enquanto nos níveis mais baixos podemos encontrar os padrões, procedimentos e guias. Isto não quer dizer que as políticas sejam mais importantes que os guias, procedimentos e padrões.

As políticas superiores devem ser definidas em primeiro lugar por questões estratégicas, enquanto os outros documentos seguem como elementos táticos, como uma política de segurança para *firewall*, que se refere a controles de acessos e lista de roteamento de informações.

O primeiro documento a ser definido deve conter o comprometimento da alta administração, deixando clara a importância da segurança da informação e dos recursos computacionais para a missão institucional. É uma declaração que fundamenta a segurança da informação na totalidade da instituição. Deve conter ainda a autorização para a definição dos padrões, procedimentos e guias de mais baixo nível.

As políticas de alerta não são mandatórias, mas são fortemente incentivadas, normalmente incluindo as conseqüências da não conformidade com as mesmas.

A política informativa é aquela que existe simplesmente para informar aos usuários de um determinado ambiente. Não implicam necessariamente em requisitos específicos, e seu publico alvo pode ser determinados setores somente ou ate mesmo parceiros externos. Possuindo caráter genérico, pode ser distribuída para parceiros externos, como fornecedores, por exemplo, que acessam a rede da instituição, sem que isso acarrete o comprometimento da informação interna.

Os regulamentos de segurança são políticas que uma instituição deve implementar em conformidade com legislação em vigor, garantindo aderência à padrões e procedimentos básicos de setores específicos.

Os padrões especificam o uso uniforme de determinadas tecnologias. Normalmente são mandatórios e implementados através de toda a instituição, a fim de proporcionar maiores benefícios.

Os fundamentos ou princípios são semelhantes aos padrões, com pequena diferença. Uma vez que um conjunto consistente de fundamentos seja definido, a arquitetura de segurança de uma instituição pode ser planejada e os padrões podem ser definidos. Os fundamentos devem levar em conta as diferenças entre as plataformas existentes, para garantir que a segurança seja implementada uniformemente em toda a instituição. Quando adotados, são mandatórios.

Os guias são similares aos padrões, embora mais flexíveis, se referindo a metodologias para os sistemas de segurança, contendo apenas ações recomendadas e não mandatórias. Consideram a natureza distinta de cada sistema de informação.

Podem ser usados para especificar a maneira pela qual os padrões devem ser desenvolvidos, como quando indicam a conformidade com certos princípios da segurança da informação.

Os procedimentos contêm os passos detalhados que devem ser seguidos para a execução de tarefas específicas. São ações detalhadas que os funcionários envolvidos devem seguir. São considerados como inseridos no mais baixo nível em uma cadeia de políticas. O seu propósito é fornecer os passos detalhados para a implementação das políticas, padrões e guias. Também podem ser chamados de *práticas*.

As responsabilidades devem estar relacionadas com o perfil de cada funcionário envolvido no processo, como nos exemplos listados a seguir:

- Gerentes de mais alto nível – Estão envolvidos com toda a responsabilidade da segurança da informação. Podem delegar a função de segurança, mas são visto como o principal ponto quando são consideradas as responsabilizações por eventos relacionados com a segurança;

- Profissionais de segurança dos sistemas de informação – Recebem da gerência de mais alto nível a responsabilidade pela implementação e manutenção da segurança. Estão sob sua responsabilidade o projeto, a implementação, o gerenciamento e a revisão das políticas, padrões, guias e procedimentos;

- Possuidores de dados – São responsáveis pela classificação da informação. Podem também ser responsabilizados pela exatidão e integridade das informações;

- Usuários – Devem aderir às determinações definidas pelos profissionais de segurança da informação;

Auditores de sistemas de informação – São responsáveis pelo fornecimento de relatórios para a gerencia superior sobre a eficácia dos controles de segurança, consolidados através de auditorias independentes e periódicas. Também analisam se

as políticas, padrões, guias e procedimentos são eficazes e estão em conformidade com os objetivos de segurança definidos para a instituição.

2. Recomendações Gerais

2.1 Recomendações para o uso aceitável dos recursos de TI

O uso correto e responsável dos recursos de TI deve ser aplicado a todos os usuários da APF, inclusive aos externos, servidores e prestadores de serviço, que utilizam esses recursos e a infra-estrutura disponível.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelo usuário, no âmbito da infra-estrutura de TI, ficando os transgressores sujeitos à Lei Penal, Civil e Administrativa, na medida da conduta, dolosa ou culposa, que praticarem.

Os documentos produzidos por intermédio dos sistemas de TI são de propriedade da Administração Pública Federal. De igual modo, os programas desenvolvidos para a APF, por servidores do quadro ou prestadores de serviço.

Os sistemas de TI deverão ser utilizados sem violação dos direitos de propriedade intelectual de qualquer pessoa ou empresa, como marcas e patentes, nome comercial, segredo empresarial, domínio na Internet, desenho industrial ou qualquer outro material, que não tenha autorização expressa do autor ou proprietário dos direitos, relativos à obra artística, científica ou literária.

As informações pertencentes ao órgão ou instituição pública da APF ou sob salvaguarda destes devem ser utilizadas apenas para os propósitos definidos na sua missão institucional.

2.2 Recomendações para o uso seguro dos recursos de TI

O envolvimento do usuário é importante no processo da segurança dos recursos de TI, pois é na adequada utilização destes recursos, como instrumento de trabalho, que se inicia a formação de uma sólida cultura de segurança da informação.

Desta forma, recomenda-se aos usuários a adoção das seguintes práticas:

1. Fazer regularmente cópias de segurança de seus dados;
2. Manter registro das cópias de segurança;
3. Guardar as cópias de segurança em local seguro e distinto daquele onde se encontra a informação original;
4. Utilizar senhas que contenham, pelo menos, oito caracteres, compostos de letras, números e símbolos, evitando o uso de nomes, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com o usuário ou palavras constantes em dicionários;
5. Alterar periodicamente suas senhas;
6. Utilizar criptografia sempre que enviar ou receber dados com informações sensíveis;
7. Certificar a procedência do sítio e a utilização de conexões seguras (criptografadas) ao realizar transações via web;
8. Verificar se o certificado do sítio ao qual se deseja acessar, esta integro e corresponde realmente aquele sítio, observando ainda, se o mesmo está dentro do prazo de validade;
9. Certificar que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, antes de realizar qualquer ação ou transação;
10. Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino;

11. Não abrir arquivos ou executar programas anexados a e-mails, sem antes verificá-los com um antivírus;

12. Não utilizar o formato executável em arquivos compactados, pois estes tipos são propícios à propagação de vírus.

2.3 Recomendações sobre atividades permitidas

1. Utilizar programas de computador licenciados para uso pelo órgão público, de acordo com as disposições específicas previstas em contrato. A instalação de programas e sistemas homologados é atribuição da administração de sistemas e TI;

2. Criar, transmitir, distribuir, disponibilizar e armazenar documentos, desde que respeite às leis e regulamentações, notadamente àquelas referentes aos crimes informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade;

3. Fazer cópia de documentos e ou programas de computador a fim de salvaguardá-los, respeitada a legislação que rege a salvaguarda de dados, informações, documentos e materiais sigilosos no âmbito da Administração Pública Federal, exigindo-se autorização para aqueles protegidos pelos direitos autorais, inclusive músicas, textos, documentos digitalizados e qualquer conteúdo encontrado em revistas, livros ou quaisquer outras fontes protegidas por direitos autorais.

2.4 Recomendações sobre atividades NÃO permitidas

1. Introduzir códigos maliciosos nos sistemas de TI;

2. Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;

3. Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI;

4. Tentar interferir ou interferir desautorizadamente em um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;

5. Alterar registro de evento dos sistemas de TI;

6. Modificar cabeçalho de qualquer protocolo de comunicação de dados;

7. Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;

8. Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente;

9. Violar medida de segurança ou de autenticação, sem autorização de autoridade competente;

10. Fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente;

11. Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente;

12. Armazenamento ou uso de jogos em computador ou sistema informacional dos órgãos e instituições da APF;

13. Uso de recurso informacional da entidade pública para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza;

14. Uso de aplicativos não homologados nos recursos informacionais do Órgão Público.

3. Recomendações Específicas

3.1 Recomendações para controle de acesso

1. O acesso a informações rotuladas como públicas e uso interno não é restringido com controles de acesso que discriminam o usuário. Por outro lado, o acesso às informações confidenciais ou restritas será permitido apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso aprovado pela unidade responsável. Da mesma forma, o acesso a alguns equipamentos de hardware e/ou software especiais (como equipamentos de diagnóstico de rede chamados “sniffers”) deve ser restrito a profissionais competentes, com uso registrado e baseado nas necessidades do órgão.

2. Recursos automáticos – Será dado a todos os usuários, automaticamente, o acesso aos serviços básicos como correio eletrônico, aplicações de produtividade e browser WEB. Estas facilidades básicas irão variar de acordo com os cargos e serão determinadas pela autoridade competente em cada órgão público. Todos os outros recursos dos sistemas serão providos via perfis de trabalho ou por uma solicitação especial feita ao proprietário da informação envolvida. A existência de acessos privilegiados, não significa por si só, que um individuo esteja autorizado a usar esses privilégios. Se os usuários tiverem quaisquer questões sobre controle de acessos privilegiados, deverão direcionar suas perguntas unidade competente dentro do Órgão Público.

3. Solicitação de acesso – As solicitações para novas identificações de usuários e alterações de privilégios devem ser feitas por escrito e aprovadas pela chefia imediata do usuário antes que um administrador de sistema realize tal solicitação. Os usuários devem declarar, claramente, porque são necessárias alterações em seus privilégios e a relação de tais alterações com as atividades exercidas.

4. O processo de aprovação do acesso deve ser iniciado pelo superior do usuário e os privilégios garantidos continuarão em efeito até que o usuário mude suas atividades ou deixe o Órgão Público. Se um desses dois eventos ocorrer, o superior hierárquico tem que notificar imediatamente a unidade responsável. Todos aqueles que não são usuários diretos do Órgão Público (contratados, consultores, temporários, etc) têm que se submeter a um processo semelhantes através de seus gerentes de projetos. Os privilégios destas pessoas deverão ser imediatamente revogados quando da finalização do projeto. O mesmo deverá ser observado no desligamento antecipado, considerando ainda a responsabilização pelas atividades e atos cometidos durante a sua permanência no Órgão Público.

5. Os privilégios para todos os usuários dos serviços da rede deverão ser revistos a cada seis meses.

6. Termo de Responsabilização e Sigilo – Todos os usuários que desejam usar os sistemas de Órgão Público devem assinar este termo antes da criação de uma identificação de usuário. Nos casos em que o usuário já possua a identificação e acesso, mas que ainda não tenha assinado tal termo, a assinatura do termo deve ser obtida em caráter de urgência. A assinatura deste termo indica que o usuário em questão entende e concorda com as políticas, padrões, normas e procedimentos do Órgão Público relacionados ao ambiente de TI (incluindo as instruções contidas neste documento), bem como as implicações legais decorrentes do não cumprimento do disposto no termo.

7. Senha de Acesso – As senhas de acesso são controles de segurança essenciais para os sistemas de segurança do ambiente de TI da Administração Pública Federal. Para garantir que os sistemas de segurança façam a parte do trabalho para o qual eles

foram desenvolvidos, os usuários devem escolher senhas que sejam difíceis de serem deduzidas.

8. Proibição de Senhas de Acesso Cíclicas – Os usuários dos recursos de TI devem utilizar sempre novas senhas e o histórico das senhas já utilizadas deve ser mantido pela gerencia de redes

9. Senha de fácil memorização – Os usuários podem escolher senhas de fácil memorização, mas que sejam ao mesmo tempo difíceis de serem descobertas por outras pessoas. Por exemplo:

    - Encadear várias palavras formando o que é conhecido como "frases de acesso".
    - Combinar números e pontuação em uma palavra regular.
    - Criar acrônimos a partir de palavras de música, um poema ou uma outra seqüência de palavras conhecidas.

10. Senha de Boot – Todas as estações de trabalho utilizadas no Órgão Público, não importando sua localização física, deve ter seu acesso controlado a partir de um sistema de controle de acesso definido pela unidade competente e que esteja em conformidade com os requisitos de segurança do Órgão Público.

11. Em caso suspeita de exposição indevida do ambiente de TI do Órgão Público, todas as senhas de acesso devem ser imediatamente alteradas.

12. Os usuários devem possuir orientação sobre a manutenção sigilosa das suas senhas de acesso e as responsabilidades envolvidas com o mal uso das mesmas.

13. Independente das circunstâncias, as senhas de acesso não devem ser compartilhadas ou reveladas para outras pessoas que não o usuário autorizado, ficando o proprietário da senha responsável legal por qualquer prática indevida cometida.

14. Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas. Nestes eventos uma versão segura do sistema operacional assim como dos softwares de segurança deverão ser baixados novamente. Da mesma forma, sob uma dessas circunstancias, todas as alterações recentes de usuários e privilégios do sistema devem ser revisadas a fim de detectar modificações não autorizada de dados. Além destas ações, o responsável pela segurança da informação do Òrgão Público poderá interagir com o Órgão de Resposta a Incidentes do Governo Federal – CTIR-Gov (www.ctir.gov.br).

15. Todos os usuário têm que ser corretamente identificados antes de estarem aptos a utilizar qualquer atividade em computador ou recursos do ambiente de TI.

16. Qualquer computadores que tenham comunicação remota em tempo real com os sistemas de TI do Órgão Público devem se submeter ao mecanismo de controle de acesso definido pela unidade competente, levando-se sempre em consideração os privilégios necessários ao acesso a cada tipo de informação.

17. Os computadores com informações sensíveis e/ou classificadas deverão, obrigatoriamente, ser desligados ou bloqueados na ausência do usuário.

18. Quando os equipamentos ou contas de usuário não estiverem em uso deveram ser imediatamente bloqueados ou desligados.

3.2 Recomendações para a Utilização do Correio Eletrônico Corporativo

1. Deve ser vedado o acesso não autorizado às caixas postais de terceiros e as tentativas de acesso deverão ser registradas em log,

inclusive acessos feitos indevidamente por administradores de sistemas;

2. Deve ser vedado o envio de informações críticas para pessoas ou organizações não autorizadas observando quando for o caso, orientações para o tratamento de informações classificadas;

3. Deve ser vedado o envio de material obsceno, ilegal ou não ético, envio de propaganda, mensagem do tipo corrente e de entretenimento, relacionadas com nacionalidade, raça, orientação sexual, religiosa, convicção política ou qualquer outro assunto que possa vir a difamar o usuário como cidadão e que não tenha relação com o serviço a que o usuário é destinado no ambiente do TI do Órgão Público;

4. Deve ser vedado o envio de mensagens simultâneas aos usuários da rede, exceto por intermédio da administração desta;

5. Deve ser vedado a participação em Listas de Discussão, utilizando o serviço de Correio Eletrônico Corporativo, que possam abordar assuntos alheios ao Órgão Público, suas diretorias e suas gerências, exceto em casos de participação em Listas de Discussão sobre assuntos relacionados às atividades desenvolvidos no órgão público;

6. É necessário o registro por parte do usuário, enquanto funcionário do Órgão Público, das listas de discussão em que se encontra inserido, para fins de controle e possível cancelamento quando houver necessidade;

7. É recomendada a utilização de Assinatura Digital, para o envio de mensagens internas via Correio Eletrônico Corporativo quando do tramite de informações **classificadas**, seguindo sempre a legislação vigente que trata deste assunto.

8. O Correio Eletrônico do Órgão Público deve ser utilizado sempre baseado no bom senso e de acordo com os preceitos legais.

3.3 Recomendações para a Utilização de Aplicações Corporativas e Software de Terceiros

1. Deve ser vedado aos usuários que fazem uso de sistemas de informação o acesso não autorizado a qualquer outro sistema que não possua permissão de uso, assim como a danificação, a alteração a interrupção da operação de qualquer sistema do ambiente de TI. Da mesma maneira deve ser vedado aos usuários a obtenção indevida de senhas de acesso, chaves criptográficas ou qualquer outro mecanismo de controle de acesso que possa possibilitar o acesso não autorizado a recursos informacionais;

2. A classificação ou reclassificação da informação deve seguir as orientações da legislação vigente, assim como aquelas regras definidas pelo Decreto Nº 4553 ou sua atualização;

3. Deve ser vedado aos usuários o acesso, modificação, a remoção ou a cópia de arquivos que pertençam a outro usuário sem a permissão expressa do mesmo;

4. O órgão público deve se reservar o direito de revogar os privilégios de usuário de qualquer sistema e a qualquer momento. Não sendo permitidas condutas que interfiram com a operação normal e adequada dos sistemas de informação do Órgão Público e que adversamente afetem a capacidade de outras pessoas utilizarem esses sistemas de informação, bem como condutas que sejam prejudiciais e ofensivas;

5. Deve ser vedado aos usuários a execução de testes ou tentativas de comprometimento de controles interno, este tipo de pratica somente pode ser permitada a usuários técnico, em situações nas

quais esteja ocorrendo monitoração e analise de riscos, com a autorização da unidade competente;

6. Deve ser exigido a assinatura de termo de confidencialidade antes que seja fornecido o acesso aos sistemas governamentais relacionados com a cadeia de privilégios do usuário.

7. As configurações e atribuição de parâmetros em todos os computadores conectados à rede do Órgão Público devem estar de acordo com as políticas e normas de gerenciamento internas.

8. Quando um usuário do desligamento do usuário, seus arquivos armazenados em estação de trabalho ou em qualquer servidor de rede do Órgão Público e, também, seus documentos em papel devem ser imediatamente revisados pela chefia imediata para determinar quem tornar-se-á curador das informações relacionadas, assim como nos casos devidos, identificar o método mais adequado para a eliminação das mesmas, levando-se em conta as orientações sobre a eliminação de informações classificadas contidas na legislação vigente.

9. Todas as atividades dos usuários que podem afetar os sistemas de informação governamentais devem ser possíveis de reconstituição a partir dos logs de maneira a evitar ou dissuadir o comportamento incorreto. Estes procedimentos devem contar inclusive com mecanismos de responsabilização claros e amplamente divulgados nos meios de comunicação internos.

10. A divulgação das regras e orientações de segurança aplicadas aos usuários finais deverão ser objeto de campanhas internas permanentes, seminários de conscientização e quaisquer outros meios de maneira a criar uma cultura de segurança dentro da instituição pública.

11. Deve ser vedada a utilização de software da Internet ou de qualquer outro sistema externo ao Órgão Público. Esta proibição é necessária porque tal software pode conter vírus, worms, cavalos de tróia e outros softwares maliciosos que podem comprometer o ambiente de TI. Caso haja uma legítima necessidades de obtenção de aplicações de terceiros o fato deve ser comunicado à unidade competente para que a mesma estabeleça os procedimentos de segurança necessários.

12. Deve ser vedada a utilização de disquetes de origem externa, nas estações de trabalho do Órgão Público ou nos servidores de rede antes de serem submetidos a um sotware antivírus.

13. Todos os softwares e arquivos transferidos de fontes que não sejam do próprio Órgão Público via Internet (ou qualquer outra rede Pública) devem ser examinados com o software de detecção de vírus utilizado pelo Ministério. Este exame deve acontecer antes que o arquivo seja executado ou aberto por um outro programa, como por exemplo, por um processador de texto e também, antes e depois que o material tenha sido descompactado.

14. O usuário do ambiente de TI de Órgão Público não deve executar ou desenvolver qualquer tipo de programa ou processo externo às suas atividades.

15. Os usuários não devem desenvolver, gerar, compilar, copiar, coletar, propagar, executar ou tentar introduzir qualquer código projetado para se auto-replicar, danificar ou de outra maneira obstruir o acesso ou afetar o desempenho de qualquer computador, rede ou sistema de TI da APF.

16. Deve ser vedado aos usuários e visitantes fumar, comer ou beber próximo aos equipamentos de TI.

3.4 Recomendações para a Manipulação das Informações

1. A palavra “usuário” será utilizada para designar todos utilizadores do ambiente de TI, independente do cargo ocupado;

2. Instruções claras e bem divulgadas sobre normas existentes sobre a manipulação de informações;

3. Todos os usuários têm que observar as exigências para manipulação da informação, baseadas no tipo de informação considerada e que será definida pelo seu proprietário (ou responsável) seguindo as orientações encontradas no documento de Política de Segurança de cada órgão ou instituição. Os proprietários podem atribuir controles adicionais para maior restrição de acesso ou para ampliar a proteção a suas informações.

4. A divulgação de informações CONFIDENCIAL ou RESTRITA, para qualquer pessoa (usuário ou não do ambiente de TI do órgão ou instituição), é proibida, a menos que este acesso tenha sido previamente autorizado pelo proprietário da informação. Todas as pessoa que não forem usuários diretos do órgão ou instituição devem assinar um termo de confidencialidade antes de terem acesso a esses tipos de informação. Os curadores dessas informações devem verificar a existência deste termo, devidamente assinado, antes de divulgá-las para pessoas que não pertençam ao quadro funcional do órgão ou instituição. O acesso a este tipo de informação deve ser sempre devidamente registrado.

5. A reprodução da informação CONFIDENCIAL e/ou RESTRITA, incluindo a impressão de cópias adicionais, não é permitida a menos que seja explicitamente autorizada por seu proprietário. Da mesma forma, trechos, resumos, traduções ou qualquer material derivado de informações sensíveis ou resguardadas por direitos autorais, não poderam ser feito a menos que o proprietário da informação tenha aprovado previamente.

6. O transporte físico das informações CONFIDENCIAL e/ou RESTRITA requer a observação no disposto em legislação relacionada.

7. Quando as informações são CONFIDENCIAL e/ou RESTRITAS não forem mais necessárias e quando exigências legais ou regulatórias para sua retenção não se aplicarem mais, elas deverão ser destruídas de acordo com os métodos aprovados. É proibida a eliminação em latas de lixo ou em depósitos de papel que serão encaminhados para reciclagem. A informação sensível em forma de papel deve ser eliminada com o uso de picotador de papel. A informação sensível armazenada em disquetes, fitas magnéticas ou outras mídias magnéticas computacionais deve ser destruída via refornatação ou apagando-se a informação caso a mídia seja reutilizada por outros sistemas do órgão ou instituição pública. A simples “remoção” de uma informação sensível armazenada em uma mídia magnética não é suficiente porque a informação pode ser definitivamente destruída com cortadores ou colocada em um recipiente especialmente destinado a armazenagem de informação sensível que será destruída.

3.5 Responsabilidade dos Órgãos Públicos

É de competência de cada órgão elaborar termo de responsabilidade para assinatura de seus usuários, objetivando a declaração de conhecimento de suas normas de segurança.

As transgressões a tais normas deverão ser apuradas em conformidade com a legislação aplicável.

Anexo I - Glossário de Termos Técnicos

A

Ambiente do Sítio - Infra-estrutura computacional, de rede e lógica, que compõe a base para o provimento do serviço Web..

Arquitetura de Rede – É uma definição de alto nível do comportamento e das conexões entre os nós em uma rede, suficiente para possibilitar a avaliação das propriedades da rede.

Atacante - Indivíduo responsável pela realização de um ataque.

Ataque - Ação que constitui uma tentativa delibarada e não autorizada para acessar/manipular informações, ou tornar um sistema não confiável, ou indisponível, violando assim a política de segurança. Um ataque bem sucedido que resulte no acesso ou manipulação de informações, de forma não autorizada, é chamado de invasão.

Ataque de Negação de Serviço - Ataque que consiste em impedir o acesso autorizado a recursos de um sistema, seja através de uma grande sobrecarga no processamento de dados de um sistema computacional, da saturação de um ponto de acesso através de um grande tráfego de dados para uma rede, ou da indisponibilização de um ou mais serviços desse sistema.

Atividade Maliciosa - Qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema computacional.

Autenticação – Procedimento utilizado na identifição de usuários, dispositivos ou processos, e que é pré-requisito para o acesso aos recursos de um sistema.

Autorização – É o direito ou permissão de acesso a um recurso de um sistema.

B

Backdoor - Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

C

Capacidade de Sobrevivência (Survivability) - É a capacidade de um sistema de cumprir a sua missão, no momento certo, na presença de ataques, falhas ou incidentes.

Cavalo de Tróia - É um Programa que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Cenário de Uso - É uma instancia do uso de um sistema, tanto o uso legitimo como o uso em uma invasão.

Cliente - Entidade, normalmente caracterizada por um processo ou programa de computador, que requisita e utiliza recursos/informações e interage com um serviço fornecido por um sistema computacional, como por exemplo um servidor Web (ver Servidor Web, Serviço Web).

Código Malicioso - Programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente através de exploração de alguma vulnerabilidade desse sistema.

Comprometimento de segurança - É uma violação de segurança na qual os recursos do sistema são expostos, ou potencialmente expostos, a um acesso não autorizado.

Confiança - Atributo de um sistema de informação que provê a base para ter a confiança de que o sistema opera de forma a cumprir a política de segurança.

Confiança (Assurance) – Medida de confiança garantida pela arquitetura ou pelas características de segurança implementadas em um sistema de informação automatizado.

Confidencialidade - É o requisito que diz que uma informação não é disponibilizada ou revelada para partes não autorizadas.

Contato Técnico de Segurança - Pessoa ou equipe a ser acionada em caso de incidente de segurança envolvendo um sítio governamental, com atribuições eminentemente técnicas sobre a questão.

Correção de Segurança - Software que têm por finalidade corrigir os problemas de segurança referentes a vulnerabilidades conhecidas. Também chamado de *patch, hot fix ou service pack.*

Criptografia - É a disciplina que trata dos princípios, meios e métodos para a transformação de dados, tornando-os ininteligíveis, de forma a possibilitar a detecção de modificações no conteúdo da informação e/ou prevenir seu uso não autorizado.

Controle de Acesso - Mecanismo utilizado para proteger os recursos de um sistema de acesso não autorizado. Deve permitir, de acordo com uma política de segurança, o acesso somente a entidades autorizadas, como usuários, processos, programas ou outros sistemas.

D

Desfiguração de Sítio - Ataque que consiste em desfigurar, ou seja, substituir ou alterar o conteúdo de uma ou mais páginas Web em um sítio. A desfiguração normalmente é conseqüência da exploração bem sucedida de uma vulnerabilidade no servidor Web que hospeda as páginas do sítio.

Detecção de Intrusão - Consiste no monitoramento e análise de eventos em sistemas computacionais, com o propósito de detectar e prover alertas sobre tentativas de acesso não autorizado a recursos destes sistemas.

Direito de Acesso - É a permissão dada a uma entidade para acessar e manipular informações presentes em um sistema.

Disponibilidade - É o requisito que diz que os recursos de um sistema estarão disponíveis para acesso, por entidades autorizadas, sempre que venham a ser solicitados.

F

Firewall - Um sistema, constituído pela combinação de software e hardware, que intermedia o acesso a uma rede, permitindo ou proibindo certos tipos de acesso, de acordo com uma política de segurança pré-estabelecida.

Firewall Pessoal - Um sistema utilizado para proteger um único computador contra acessos não autorizados. Constitui um tipo específico de firewall.

I

Incidente de Segurança - Um incidente de segurança é caracterizado por qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas computacionais ou de redes de computadores. Tentativas de obter acesso não autorizado a sistemas ou dados, ataques de negação de serviço, uso ou acesso não autorizado a um sistema e desrespeito à política de segurança ou à política de uso aceitável de uma instituição são exemplos de incidentes de segurança.

Informação de Autenticação - Informação apresentada e utilizada para confirmar a identidade de uma entidade, como usuários, processos, programas ou sistemas.

Integridade - É o requisito que diz que uma informação não é modificada ou destruída de maneira não autorizada ou acidental.

Intrusão - Ver Invasão.

Intruso - Ver Invasor.

Invasão - Evento ou combinação de eventos que constituem um incidente de segurança em que um invasor ou um código malicioso obtém acesso a um sistema, ou a recursos de um sistema, de forma não autorizada.

Invasor - Indivíduo responsável pela realização de uma invasão.

Irretratabilidade - Garantia de que o emissor de uma mensagem não irá negar posteriormente a sua autoria ou participação em uma transação. É controlada pela existência de uma assinatura digital que somente o emissor pode gerar.

M

Mecanismo de Controle de Acesso (Access Control Mechanism) – São mecanismos de hardware ou software, procedimentos operacionais ou gerenciais usados para detectar e prevenir os sistemas computacionais contra acessos não autorizados.

Modelo de Uso (Usage Model) – É a definição de todos os cenários de utilização possíveis de um ambiente de sistemas, incluindo o uso legitimo e aquele possível de ser explorado por um intruso.

Mecanismos de Controle de Acesso - São mecanismos de hardware ou software, ou procedimentos operacionais ou gerenciais, usados para proteger os sistemas computacionais contra acessos não autorizados.

Modo seguro - É o conjunto que envolve configurações, procedimentos e diretrizes de segurança recomendados por entidades notoriamente reconhecidas na área de segurança da informação.

N

Negação de Serviço – É o ataque a segurança feito a partir da saturação de um ponto de acesso de forma que este não disponha de banda passante para o atendimento do seus usuários legítimos.

O

Órgãos Conveniados - São aquelas entidades que não fazem parte das estruturas organizacionais da Administração Pública Federal (APF), e, mediante convênio, utilizam os serviços oferecidos por meio dos Sistemas de TI destas.

Órgão Proprietário do Sítio Governamental - Entidade governamental proprietária do domínio onde se encontram armazenadas as informações e serviços prestados.

P

Plug-in - Módulo constituído por um dispositivo de hardware ou software, queadiciona uma característica, funcionalidade ou serviço específico a um sistema.

Política de Segurança - Atribui direitos e responsabilidades aos indivíduos que lidam com os recursos computacionais de uma instituição e com as informações neles armazenadas. Define as atribuições de cada indivíduo em relação à segurança dos recursos com os quais trabalha. Qualquer evento que resulte no descumprimento da política de segurança é considerado um incidente de segurança.

Política de Uso Aceitável – Documento que define como os recursos computacionais de uma instituição podem ser utilizados. Também define os direitos e responsabilidades dos usuários destes recursos.

R

Recursos da Infra-estrutura de TI - Os recursos da infra-estrutura de TI incluem equipamentos, utilitários, aplicativos, sistemas operacionais, mídias de armazenamento, contas em servidores, contas de correio eletrônico, navegação na Internet e intranet, serviço de transferências de dados, terminal virtual, comunicação interativa e sistemas de gestão.

Rede Sem Perímetro – É uma rede caracterizada por topologia e funcionalidade que não podem ser determinadas, assim como pela ausência de controle centralizado.

Registro de Evento - Conjunto de informações armazenadas e que estão relacionadas aos eventos ocorridos em um determinado contexto, como serviços Web, autenticação de usuários, etc.

Requisitos de Sobrevivência de Serviços – É a definição dos serviços essenciais assim com das funcionalidades relacionadas com a resistência, reconhecimento, recuperação e adaptação, e evolução que são suficientes para se satisfazer os requisitos necessários à garantia da sobrevivência do sistema.

S

Script - Um script consiste em uma lista de comandos que podem ser executados sem a interação do usuário. Normalmente é escrito em uma linguagem de programação simples, que facilita o seu desenvolvimento. É bastante utilizado, por exemplo, em serviços Web, para a realização de buscas, processamento e fornecimento de informações em páginas Web.

Serviços de Adaptação e Evolução – São funções que melhoram continuamente a capacidade do sistema de fornecer os serviços essenciais, melhorando sua resistência, capacidade de reconhecimento e recuperação.

Serviços Subsidiários – São serviços adicionais à emissão dos certificados que suportam a assinatura digital e outros serviços relacionados ao comercio eletrônico como criptografia de dados. Como exemplo deste tipo de serviços pode-se citar serviços de diretório e serviços de geração de pares de chaves. O serviço de diretório possibilitam que os usuários recuperem certificados e outras informações sobre pessoas, como nomes distintos e endereços de e-mail. Serviços de geração de pares de chaves fornecem aos usuários pares de chaves pública/privada de alta qualidade apropriadas para um algoritmo criptográfico particular. As chaves privadas são seguramente destruídas após a sua geração de forma a evitar potenciais comprometimentos.

Serviços Essenciais – São serviços para os usuários de um sistema que deverão ser providos mesmo na presença de um intruso, de falhas ou acidentes.

Serviços Não Essenciais – São serviços que podem ser temporariamente suspensos para permitir que os serviços essenciais não sejam interrompidos quando um sistema esta sob ataque ou invasão.

Serviços de Reconhecimento – São funções que detectam tentativas e invasões.

Serviços de Recuperação – São funções que possibilitam a recuperação do sistema após uma invasão.

Serviços de Resistência – São funções e propriedades do sistema que dificultam e torna dispendiosa uma invasão.

Serviço Web - Serviço em rede de computadores disponibilizado por meio da Internet.

Servidor Web - Computador encarregado de prover serviços web.

Sigilo - Classificação dada a informações onde apenas entidades autorizadas e previamente autenticadas poderão ter acesso.

Sistema de TI - Sistema de Tecnologia da Informação (TI) é o conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens; que possibilitam a agregação dos recursos de informática e telecomunicações de maneira integrada.

Sítio - Endereço eletrônico de serviço web.

Anexo II - Referências de Legislação

3.2 **Decreto Nº 8.183, de 11 de abril de 1991**
Dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacioal.

3.3 **Decreto Nº 1.048, de 21 de janeiro de 1994**
Dispõe sobre a estrutura e o funcionamento do SISP

3.4 **Decreto 3505, de 13 de junho de 2000**
Define a política de segurança para a Administração Pública Federal

3.5 **Lei Nº 9983, de 14 de julho de 2000**
Atualiza o código penal e da outras providencias

3.6 **Decreto 4553**
Define procedimentos para a classificação de informações sensíveis.

3.7 **Medida Provisória 2200-2**
Define a Infra-estrutura de Chaves Públicas Brasileira

Anexo III – Exemplo de Termo de Confidencialidade

O texto a seguir pode ser adaptado para utilização em casos específicos, visando salvaguardar a confidencialidade e o sigilo.

Identificação do órgão, brasão, etc....

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

Eu, _____,

Portador do documento de identidade nº _____, expedido pela _____, CPF nº _____, órgão de origem _____, lotado no(a) _____, comprometo-me a manter sigilo sobre dados, processos, informações, documentos e materiais que eu venha a ter acesso ou conhecimento no âmbito do ORGÃO, em razão das atividades profissionais a serem realizados e ciente do que preceituam a Lei 10.406, de 10 de janeiro de 2002 (Código Civil), no seu art. 229, inciso I; o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), nos arts. 153, 154, 314, 325 e 327; o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), no art. 207; a Lei nº 5.689, de 11 de janeiro de 1973 (Código de Processo Civil), nos arts. 116, 117, 132 e 243; a Lei nº 8.159, de 8 de janeiro de 1991 (Lei de Arquivos), nos arts. 4, 6, 23 e 25; a Lei nº 9.983, de 14 de julho de 2000 (Alteração do Código Penal); o Decreto nº 1.171, de 22 de junho de 1994 (Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal); e o Decreto nº 4.553, de 27 de dezembro de 2002 (Salvaguarda de dados, informações, documentos e materiais sigilosos).

E por estar de acordo com o presente Termo, assino-o na presença das testemunhas abaixo mencionadas.

Assinatura e

Testemunhas