PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

DIRETRIZES PARA DESENVOLVIMENTO E OBTENÇÃO DE SOFTWARE SEGURO NOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA LEGAL E NORMATIVA

Decreto nº 3.505, de 13 de junho de 2000.
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008, e respectivas normas complementares.
NBR ISO/IEC 27002:2005.
NBR ISO/IEC 27005:2011.
Decreto nº 7579, de 11 de outubro de 2011.
Decreto de 18 de outubro de 2000 - Governo Eletrônico.
Decreto nº 4553, de 27 de dezembro de 2002.
Instrução Normativa nº 04/2010 da Secretaria de Logística e Tecnologia da Informação/MPOG.

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR

Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Estabelecer diretrizes de Segurança da Informação e Comunicações para a obtenção de software seguro nos órgãos e entidades da Administração Pública Federal, direta e indireta.

2 CONSIDERAÇÕES INICIAIS

2.1 As organizações modernas cada vez mais se veem dependentes de tecnologias que possam fazer suas informações circularem rapidamente, de forma a atenderem as necessidades negociais das quais se encontram atreladas.

2.2 Paralelamente ao desenvolvimento e emprego de novas tecnologias, essas mesmas organizações vêm sofrendo ataques ao seu acervo de informações, cuja frequência é cada vez maior e com uso mais aprimorado de recursos computacionais. Os órgãos e entidades da Administração Pública Federal, direta e indireta não se encontram isentos dessa realidade, e, portanto devem estar capacitados para prover as respostas adequadas, garantindo a segurança de seus serviços.

2.3 Com o uso intensificado de softwares e hardwares específicos para prover níveis de segurança adequados às informações, novas formas de ataques foram elaboradas, sendo que, atualmente, o foco concentra-se na exploração de vulnerabilidades de segurança existentes nos sistemas desenvolvidos ou adquiridos pelos órgãos, uma vez que muitos deles não foram implementados considerando boas práticas de codificação segura, ou, que não foram objeto de um processo de desenvolvimento suportado por testes que validem os controles aplicados.

2.4 Grande parte dessas vulnerabilidades de segurança ocorre em consequência de defeitos que podem ser introduzidos durante o ciclo de desenvolvimento de um software.

2.5 Se a engenharia de segurança for integrada ao ciclo de vida de desenvolvimento do software, pode-se garantir uma redução dessas vulnerabilidades, assegurando que os aspectos da segurança da informação sejam considerados durante a obtenção do software seguro.

2.6 Considerando as vulnerabilidades resultantes da não adoção de práticas seguras durante o processo de desenvolvimento e manutenção de sistemas, torna-se necessário definir requisitos mínimos com o objetivo de proteger os ativos de informação dos órgãos e entidades Administração Pública Federal, direta e indireta.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações – DSIC estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

4 CONCEITOS E DEFINIÇÕES

4.1 Os processos para obtenção de software seguro englobam (de forma isolada ou em conjunto):

a) a aquisição, paga ou não, de software pronto;
b) o desenvolvimento e/ou manutenção de software realizado por profissionais da própria organização; e
c) a contratação de terceiros para o desenvolvimento e/ou manutenção de software.

4.2 Para os efeitos desta Norma Complementar são estabelecidos ainda, os seguintes conceitos e definições:

a) **Análise Dinâmica**: tipo de teste de software que verifica seu comportamento externo em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de interações com o software em execução;

b) **Análise Estática**: tipo de teste de software que verifica sua lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio da verificação do código-fonte ou dos binários;

c) **Autenticidade:** propriedade de que a informação foi produzida, modificada ou descartada por uma determinada pessoa física, órgão, entidade ou sistema;

d) **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

e) **Controles de Segurança**: medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: a criptografia, as funções de “hash”, a validação de entrada, o balanceamento de carga, as trilhas de auditoria, o controle de acesso, a expiração de sessão, os “backups”, etc.;

f) **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

g) **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

h) **Requisitos de segurança**: conjunto de necessidades de segurança que o software deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, compreendendo aspectos funcionais e não funcionais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários (administradores, usuários comuns, etc.), autenticação com o uso de credenciais (usuário e senha, certificados digitais, etc.), dentre outros. Os aspectos não funcionais descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente mesmo quando sob uso indevido. São exemplos de requisitos não funcionais, dentre outros, a validação das entradas de dados

e o registro de logs de auditoria com informações suficientes para análise forense;

i) **Segurança da Informação e Comunicações**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações; e

j) **Vulnerabilidade**: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

5 DIRETRIZES PARA O PROCESSO DE DESENVOLVIMENTO DE SOFTWARE SEGURO

Para o processo de desenvolvimento de software seguro nos órgãos e entidades da Administração Pública Federal, direta e indireta recomenda-se:

a) estabelecer normas internas baseadas nesta norma complementar para o desenvolvimento de software seguro;

b) identificar os responsáveis pela definição e validação dos requisitos de segurança que o software deva atender;

- recomenda-se o estabelecimento formal desses responsáveis.

c) definir os requisitos de segurança logo no início de qualquer projeto de desenvolvimento de software;

d) implementar controles de segurança necessários para proteger os ativos de informação, de acordo com a sua criticidade que deve ser definida pelos respectivos órgãos e entidades da Administração Pública Federal, direta e indireta;

e) usar controles de segurança como componentes, de forma que sejam catalogados e reutilizados em outros sistemas;

- é recomendado que esses componentes sejam baseados em padrões de referência do mercado; e

- fica a cargo de cada órgãos e entidades da Administração Pública Federal, direta e indireta a escolha das melhores soluções de mercado.

f) considerar o controle de acesso durante a etapa de desenvolvimento;

- orienta-se que esse controle seja feito por meio de componentes isolados.

g) implementar os controles de segurança por múltiplas camadas, de acordo com a criticidade das informações tratadas pelo software;

- a utilização dos controles em múltiplas camadas dificulta a exploração de vulnerabilidades.

h) considerar o uso da arquitetura do software de forma a privilegiar a alta coesão e baixo acoplamento, a facilidade de uso e a não implementação de mecanismos de segurança desnecessários;

i) construir o software de forma que suas mensagens de erro não revelem detalhes da sua estrutura interna.

j) verificar o atendimento dos requisitos de segurança do software; e

- esta verificação pode ser realizada através de uma análise estática e/ou análise dinâmica do software.

k) configurar adequadamente o software desenvolvido quando este passar para o ambiente de produção.

- todo código de teste, de “backups” ou arquivos desnecessários, de informações sigilosas nos comentários de código e das contas criadas para teste devem ser removidos.

6 DIRETRIZES PARA A OBTENÇÃO DE SOFTWARE SEGURO.

Para o processo de obtenção de software seguro nos órgãos e entidades da Administração Pública Federal, direta e indireta recomenda-se:

a) estabelecer normas internas baseadas nesta norma complementar para a obtenção de software seguro;

b) estabelecer acordos de licenciamento, propriedade dos códigos e direitos de propriedade intelectual condizentes com o interesse de cada órgão e entidade da Administração Pública Federal, direta e indireta de forma a adquirir a titularidade do software ou para apenas exercer o direito de uso;

c) definir e documentar os requisitos específicos de segurança para a aplicação a ser adquirida ou desenvolvida externamente;

d) instaurar meios que visem o controle da qualidade e precisão do trabalho efetuado de forma a garantir que os requisitos de segurança sejam atendidos;

e) estabelecer definições sobre a custódia de código-fonte e manutenção do software em caso de falha da empresa contratada;

- caberá a cada órgão e entidade da Administração Pública Federal, direta e indireta a elaboração destas definições, quando necessário.

f) definir a execução de testes pela contratada e homologação pelos órgãos e entidades da Administração Pública Federal, direta e indireta antes da instalação do software obtido no ambiente de produção;

- orienta-se que seja realizada análise estática do software desenvolvido por terceiros; e

- o tratamento das vulnerabilidades deve ser um dos requisitos para a aceitação do sistema.

g) definir regras e procedimentos operacionais para a contratada quanto à liberação de acesso aos recursos tecnológicos e ao ambiente físico ou lógico de cada órgão e entidade da Administração Pública Federal, direta e indireta, caso seja necessário;

h) definir as regras para transferência do conhecimento sobre o software desenvolvido de modo a permitir a sua manutenção, de forma independente, por parte dos órgãos e entidades da Administração Pública Federal, direta e indireta; e

i) todos os procedimentos de segurança descritos acima devem estar previstos no instrumento contratual correspondente.

7 RESPONSABILIDADES

7.1 Os órgãos e entidades da Administração Pública Federal, direta e indireta devem planejar procedimentos relacionados à obtenção de software seguro em consonância com suas respectivas Políticas de Segurança da Informação e Comunicações (POSIC).

7.2 Os responsáveis pelos órgãos e entidades da Administração Pública Federal, direta e indireta devem oferecer conscientização em segurança de software a todos os envolvidos no processo de obtenção de softwares seguros.

7.3 Os responsáveis pelos órgãos e entidades da Administração Pública Federal, direta e indireta devem considerar a possibilidade de aplicar o disposto nessa norma nos softwares obtidos antes de sua entrada em vigor.

8 VIGÊNCIA

Esta Norma entra em vigor na data de sua publicação.