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

Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA E BIBLIOGRÁFICA

Instrução Normativa GSI Nº 01, de 13 de junho de 2008, e respectivas Normas Complementares publicadas no DOU pelo DSIC/GSIPR
ABNT NBR ISO/IEC 27002: (17799:2005)
Decreto No. 4.553 de 27 de dezembro de 2002
Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (BRASIL/GSIPR, 2010)

CAMPO DE APLICAÇÃO

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

SUMÁRIO

1. **Objetivo**
2. **Fundamento Legal da Norma Complementar**
3. **Conceitos e Definições**
4. **Princípios e Diretrizes**
5. **Procedimentos**
6. **Responsabilidades**
7. **Vigência**

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Estabelecer diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

2 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.

3 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar, aplicam-se os seguintes termos e definições:

3.1 Agente Responsável - Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar o processo de Inventário e Mapeamento de Ativos de Informação;

3.2 Ameaça – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

3.3 Ativos de Informação - os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

3.4 Autenticidade – propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

3.5 Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

3.6 Contêineres dos Ativos de Informação - o contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado.

3.7 Continuidade de Negócios - capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

3.8 Custodiante do ativo de informação - refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação;

3.9 Disponibilidade – propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

3.10 Estratégia de Continuidade de Negócios - abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior;

3.11 Gestão de riscos de segurança da informação e comunicações – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

3.12 Identificação e Classificação de Ativos de Informação - é um processo composto por 6 (seis) etapas: (a) coletar informações gerais; (b) definir as informações dos ativos; (c) identificar o(s) responsável(is); (d) identificar os contêineres dos ativos; (e) definir os requisitos de segurança; e (f) estabelecer o valor do ativo de informação;

3.13 Infraestrutura Crítica da Informação – são os meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso, que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade;

3.14 Integridade – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

3.15 Inventário e Mapeamento de Ativos de Informação - é um processo interativo e evolutivo, composto por 3 (três) etapas: (a) identificação e classificação de ativos de informação, (b) identificação de potenciais ameaças e vulnerabilidades e (c) avaliação de riscos.

3.16 Proprietário do ativo de informação - refere-se a parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação, assumindo, no mínimo, as seguintes atividades: a) descrever o ativo de informação; b) definir as exigências de segurança da informação e comunicações do ativo de informação; c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários; d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento; e, e) indicar os riscos que podem afetar os ativos de informação;

3.17 Riscos de segurança da informação e comunicações – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

3.18 Segurança da informação e comunicações - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

3.19 Valor do Ativo de Informação - valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos de um órgão ou entidade da APF, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado.

3.18 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.

4 PRINCÍPIOS E DIRETRIZES

4.1 As diretrizes gerais do processo de Inventário e Mapeamento de Ativos de Informação devem considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais, e a estrutura do órgão ou entidade da APF, além do que devem estar alinhadas à Instrução Normativa GSIPR 01/2008, bem como à Política de Segurança da Informação e Comunicações do órgão ou entidade.

4.1.1 Tais diretrizes devem, também, subsidiar propostas de novos investimentos na área de segurança da Informação e Comunicações;

4.2 O processo de Inventário e Mapeamento de Ativos de Informação objetiva a Segurança das Infraestruturas Críticas de Informação do órgão ou entidade da APF, e deve ser aplicado tanto na Gestão de Riscos de Segurança da Informação e Comunicações, quanto na Estratégia de Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações;

4.3 O processo de Inventário e Mapeamento de Ativos de Informação deve subsidiar o órgão ou entidade da APF a conhecer, valorizar, proteger e manter seus ativos de informação, em conformidade com os requisitos legais e do negócio;

4.4 O processo de Inventário e Mapeamento de Ativos de Informação tem como objetivo prover o órgão ou entidade da APF: de um entendimento comum, consistente e inequívoco de seus ativos de informação; da identificação clara de seu(s) responsável(eis) - proprietário(s) e custodiante(s); de um conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo de informação; de uma descrição do contêiner de cada ativo de informação; e da identificação do valor que o ativo de informação representa para o negócio do órgão ou entidade da APF;

4.5 O processo de Inventário e Mapeamento de Ativos de Informação deve produzir subsídios tanto para a Gestão de Segurança da Informação e Comunicações, a Gestão de Riscos de Segurança da Informação e Comunicações, e a Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, da APF, quanto para os procedimentos de avaliação da conformidade, de melhorias contínuas, auditoria e, principalmente, de estruturação e geração de base de dados sobre os ativos de informação;

4.6 O processo de Inventário e Mapeamento de Ativos de Informação, deve ser dinâmico, periódico, e estruturado, para manter a Base de Dados de Ativos de Informação atualizada e conseqüentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações. Tal Base de Dados, deve operar como infraestrutura material e técnica em condições de dar suporte às ações de cooperação entre entes federativos que têm sob as suas governança ativos de informação.

5 PROCEDIMENTOS

Apresenta-se uma abordagem sistemática do processo de Inventário e Mapeamento de Ativos de Informação, o qual é composto por 3 (três) sub-processos (1) identificação e classificação de ativos de informação, (2) identificação de potenciais ameaças e vulnerabilidades e (3) avaliação de riscos.

O sub-processo 1 é apresentado a seguir, e os sub-processos 2 e 3 são objetos tratados na Norma Complementar Nº 04 DSIC/GSIPR, e no Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (Brasil/GSIPR, 2010).

O sub-processo de Identificação e Classificação de Ativos de Informação caracteriza-se por 6 (seis) etapas: (1) coleta de informações gerais dos ativos de informação; (2) detalhamento dos ativos de informação; (3) identificação do(s) responsável(is) – proprietário(s) e custodiante(s) de cada ativo de informação; (4) caracterização dos contêineres dos ativos de informação; (5) definição dos requisitos de segurança da informação e comunicações; e (6) estabelecimento do valor do ativo de informação.

5.1 Coleta de informações gerais dos ativos de informação

Nesta etapa, deve-se definir como será a estratégia da coleta das informações gerais dos ativos de informação, quem serão os responsáveis pela coleta, qual a previsão de conclusão dos trabalhos, e qual a periodicidade de atualização. Esta análise inicial deve estar embasada nos objetivos estratégicos e no negócio do órgão ou entidade da APF.

5.1.1 Recomenda-se definir o escopo da coleta, levantando no mínimo um conjunto essencial de informações sobre cada ativo de informação. Esse escopo pode abranger o órgão ou entidade da APF como um todo, um segmento, ou mesmo, um processo; e

5.1.2 Recomenda-se adotar metodologias de Gestão de Riscos de Segurança da Informação e Comunicações e de Gestão de Continuidade de Negócios, nos aspectos relacionados à SIC, que incorporem o processo de Inventário e Mapeamento de Ativos de Informação.

5.2 Detalhamento dos ativos de informação

Nesta fase, cabe observar que o nível de detalhe das informações dos ativos de informação, deve ser definido pelo órgão ou entidade da APF, a partir da necessidade do negócio e dos objetivos estratégicos dos mesmos, bem como com vistas a atender aos interesses da sociedade e do Estado.
Recomenda-se, portanto, que o detalhamento inicial dos ativos de informação, contemple no mínimo um conjunto essencial de informações, e deva ser suficiente para:

5.2.1 determinar com clareza e objetividade o conteúdo do ativo de informação;

5.2.2 identificar o(s) responsável(is) – proprietário(s) e custodiante(s) - de cada ativo de informação;

5.2.3 identificar o valor de cada ativo de informação; e,

5.2.4 identificar os respectivos requisitos de segurança da informação e comunicações dos ativos de informação.

Recomenda-se, que o detalhamento dos ativos de informação contemple também, e sempre que possível, o levantamento das interfaces e das interdependências internas e externas dos ativos de informação considerados críticos, dos órgãos ou entidades da APF, bem como os impactos quando da indisponibilidade ou destruição de tais ativos de informação, seja no caso de incidentes ou de desastres, visando atender os interesses da sociedade e do Estado.

5.3 Identificação do(s) responsável(is) – proprietário(s) e custodiante(s) - de cada ativo de informação

5.3.1 O proprietário do ativo de informação refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

5.3.2 O proprietário do ativo de informação deve assumir, no mínimo, as seguintes atividades: 1) descrever o ativo de informação; 2) definir as exigências de segurança da informação e comunicações do ativo de informação; 3) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários; 4) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo; e, 5) indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação;

5.3.3 O custodiante do ativo de informação deve proteger um ou mais ativos de informação do órgão ou entidade da APF, como é armazenado, transportado e processado, de forma a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação. Ou seja, deve proteger os contêineres dos ativos de informação, e, consequentemente, aplicar os níveis de controles de segurança conforme as exigências de segurança da informação e comunicações, comunicadas pelo(s) proprietário(s) do(s) ativo(s) de informação.

5.4 Caracterização dos contêineres dos ativos de informação

5.4.1 O contêiner é o local onde “vive” o ativo de informação, e assim, recomenda-se que o mesmo seja caracterizado, no mínimo, com as seguintes informações: lista de todos os recipientes em que um ativo da informação é armazenado, transportado ou processado, e respectiva indicação dos responsáveis por manter estes recipientes;

5.4.2 Além disso, tanto definir os limites do ambiente que deve ser examinado para o risco, quanto descrever os relacionamentos que devem ser compreendidos para atendimento das exigências de segurança da informação e comunicações, caracterizam, também, o(s) contêiner(s) do(s) ativo(s) de informação.

5.5 Definição dos requisitos de segurança da informação e comunicações dos ativos de informação

5.5.1 Os requisitos de segurança da informação e comunicações dos ativos de informação devem ser definidos por meio de critérios que atendam a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

5.5.2 Recomenda-se que os requisitos de segurança da informação e comunicações dos ativos de informação sejam categorizados, no mínimo, em 5 categorias de controle: a) tratamento da informação; b) controles de acesso físico e lógico; c) gestão de risco de segurança da informação e comunicações; d) tratamento e respostas a incidentes em redes computacionais, e, f) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação e comunicações.

5.6 Estabelecimento do valor do ativo de informação

5.6.1 Cabe ao(s) proprietário(s) dos ativos de informação indicar o valor do ativo para o negócio do órgão ou entidade da APF, considerando fatores do(s) risco(s) os quais os ativos possam estar expostos, como ameaça, vulnerabilidade e impacto;

5.6.2 O proprietário do ativo da informação deve indicar o valor do ativo, o qual deve refletir o quão cada ativo de informação é importante para a que organização alcance seus objetivos estratégicos, e o quão o ativo de informação é imprescindível aos interesses da sociedade e do Estado.

6 RESPONSABILIDADES

6.1 Cabe à Alta Administração do órgão ou entidade da APF aprovar as diretrizes gerais e o processo de Inventário e Monitoramento de Ativos de Informação observada, dentre outros, a Política de Segurança da Informação e Comunicações e a Gestão de Riscos de Segurança da Informação e Comunicações, do órgão ou entidade da APF, bem como a sua missão e os seus objetivos estratégicos;

6.2 O Gestor de Segurança da Informação e Comunicações, no âmbito de suas atribuições, é responsável pela coordenação do Inventário e Mapeamento de Ativos de Informação nos órgãos ou entidades da APF, bem como pela indicação de Agente Responsável pela gerência de tais atividades. É responsável, também, pela análise quanto aos resultados obtidos de controle dos níveis de segurança da informação e comunicações de cada ativo de informação, e conseqüente, proposição de ajustes e de medidas preventivas e próativas à Alta Direção; e

6.3 Cabe ao Agente Responsável, no mínimo, as seguintes atividades: o processo de identificação e classificação de ativos de informação; o monitoramento dos níveis de segurança dos ativos de informação junto aos proprietários e custodiantes dos ativos de informação; e, a elaboração sistemática de relatórios para os Gestores de Segurança da Informação e Comunicações.

7 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.