ANEXO

Número da Norma Complementar	Revisão	Emissão	Folha
02/CSIC/MCTIC	00	09/NOV/2017	1/50

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
Secretaria Executiva
Comitê de Segurança da Informação e Comunicações

INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

ORIGEM

Comitê de Segurança da Informação e Comunicações.

REFERÊNCIA NORMATIVA

Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.
Norma Complementar 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013.
Norma Complementar 10/IN01/DSIC/GSI/PR, de 30 de janeiro de 2012.
Lei nº 12.527, de 18 de novembro de 2011.
Decreto nº 7.724, de 16 de maio de 2012.
Portaria nº 4.711, de 18 de agosto de 2017 – Posic/MCTIC
ABNT NBR ISO/IEC 27002:2013.

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica aos Ativos de Informação dos órgãos de assistência direta e imediata ao Ministro de Estado, órgãos específicos singulares e unidades descentralizadas.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

Gilberto Kassab
Ministro

1 FINALIDADE

Estabelecer diretrizes para o Processo de Inventário e Mapeamento de Ativos de Informação do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC).

2 DISPOSIÇÕES GERAIS

2.1 O Processo de Inventário e Mapeamento de Ativos de Informação objetiva a segurança dos recursos críticos de informação do MCTIC e favorece o conhecimento, a valorização, a proteção e a manutenção dos seus ativos de informação, em conformidade com os requisitos legais, normativos e negociais aos quais se submete.

2.2 O Processo de Inventário e Mapeamento de Ativos de Informação também objetiva prover o MCTIC:

a) de um entendimento comum, consistente e inequívoco de seus ativos de informação;

b) da identificação clara de seus responsáveis: proprietários e custodiantes;

c) de um conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo;

d) de uma descrição do contêiner de cada ativo de informação;

e) da identificação do valor que o ativo representa para as áreas meio e fim do MCTIC.

2.3 O Processo de Inventário e Mapeamento de Ativos de Informação está limitado ao escopo das ações de Segurança da Informação e Comunicações no âmbito do MCTIC, e tais ações compreendem os ativos de informação considerados críticos pelo Gestor de Segurança da Informação e Comunicações do MCTIC, que deverão ter asseguradas a sua disponibilidade, integridade, confidencialidade e autenticidade.

3 TERMOS E DEFINIÇÕES

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

3.1 **Acesso -** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade. (Ref.: NC07/IN01/DSIC/GSIPR/2010);

3.2 **Agente público -** todo aquele que exerce cargo, emprego ou função no MCTIC, ainda que transitoriamente ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores públicos, militares, servidores temporários regidos pela Lei nº 8.745/1993, empregados públicos regidos pela Lei nº 9.962/2000 e colaboradores);

3.3 **Agente responsável -** servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal (APF), direta ou indireta, incumbido de chefiar e gerenciar o Processo de Inventário e Mapeamento de Ativos de Informação. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.4 **Ativo 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. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.5 **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. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.6 **Colaborador -** pessoa jurídica ou pessoa física que desempenhe atividade de interesse do MCTIC, realize estágio ou preste serviço, em caráter permanente ou eventual;

3.7 **Comitê de Segurança da Informação e Comunicações (CSIC) -** comitê instituído no âmbito dos órgãos de assistência direta e imediata ao Ministro de Estado, dos órgãos específicos singulares e das unidades descentralizadas do MCTIC, com a competência, dentre outras, de assessorar a implementação das ações de segurança da informação e comunicações do Ministério;

3.8 **Confidencialidade -** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado. (Ref.: IN GSI/PR 01/2008);

3.9 **Contêineres dos ativos de informação -** o contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.10 **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. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.11 **Custodiante do ativo de informação -** aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

3.12 **Disponibilidade -** qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados. (Ref.: Lei nº 12.527/2011);

3.13 **Documento -** unidade de registro de informações, qualquer que seja o suporte ou formato. (Ref.: Lei nº 12.527/2011);

3.14 **Estimativa de riscos -** processo utilizado para atribuir valores à probabilidade e consequências de um risco. (Ref.: NC04/IN01/DSIC/GSIPR/2013);

3.15 **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. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.16 **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. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.17 **Gestor de segurança da informação e comunicações -** responsável pelas ações de segurança da informação e comunicações no âmbito do MCTIC;

3.18 **Gestor do ativo de informação -** autoridade legal responsável pela concessão de acesso a terceiros (pode ser a autoridade marcadora, a autoridade classificadora ou a autoridade instituidora do processo);

3.19 **Informação -** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato. (Ref.: Lei nº 12.527/2011);

3.20 **Infraestrutura crítica de 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;

3.21 **Integridade -** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.22 **Inventário e Mapeamento de Ativos de Informação -** é um processo interativo e evolutivo, que contempla as seguintes atividades: a) coleta de informações gerais dos ativos de informação; b) detalhamento dos ativos de informação; c) caracterização dos contêineres dos ativos de informação; d) definição dos requisitos de segurança da informação e comunicações; e, e) estabelecimento do valor do ativo de informação;

3.23 **Parte interessada -** toda pessoa física ou jurídica que participa do processo ou rito administrativo sobre o qual demande acesso à informação. Pode ser quem provocou o processo ou o ato, o proponente, a parte citada ou a parte que se defende;

3.24 **Política de Segurança da Informação e Comunicações (Posic) -** documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações. (Ref.: IN GSI/PR 01/2008);

3.25 **Proprietário do ativo de informação -** refere-se à parte interessada do órgão ou entidade da Administração Pública Federal (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. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.26 **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. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.27 **Segurança da informação e comunicações -** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. (Ref.: IN GSI/PR 01/2008);

3.28 **Valor do ativo de informação -** valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos do MCTIC, quanto o

quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado. (Ref.: NC10/IN01/DSIC/GSIPR/2012);

3.29 **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. (Ref.: NC10/IN01/DSIC/GSIPR/2012).

4 PRINCÍPIOS E DIRETRIZES

4.1 As diretrizes gerais do Processo de Inventário e Mapeamento de Ativos de Informação consideram, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do MCTIC, estando alinhadas à sua Política de Segurança da Informação e Comunicações, bem como à Instrução Normativa GSIPR 01/2008.

4.2 O Processo de Inventário e Mapeamento de Ativos de Informação será contínuo, tendo como principal objetivo a manutenção da segurança das Infraestruturas Críticas de Informação do MCTIC, devendo produzir subsídios para suportar os seguintes processos:

a) Gestão da Segurança da Informação e Comunicações;

b) Gestão de Riscos de Segurança da Informação e Comunicações;

c) Gestão de Continuidade de Negócios.

4.3 O Processo de Inventário e Mapeamento de Ativos subsidiará propostas de novos investimentos na área de Segurança da Informação e Comunicações. Deverá, também, auxiliar o MCTIC 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 deve ser dinâmico, periódico, e estruturado, para manter a base de dados de ativos de informação atualizada e consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações. A base de dados de ativos de informação deve operar como infraestrutura material e técnica em condições de dar suporte às ações de cooperação entre entes federativos que têm sob a sua governança ativos de informação. (Ref.: NC10/IN01/DSIC/GSIPR/2012).

4.5 O Processo de Inventário e Mapeamento de Ativos de Informação é interativo e evolutivo, devendo observar, para sua consecução, a capacidade operacional da infraestrutura de Gestão da Segurança da Informação do MCTIC e dos seus demais recursos operacionais.

5 PROCEDIMENTOS

5.1 O Gestor de Segurança da Informação e Comunicações definirá a estratégia para o Processo de Inventário e Mapeamento de Ativos para cada ciclo de execução, que incluirá:

a) o escopo de coleta;

b) o conjunto mínimo de informações de cada ativo e a identificação de seus responsáveis;

c) a caracterização dos contêineres;

d) a definição dos requisitos de segurança da informação e comunicações;

e) os critérios para a definição do valor do ativo de informação.

5.2 O Processo de Inventário e Mapeamento de Ativos de Informação é composto pelas seguintes etapas:

f) Etapa 1: Coleta de informações gerais dos ativos de informação;

g) Etapa 2: Detalhamento dos ativos de informação;

h) Etapa 3: Caracterização dos contêineres dos ativos de informação;

i) Etapa 4: Definição dos requisitos de segurança da informação e comunicações;

j) Etapa 5: Estabelecimento do valor do ativo de informação.

5.2.1 **Etapa 1: Coleta de Informações Gerais dos Ativos de Informação**

5.2.1.1 Esta etapa consiste na definição dos responsáveis pela coleta e na utilização de um conjunto essencial de informações para cada ativo de informação.

5.2.1.2 Poderão fazer parte do escopo do inventário os ativos de informação do MCTIC relacionados a:

a) Tecnologia da Informação (equipamentos, sistemas, aplicativos, serviços e comunicação de dados);

b) Documentos Físicos e Digitais (ostensivos, sigilosos e classificados);

c) Processos de Negócio e seus Viabilizadores (recursos tangíveis e intangíveis).

5.2.1.3 O Gestor de Segurança da Informação e Comunicações definirá o escopo do inventário para cada ciclo de execução.

5.2.2 **Etapa 2: Detalhamento dos Ativos de Informação**

O detalhamento do ativo deve contemplar informações que:

a) determinem com clareza e objetividade o conteúdo do ativo de informação;

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

c) identifiquem o valor de cada ativo de informação;

d) identifiquem os respectivos requisitos de segurança da informação e comunicações dos ativos de informação.

5.2.3 **Etapa 3: Caracterização dos Contêineres dos Ativos de Informação**

5.2.3.1 O contêiner é o local onde "vive" o ativo de informação e, assim, recomenda-se que tal contêiner seja caracterizado, no mínimo, com a 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.

5.2.3.2 Para completa caracterização do contêiner, devem ser definidos os limites do ambiente que deve ser examinado para o risco e devem ser descritos os relacionamentos que

necessitam ser compreendidos para atendimento das exigências de segurança da informação e comunicações.

5.2.4 **Etapa 4: Definição dos Requisitos de Segurança da Informação e Comunicações**

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

5.2.4.2 Os critérios devem ser 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) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação e comunicações.

5.2.5 **Etapa 5: Estabelecimento do Valor do Ativo de Informação**

5.2.5.1 O(s) proprietário(s) do ativo da informação deve(m) 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.

5.2.5.2 Cabe ao(s) proprietário(s) dos ativos de informação indicar o valor do ativo para o negócio do Ministério, considerando fatores do(s) risco(s) aos quais os ativos possam estar expostos, como ameaça, vulnerabilidade e impacto.

6 RESPONSABILIDADES

6.1 Responsabilidade da Secretaria Executiva do MCTIC

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 MCTIC, bem como a sua missão e os seus objetivos estratégicos.

6.2 Responsabilidade do Gestor de Segurança da Informação e Comunicações

6.2.1 Coordenar o Processo de Inventário e Mapeamento de Ativos de Informação nas unidades administrativas do Ministério.

6.2.2 Indicar de Agente Responsável pela gerência das atividades do Processo de Inventário e Mapeamento de Ativos de Informação.

6.2.3 Analisar os resultados obtidos de controle dos níveis de segurança da informação e comunicações de cada ativo de informação.

6.2.4 Propor ajustes e de medidas preventivas e proativas ao órgão.

6.3 Responsabilidade do Agente Responsável

6.3.1 Executar o processo de identificação e classificação de ativos de informação;

6.3.2 Monitorar os níveis de segurança dos ativos de informação junto aos proprietários e custodiantes dos ativos de informação.

6.3.3 Elaborar sistemática de relatórios para o Gestor de Segurança da Informação e Comunicações.

6.4 **Responsabilidade do Proprietário do Ativo de Informação**

6.4.1 Descrever o ativo de informação.

6.4.2 Definir as exigências de segurança da informação e comunicações do ativo de informação;

6.4.3 Comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;

6.4.4 Buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo;

6.4.5 Indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação.

6.5 **Responsabilidade do Custodiante**

6.5.1 Proteger um ou mais ativos de informação, isto é, como o ativo é armazenado, transportado e processado, de forma a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

6.5.2 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.

7 VIGÊNCIA

Esta norma entra em vigor na data de sua publicação.