PORTARIA MCOM Nº 4.549/2021 de 28 de janeiro de 2021

Aprova a Norma Complementar para Inventário e Mapeamento de Ativos de Informação.

A GESTORA DE SEGURANÇA DA INFORMAÇÃO, no uso das atribuições que lhe confere o inciso XII, do art. 2º, da Portaria nº 67/SEI-MCOM, de 4 de março de 2021, e tendo em vista o disposto no art. 15, inciso III, do Decreto nº 9.637, de 26 de dezembro de 2018, a Portaria MCOM Nº 2.454, de 22 de abril de 2021, os arts. 10, 15 e 19, da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança institucional da Presidência da República, resolve:

Art. 1º Aprovar a Norma Complementar para Inventário e Mapeamento de Ativos de Informação.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

WANESSA QUEIROZ DE SOUZA OLIVEIRA
Gestora de Segurança da Informação

NORMA COMPLEMENTAR PARA INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

OBJETIVO
Estabelecer diretrizes para o Processo de Inventário e Mapeamento de Ativos de Informação do Ministério das Comunicações - MCOM.

APLICAÇÃO
Os termos definidos nesta norma aplicam-se a todos os agentes públicos do Ministério das Comunicações.

REFERÊNCIA LEGAL E NORMATIVA
Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
Instrução Normativa nº 2, de 24 de julho de 2020, altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
Portaria MCOM Nº 2.454, de 22 de abril de 2021, que aprova a Política de Segurança da Informação do Ministério das Comunicações;
Portaria MCOM Nº 67, de 4 de março de 2021, que designa a Gestora de Segurança da Informação do Ministério das Comunicações;
Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação;

Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;
Revisão 01 da Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

1. CONCEITOS E DEFINIÇÕES:

1.1. Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
1.2. Agente responsável pela gestão de ativos: servidor público ou empregado público, ocupante de cargo efetivo incumbido de gerenciar o processo de inventário e mapeamento de ativos de informação;
1.3. Ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
1.4. Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
1.5. Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;
1.6. Contêiner dos ativos de informação: local onde se encontra o ativo de informação. Geralmente, um contêiner descreve algum tipo de ativo tecnológico -hardware, software ou sistema de informação (mas também pode se referir a pessoas ou mídias como papel, CD-ROM ou DVD-ROM). Um contêiner, portanto, é qualquer tipo de ativo dentro do qual um ativo de informação é armazenado, transportado ou processado. Ele pode ser um único ativo tecnológico (como um servidor), uma coleção de ativos tecnológicos (como uma rede) ou uma coletânea de mídias digitais, entre outros;
1.7. Custodiante da informação: qualquer indivíduo ou estrutura de órgão ou entidade da administração pública federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança, em conformidade com as exigências de segurança da informação, comunicadas pelo proprietário da informação;
1.8. Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
1.9. Documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;
1.10. Gestão de Continuidade de Negócios: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;
1.11. Gestão de Riscos de Segurança da Informação: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;
1.12. Gestor de segurança da informação e comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do MCOM;
1.13. Informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
1.14. Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
1.15. Proprietário da informação: parte interessada do órgão ou entidade da administração pública federal, direta e indireta, ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação;
1.16. 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 MCOM, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado;

1.17. Vulnerabilidade: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha;

2 DISPOSIÇÕES GERAIS

2.1. O processo de inventário e mapeamento de ativos de informação tem o objetivo de estruturar e manter um registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

2.2. O processo de mapeamento de ativos de informação deve considerar, preliminarmente:

a) os objetivos estratégicos da organização;

b) os processos internos da organização;

c) os requisitos legais; e

d) a estrutura do órgão ou da entidade.

2.3. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter:

a) os responsáveis - proprietários e custodiantes - de cada ativo de informação;

b) as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação;

c) os contêineres de cada ativo de informação; e

d) as interfaces de cada ativo de informação e as interdependências entre eles.

2.4. O registro de ativos de informação deverá ser homologado por meio de ato do titular do órgão ou da entidade.

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

2.6. São atribuições do Gestor de Segurança da Informação:

a) coordenar o processo de inventário e mapeamento de ativos de informação nas unidades administrativas do Ministério;

b) indicar o agente responsável pela gestão de ativos de informação;

c) analisar os resultados obtidos de controle dos níveis de segurança da informação e comunicações de cada ativo de informação; e

d) propor ajustes e de medidas preventivas e proativas ao órgão.

2.7. São atribuições do agente responsável pela gestão dos ativos de informação:

a) identificar e classificar os ativos de informação por nível de criticidade;

b) identificar potenciais ameaças aos ativos de informação;

c) identificar vulnerabilidades dos ativos de informação;

d) consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

e) autorizar a atualização do relatório mencionado na alínea “d” do caput; e

f) avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

2.8. São atribuições do proprietário do ativo de informação:

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 contínuo; e

e) indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação.

2.9. São atribuições do custodiante:

a) 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; e

b) 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.

3 PROCEDIMENTOS

3.1. O Gestor de Segurança da Informação 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.

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

a) Etapa 1: Coleta de informações gerais dos ativos de informação;
b) Etapa 2: Detalhamento dos ativos de informação;
c) Etapa 3: Caracterização dos contêineres dos ativos de informação;
d) Etapa 4: Definição dos requisitos de segurança da informação e comunicações;
e) Etapa 5: Estabelecimento do valor do ativo de informação.

3.3. Etapa 1: Coleta de Informações Gerais dos Ativos de Informação

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

3.3.2. Poderão fazer parte do escopo do inventário os ativos de informação do MCOM 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).

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

3.4. Etapa 2: Detalhamento dos Ativos de Informação

3.4.1. 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.

3.5. Etapa 3: Caracterização dos Contêineres dos Ativos de Informação

3.5.1. 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.

3.5.2. 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.

3.6. Etapa 4: Definição dos Requisitos de Segurança da Informação e Comunicações

3.6.1. 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.

3.6.2. 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.

3.7. Etapa 5: Estabelecimento do Valor do Ativo de Informação

3.7.1. 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.

3.7.2. 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.

Documento assinado eletronicamente por **Wanessa Queiroz de Souza Oliveira**, **Gestora de Segurança da Informação**, em 28/01/2022, às 10:52 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **9296742** e o código CRC **AD9758B6**.

Referência: Processo nº 53115.007158/2021-12 SEI nº 9296742