MINISTÉRIO DA INFRAESTRUTURA

DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES

INSTRUÇÃO NORMATIVA Nº 20/DNIT SEDE, DE 28 DE ABRIL DE 2021

Dispõe sobre procedimentos para inventariar os ativos de informação no âmbito do Departamento Nacional de Infraestrutura de Transportes - DNIT.

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES - DNIT, no uso das atribuições que lhe conferem o inciso IV, art. 173 do Regimento Interno, aprovado pela Resolução/CONSAD nº 39, de 17/11/2020, publicada no D.O.U. de 19/11/2020, o Relato nº. 90/2021/DAF/DNIT SEDE, o qual foi incluído na Ata da 16ª Reunião Ordinária da Diretoria Colegiada, realizada em 26/04/2021 e o constante no Processo nº 50600.004922/2021-38, resolve:

Art. 1º APROVAR os procedimentos para inventariar os ativos de informação, na forma descrita abaixo, para observância e aplicação em todo o órgão.

CAPÍTULO I
DO OBJETIVO

Art. 2º O processo de Inventário e Mapeamento de Ativos de Informação tem como objetivo prover o Departamento Nacional de Infraestrutura de Transportes - DNIT:

I - de um entendimento comum, consistente e inequívoco de seus ativos de informação;

II - de uma identificação clara dos responsáveis ou proprietário(s) e os custos dos ativos de informação;

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

IV - de uma descrição do local (*contêiner*) de cada ativo de informação; e

V - de subsídios para realização de processos de segurança da informação específicos, como, por exemplo, a análise de riscos e o plano de continuidade de negócios.

CAPÍTULO II
DA FUNDAMENTAÇÃO LEGAL

Art. 3º Esta norma está em consonância com as normas legais na Administração Pública Federal e obedece as seguintes diretrizes e normas superiores:

I - a Política Nacional de Segurança da Informação - PNSI, nos Órgãos da Administração Pública Federal instituída, pelo Decreto nº 9637, de 26 de dezembro de 2018, em especial aos aos objetivos previstos em seu Art. 4º;

II - a Norma ABNT NBR ISO/IEC 27002 (17799:2005) - Tecnologia da Informação - Código de Prática para a Gestão da Segurança da Informação;

III - a Norma Complementar 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, do Departamento de Segurança da Informações e Comunicações, do Gabinete de Segurança Institucional da Presidência da República, que trata de Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal; e

IV - a Política de Segurança da Informação e Comunicações, PoSIC, do Departamento Nacional de Infraestrutura de Transportes, DNIT, criada pela Portaria no 1745, de 29 de março de 2021, publicada no Boletim Administrativo nº 060, de 30 de março de 2021, ou aquela vigente à época, que determina em suas diretrizes a realização de inventário e proteção dos ativos de informação.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para os efeitos desta Instrução Normativa são estabelecidos os seguintes conceitos e definições:

I - agente responsável - Servidor Público ocupante de cargo efetivo ou em comissão da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar o processo de Inventário e Mapeamento de Ativos de Informação;

II - ameaça – evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

III - análise de riscos – uso sistemático de informações para identificar fontes e estimar o risco. A análise de risco deve elaborar a relação dos ativos, indicar seus riscos e quais controles devem ser implementados estabelecendo os prazos;

IV - ativos de informação - são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e pessoas que a eles têm acesso;

V - 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. Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta a informação;

VI - classificação da Informação – identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de segurança da informação para assegurar que os riscos sejam reduzidos a um nível aceitável. A classificação dada à informação é uma maneira de determinar como esta informação será tratada e protegida, de acordo com seu grau de sigilo;

VII - confidencialidade - propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado. Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação;

VIII - contêineres dos ativos de informação - o contêiner é o local onde está armazenada a informação, e é caracterizado com as seguintes informações: lista de todos os recipientes em que o ativo da informação é armazenado, transportado ou processado, e respectiva indicação dos responsáveis por manter estes recipientes;

IX - 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;

X - controle - forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Também pode ser usado como um sinônimo para proteção ou contramedida. Exemplos de alguns controles importantes numa organização: privacidade de informações pessoais, documento da política de segurança da informação e gestão de incidentes de segurança da informação;

XI - custodiante, diante do Ativo de Informação – é aquele que, delegado pelo proprietário do ativo de informação, zela pelo armazenamento, transporte, processamento, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia. Dessa forma procura assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação. 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;

XII - diretriz - descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas;

XIII - disponibilidade - propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço;

XIV - 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;

XV - evento de segurança da informação e comunicações - ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

XVI - gestão de ativos – processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles de segurança da informação desses ativos;

XVII - gestão de riscos de segurança da informação e comunicações - conjunto de processos coordenados 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;

XVIII - incidente de segurança da informação - é um incidente de segurança da informação, indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XIX - informação – conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XX - 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 das atividades críticas da Organização;

XXI - infraestrutura de tecnologia da informação - são instalações prediais (energia, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

XXII - integridade – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. Consiste na fidedignidade de informações;

XXIII - plano de contingência – conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área depara-se com problemas que comprometem o andamento

normal dos processos e a consequente prestação dos serviços. É um conjunto de medidas que combinam ações preventivas e de recuperação;

XXIV - política – intenções e diretrizes globais formalmente expressas pela direção da organização;

XXV - proprietário do ativo de informação - refere-se à parte interessada do Departamento Nacional de Infraestrutura de Transportes - DNIT, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação. O proprietário pode ser designado para: um processo do negócio; um conjunto de atividades definidas; uma aplicação; ou um conjunto de dados definido;

XXVI - risco – combinação da probabilidade de um evento e dos impactos decorrentes;

XXVII - 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. Devem ser considerados os riscos relativo a ocorrência de desastres naturais (enchentes, terremotos, etc.), incêndios, desabamentos, falhas de equipamentos, acidentes, greves, terrorismo, sabotagem, ações intencionais;

XXVIII - segurança da informação e comunicações - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. Objetiva a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio;

XXIX - serviços - serviços de computação e comunicação e utilidades gerais (exemplos: aquecimento, iluminação, eletricidade, refrigeração);

XXX - 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 Departamento Nacional de Infraestrutura de Transportes - DNIT, quanto cada ativo de informação é imprescindível aos interesses da sociedade e do Estado; e

XXXI - 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.

Art. 5º A identificação e classificação de Ativos de Informação é um processo composto por 6 (seis) etapas:

I - coletar informações gerais;

II - definir as informações dos ativos;

III - identificar o(s) responsável(is);

IV - identificar os contêineres dos ativos;

V - definir os requisitos de segurança; e

VI - estabelecer o valor do ativo de informação.

Art. 6º O inventário e mapeamento de Ativos de Informação é um processo interativo e evolutivo, composto por 3 (três) etapas:

I - identificação e classificação de ativos de informação;

II - identificação de potenciais ameaças e vulnerabilidades; e

III - avaliação de riscos.

CAPÍTULO IV

DOS PRINCÍPIOS E DIRETRIZES DO PROCESSO DE INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 7º As diretrizes gerais do processo de Inventário e Mapeamento de Ativos de Informação considera os objetivos estratégicos, os processos, os requisitos legais, e a estrutura do Departamento Nacional de Infraestrutura de Transportes - DNIT, bem como à sua Política de Segurança da Informação e Comunicações.

Art. 8º São diretrizes do processo de Inventário e Mapeamento de Ativos de Informação:

I - subsidiar o Departamento Nacional de Infraestrutura de Transportes - DNIT a conhecer, valorizar, proteger e manter seus ativos de informação, em conformidade com os requisitos legais e do negócio;

II - prover o Departamento Nacional de Infraestrutura de Transportes-DNIT de um entendimento comum, consistente e inequívoco de seus ativos de informação; da identificação clara de seu (s) responsável (eis) – proprietário (s) e custo diante (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 Departamento Nacional de Infraestrutura de Transportes - DNIT;

III - 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, do DNIT, 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;

IV - 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. 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 governanças ativos de informação.

Parágrafo único. Tais diretrizes se destinam, também, a subsidiar as propostas de novos investimentos na área de segurança da Informação e Comunicações.

Art. 9º O processo de Inventário e Mapeamento de Ativos de Informação objetiva a Segurança das Infraestruturas Críticas de Informação do DNIT, 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.

CAPÍTULO V
DOS PROCEDIMENTOS

Art. 10. Deverá ser adotada uma abordagem sistemática do processo de Inventário e Mapeamento de Ativos de Informação, a qual é composto por 4 (quatro) subprocessos:

I - identificação de ativos de informação;

II - classificação da informação;

III - identificação de potenciais ameaças e vulnerabilidades; e

IV - avaliação de riscos.

§1º O subprocesso mencionado inciso I deste artigo, será tratado nesta norma e é composto por 4 (quatro) etapas:

a) coleta de informações gerais dos ativos de informação;

b) detalhamento dos ativos de informação;

c) identificação do (s) responsável (is) – proprietário (s) e custo diante (s) de cada ativo de informação;

d) caracterização dos contêineres dos ativos de informação.

§2º Os subprocessos “II”, “III” e “IV” são objetos tratados através de normas específicas abordando a Classificação da Informação e a Gestão de Riscos.

CAPÍTULO VI
DA ETAPA DE COLETA DE INFORMAÇÕES GERAIS DOS ATIVOS DE INFORMAÇÃO

Art. 11. Caberá a Coordenação de Infraestrutura de Tecnologia da Informação - COINF/CGTI, levantar as informações dos ativos de informação no prazo de 1 (um) ano a contar da data da publicação desta Norma Complementar, e, anualmente, as informações deverão ser atualizadas.

Parágrafo único. O levantamento deverá abranger a estrutura do Departamento Nacional de Infraestrutura de Transportes - DNIT em todo território nacional.

Art. 12. Deverão ser adotadas metodologias de Gestão de Riscos de Segurança da Informação e Comunicações (SIC) e de Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, que incorporem o processo de Inventário e Mapeamento de Ativos de Informação.

Art. 13. Com relação especificamente à gestão dos ativos de equipamentos de informática, equipamentos de comunicação e programas de computador, são considerados ativos, entre outros:

I - computador;

II - *notebook;*

III - monitor;

IV - *netbook;*

V - impressora;

VI - *switch;*

VII - roteador;

VIII - modem externo;

IX - servidor de rede;

X - licença de software; e

XI - equipamentos *fax*.

Art. 14. A Coordenação de Infraestrutura de Tecnologia da Informação - COINF/CGTI, deve prover uma ferramenta informatizada de inventário de ativos responsável por:

I - coletar e/ou atualizar as informações de software e hardware dos equipamentos de informática conectados. No caso de ativos fora da rede,a coleta deverá ser realizada pelos meios disponíveis (levantamentos, formulários, etc), assim como sua localização física;

II - coletar e identificar todos os ativos de rede;

III - detectar e identificar dispositivos ligados a rede, incluindo posteriormente informações para a gestão de licenças, de compras e de garantias;

IV - alertar ao administrador quando houver alterações na configuração dos componentes de hardware, ou quando houver alteração na sua conectividade ao ambiente de rede (alteração da porta de *switch* utilizada);

V - controlar as licenças de softwares instaladas nas estações da rede, visualizando o saldo das licenças de softwares, licenças faltantes e excedidas;

VI - manter um histórico de hardware e software a cada evento gerado;

VII - proporcionar um inventário detalhado e automatizado; e

VIII - enviar o agente pela rede realizando sua instalação de forma remota nas estações de trabalho da rede de dados, não necessitando visitar cada estação de trabalho para proceder esta instalação.

CAPÍTULO VII
DA ETAPA DE DETALHAMENTO DOS ATIVOS DE INFORMAÇÃO

Art. 15. O detalhamento inicial dos ativos de informação, contemplará no mínimo um conjunto de informações:

I - que determine com clareza e objetividade o conteúdo do ativo de informação;

II - que identifique o(s) responsável(is) - proprietário(s)- de cada ativo de informação;

III - necessárias à recuperação do ativo de um desastre, descrevendo o tipo do ativo, formato, localização, informações sobre cópias de segurança, informações sobre licenças, versão do aplicativo, configurações necessárias para seu funcionamento, etc;

IV - identificar os ativos de informação considerados críticos, bem como identificar as interfaces e as interdependências internas e externas destes; e

V - identificar impactos quando da indisponibilidade ou destruição de tais ativos de informação, seja no caso de incidentes ou de desastres, visando atender os processos de negócios do Departamento Nacional de Infraestrutura de Transportes - DNIT.

CAPÍTULO VIII
DA ETAPA DE IDENTIFICAÇÃO DO(S) RESPONSÁVEL(IS) - PROPRIETÁRIO(S) E CUSTODIANTE(S) - DE CADA ATIVO DE INFORMAÇÃO

Art. 16. O proprietário do ativo de informação é a parte interessada do Departamento Nacional de Infraestrutura de Transportes - DNIT, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

Art. 17. O proprietário do ativo de informação assume, no mínimo, as seguintes responsabilidades:

I - de descrever o ativo de informação;

II - de comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários.

§1º O proprietário do ativo de informação pode delegar a um custodiante as tarefas consideradas de rotina. Porém a responsabilidade sobre o ativo permanece com o proprietário.

§2º Quando de sistemas de informação complexos, pode-se definir um grupo de ativos que juntos fornecem um serviço. Neste caso, o proprietário do serviço é o responsável (área de negócios) pela entrega do serviço, incluindo o funcionamento dos ativos que provê os serviços.

CAPÍTULO IX
DA ETAPA DE CARACTERIZAÇÃO DOS CONTÊINERES DOS ATIVOS DE INFORMAÇÃO

Art. 18. Serão definidos os limites do ambiente que devem ser examinados para o risco, quanto a descrever os relacionamentos que devem ser compreendidos para atendimento das exigências de segurança da informação e comunicações, bem como caracterizar também o(s) contêiner(s) do(s) ativo(s) de informação.

CAPÍTULO X
DAS RESPONSABILIDADES

Art. 19. A Coordenação de Infraestrutura de Tecnologia da Informação - COINF/CGTI, no âmbito de suas atribuições, é responsável pela coordenação do Inventário e Mapeamento de Ativos de Informação do DNIT, bem como pela indicação de Agente Responsável pela gerência de tais atividades.

Parágrafo único. A COINF 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 consequente, proposição de ajustes e de medidas preventivas e pró ativas à Alta Direção.

CAPÍTULO XI
DAS DISPOSIÇÕES GERAIS

Art. 20. A Coordenação de Infraestrutura de Tecnologia da Informação - COINF, deverá disponibilizar um banco de dados específico para armazenar o inventário de ativos, bem como uma aplicação especializada para permitir sua gestão.

Art. 21. Esta norma deverá ser revisada anualmente, ou por deliberação do Comitê de Segurança da Informação e Comunicação do Departamento Nacional de Infraestrutura de Transportes.

Art. 22. O Comitê de Segurança da Informação e o Departamento Nacional de Infraestrutura de Transportes formalizará a proposta de revisão desta norma por meio de instrumento legal, o qual deve ser aprovado pelo Diretor-Geral do DNIT.

Art. 23. Os casos omissos serão analisados pelo Comitê de Segurança Institucional, presidido pelo Diretor-Geral ou pela autoridade a que esta atribuição seja delegada.

Art. 24. Fica revogada a Portaria nº 1.953, de 12 de dezembro de 2014, publicada no Boletim Administrativo nº 050 de 08 a 12/12/2014.

Art. 25. Esta Instrução Normativa entra em vigor em 1º de junho de 2021.

ANTÔNIO LEITE DOS SANTOS FILHO
Diretor-Geral

Documento assinado eletronicamente por **Antônio Leite dos Santos Filho**, **Diretor-Geral**, em 28/04/2021, às 18:25, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.dnit.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **8039181** e o código CRC **A1AE7C61**.

Referência: Processo nº 50600.004922/2021-38 SEI nº 8039181

Setor de Autarquias Norte | Quadra 3 | Lote A
CEP 70040-902
Brasília/DF | (061) 3315-4201

§ 1º Havendo manifestação da empresa contratada deverá esta ser submetida para análise e emissão de Parecer da Procuradoria Federal Especializada visando posterior submissão à apreciação da Diretoria Colegiada, para ratificação ou revogação da rescisão contratual;

§ 2º Nos casos de inércia da empresa contratada, findo o prazo assinalado no *caput* deste artigo, deverá a rescisão ser encaminhada para publicação.

Art. 4º O Gestor do Contrato deverá promover todos os atos necessários para a continuidade do empreendimento e/ou serviço no prazo de 30 dias a contar da publicação da rescisão unilateral, no intuito de evitar maiores prejuízos à Administração.

Art. 5º Fica vedado, o bloqueio de pagamentos devidos por serviços prestados, salvo por imposição de decisão judicial ou para resguardar a Administração de valor a ser pago a título de multa contratual.

Art. 6º Deverão os novos instrumentos contratuais firmados conter, obrigatoriamente, como cláusula contratual a observância da presente Instrução Normativa.

Art. 7º Poderão ser submetidos às penalidades legais e administrativas os gestores desta Autarquia que não observarem o preceituado na presente Instrução Normativa.

CAPÍTULO III
DISPOSIÇÕES FINAIS

Art. 8º Fica revogada a Instrução Normativa/DG nº 1, de 27/07/2010, publicada no Boletim Administrativo nº 030, de 26 a 30/07/2010.

Art. 9º Esta Instrução Normativa entra em vigor em 1º de junho de 2021.

ANTÔNIO LEITE DOS SANTOS FILHO
Diretor-Geral

INSTRUÇÃO NORMATIVA Nº 20/DNIT SEDE, DE 28 DE ABRIL DE 2021

Dispõe sobre procedimentos para inventariar os ativos de informação no âmbito do Departamento Nacional de Infraestrutura de Transportes - DNIT.

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES - DNIT, no uso das atribuições que lhe conferem o inciso IV, art. 173 do Regimento Interno, aprovado pela Resolução/CONSAD nº 39, de 17/11/2020, publicada no D.O.U. de 19/11/2020, o Relato nº 90/2021/DAF/DNIT SEDE, o qual foi incluído na Ata da 16ª Reunião Ordinária da Diretoria Colegiada, realizada em 26/04/2021 e o constante no **Processo nº 50600.004922/2021-38**, resolve:

Art. 1º **APROVAR** os procedimentos para inventariar os ativos de informação, na forma descrita abaixo, para observância e aplicação em todo o órgão.

CAPÍTULO I
DO OBJETIVO

Art. 2º O processo de Inventário e Mapeamento de Ativos de Informação tem como objetivo prover o Departamento Nacional de Infraestrutura de Transportes - DNIT:

I - de um entendimento comum, consistente e inequívoco de seus ativos de informação;

II - de uma identificação clara dos responsáveis ou proprietário(s) e os custos dos ativos de informação;

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

IV - de uma descrição do local (*contêiner*) de cada ativo de informação; e

V - de subsídios para realização de processos de segurança da informação específicos, como, por exemplo, a análise de riscos e o plano de continuidade de negócios.

CAPÍTULO II
DA FUNDAMENTAÇÃO LEGAL

Art. 3º Esta norma está em consonância com as normas legais na Administração Pública Federal e obedece as seguintes diretrizes e normas superiores:

I - a Política Nacional de Segurança da Informação - PNSI, nos Órgãos da Administração Pública Federal instituída, pelo Decreto nº 9637, de 26 de dezembro de 2018, em especial aos aos objetivos previstos em seu Art. 4º;

II - a Norma ABNT NBR ISO/IEC 27002 (17799:2005) - Tecnologia da Informação - Código de Prática para a Gestão da Segurança da Informação;

III - a Norma Complementar 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, do Departamento de Segurança da Informações e Comunicações, do Gabinete de Segurança Institucional da Presidência da República, que trata de Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal; e

IV - a Política de Segurança da Informação e Comunicações, PoSIC, do Departamento Nacional de Infraestrutura de Transportes, DNIT, criada pela Portaria no 1745, de 29 de março de 2021, publicada no Boletim Administrativo nº 060, de 30 de março de 2021, ou aquela vigente à época, que determina em suas diretrizes a realização de inventário e proteção dos ativos de informação.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para os efeitos desta Instrução Normativa são estabelecidos os seguintes conceitos e definições:

I - agente responsável - Servidor Público ocupante de cargo efetivo ou em comissão da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar o processo de Inventário e Mapeamento de Ativos de Informação;

II - ameaça – evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

III - análise de riscos – uso sistemático de informações para identificar fontes e estimar o risco. A análise de risco deve elaborar a relação dos ativos, indicar seus riscos e quais controles devem ser implementados estabelecendo os prazos;

IV - ativos de informação - são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e pessoas que a eles têm acesso;

V - 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. Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta a informação;

VI - classificação da Informação – identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de segurança da informação para assegurar que os riscos sejam reduzidos a um nível aceitável. A classificação dada à informação é uma maneira de determinar como esta informação será tratada e protegida, de acordo com seu grau de sigilo;

VII - confidencialidade - propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado. Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação;

VIII - contêineres dos ativos de informação - o contêiner é o local onde está armazenada a informação, e é caracterizado com as seguintes informações: lista de todos os recipientes em que o ativo da informação é armazenado, transportado ou processado, e respectiva indicação dos responsáveis por manter estes recipientes;

IX - 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;

X - controle - forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Também pode ser usado como um sinônimo para proteção ou contramedida. Exemplos de alguns controles importantes numa organização: privacidade de informações pessoais, documento da política de segurança da informação e gestão de incidentes de segurança da informação;

XI - custodiante, diante do Ativo de Informação – é aquele que, delegado pelo proprietário do ativo de informação, zela pelo armazenamento, transporte, processamento, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia. Dessa forma procura assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação. 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;

XII - diretriz - descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas;

XIII - disponibilidade - propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço;

XIV - 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;

XV - evento de segurança da informação e comunicações - ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

XVI - gestão de ativos – processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles de segurança da informação desses ativos;

XVII - gestão de riscos de segurança da informação e comunicações - conjunto de processos coordenados 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;

XVIII - incidente de segurança da informação - é um incidente de segurança da informação, indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XIX - informação – conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XX - 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 das atividades críticas da Organização;

XXI - infraestrutura de tecnologia da informação - são instalações prediais (energia, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

XXII - integridade – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. Consiste na fidedignidade de informações;

XXIII - plano de contingência – conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área depara-se com problemas que comprometem o andamento normal dos processos e a consequente prestação dos serviços. É um conjunto de medidas que combinam ações preventivas e de recuperação;

XXIV - política – intenções e diretrizes globais formalmente expressas pela direção da organização;

XXV - proprietário do ativo de informação - refere-se à parte interessada do Departamento Nacional de Infraestrutura de Transportes - DNIT, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação. O proprietário pode ser designado para: um processo do negócio; um conjunto de atividades definidas; uma aplicação; ou um conjunto de dados definido;

XXVI - risco – combinação da probabilidade de um evento e dos impactos decorrentes;

XXVII - 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. Devem ser considerados os riscos relativo a ocorrência de desastres naturais (enchentes, terremotos, etc.), incêndios, desabamentos, falhas de equipamentos, acidentes, greves, terrorismo, sabotagem, ações intencionais;

XXVIII - segurança da informação e comunicações - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. Objetiva a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio;

XXIX - serviços - serviços de computação e comunicação e utilidades gerais (exemplos: aquecimento, iluminação, eletricidade, refrigeração);

XXX - 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 Departamento Nacional de Infraestrutura de Transportes - DNIT, quanto cada ativo de informação é imprescindível aos interesses da sociedade e do Estado; e

XXXI - 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.

Art. 5º A identificação e classificação de Ativos de Informação é um processo composto por 6 (seis) etapas:

I - coletar informações gerais;

II - definir as informações dos ativos;

III - identificar o(s) responsável(is);

IV - identificar os contêineres dos ativos;

V - definir os requisitos de segurança; e

VI - estabelecer o valor do ativo de informação.

Art. 6º O inventário e mapeamento de Ativos de Informação é um processo interativo e evolutivo, composto por 3 (três) etapas:

I - identificação e classificação de ativos de informação;

II - identificação de potenciais ameaças e vulnerabilidades; e

III - avaliação de riscos.

CAPÍTULO IV
DOS PRINCÍPIOS E DIRETRIZES DO PROCESSO DE INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 7º As diretrizes gerais do processo de Inventário e Mapeamento de Ativos de Informação considera os objetivos estratégicos, os processos, os requisitos legais, e a estrutura do Departamento Nacional de Infraestrutura de Transportes - DNIT, bem como à sua Política de Segurança da Informação e Comunicações.

Art. 8º São diretrizes do processo de Inventário e Mapeamento de Ativos de Informação:

I - subsidiar o Departamento Nacional de Infraestrutura de Transportes - DNIT a conhecer, valorizar, proteger e manter seus ativos de informação, em conformidade com os requisitos legais e do negócio;

II - prover o Departamento Nacional de Infraestrutura de Transportes-DNIT de um entendimento comum, consistente e inequívoco de seus ativos de informação; da identificação clara de seu (s) responsável (eis) – proprietário (s) e custo diante (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 Departamento Nacional de Infraestrutura de Transportes - DNIT;

III - 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, do DNIT, 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;

IV - 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. 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 governanças ativos de informação.

Parágrafo único. Tais diretrizes se destinam, também, a subsidiar as propostas de novos investimentos na área de segurança da Informação e Comunicações.

Art. 9º O processo de Inventário e Mapeamento de Ativos de Informação objetiva a Segurança das Infraestruturas Críticas de Informação do DNIT, 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.

CAPÍTULO V
DOS PROCEDIMENTOS

Art. 10. Deverá ser adotada uma abordagem sistemática do processo de Inventário e Mapeamento de Ativos de Informação, a qual é composto por 4 (quatro) subprocessos:

I - identificação de ativos de informação;

II - classificação da informação;

III - identificação de potenciais ameaças e vulnerabilidades; e

IV - avaliação de riscos.

§1º O subprocesso mencionado inciso I deste artigo, será tratado nesta norma e é composto por 4 (quatro) etapas:

a) coleta de informações gerais dos ativos de informação;

b) detalhamento dos ativos de informação;

c) identificação do (s) responsável (is) – proprietário (s) e custo diante (s) de cada ativo de informação;

d) caracterização dos contêineres dos ativos de informação.

§2º Os subprocessos “II”, “III” e “IV” são objetos tratados através de normas específicas abordando a Classificação da Informação e a Gestão de Riscos.

CAPÍTULO VI
DA ETAPA DE COLETA DE INFORMAÇÕES GERAIS DOS ATIVOS DE INFORMAÇÃO

Art. 11. Caberá a Coordenação de Infraestrutura de Tecnologia da Informação - COINF/CGTI, levantar as informações dos ativos de informação no prazo de 1 (um) ano a contar da data da publicação desta Norma Complementar, e, anualmente, as informações deverão ser atualizadas.

Parágrafo único. O levantamento deverá abranger a estrutura do Departamento Nacional de Infraestrutura de Transportes - DNIT em todo território nacional.

Art. 12. Deverão ser adotadas metodologias de Gestão de Riscos de Segurança da Informação e Comunicações (SIC) e de Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, que incorporem o processo de Inventário e Mapeamento de Ativos de Informação.

Art. 13. Com relação especificamente à gestão dos ativos de equipamentos de informática, equipamentos de comunicação e programas de computador, são considerados ativos, entre outros:

I - computador;

II - *notebook;*

III - monitor;

IV - *netbook;*

V - impressora;

VI - *switch;*

VII - roteador;

VIII - modem externo;

IX - servidor de rede;

X - licença de software; e

XI - equipamentos *fax*.

Art. 14. A Coordenação de Infraestrutura de Tecnologia da Informação - COINF/CGTI, deve prover uma ferramenta informatizada de inventário de ativos responsável por:

I - coletar e/ou atualizar as informações de software e hardware dos equipamentos de informática conectados. No caso de ativos fora da rede,a coleta deverá ser realizada pelos meios disponíveis (levantamentos, formulários, etc), assim como sua localização física;

II - coletar e identificar todos os ativos de rede;

III - detectar e identificar dispositivos ligados a rede, incluindo posteriormente informações para a gestão de licenças, de compras e de garantias;

IV - alertar ao administrador quando houver alterações na configuração dos componentes de hardware, ou quando houver alteração na sua conectividade ao ambiente de rede (alteração da porta de *switch* utilizada);

V - controlar as licenças de softwares instaladas nas estações da rede, visualizando o saldo das licenças de softwares, licenças faltantes e excedidas;

VI - manter um histórico de hardware e software a cada evento gerado;

VII - proporcionar um inventário detalhado e automatizado; e

VIII - enviar o agente pela rede realizando sua instalação de forma remota nas estações de trabalho da rede de dados, não necessitando visitar cada estação de trabalho para proceder esta instalação.

CAPÍTULO VII
DA ETAPA DE DETALHAMENTO DOS ATIVOS DE INFORMAÇÃO

Art. 15. O detalhamento inicial dos ativos de informação, contemplará no mínimo um conjunto de informações:

I - que determine com clareza e objetividade o conteúdo do ativo de informação;

II - que identifique o(s) responsável(is) - proprietário(s)- de cada ativo de informação;

III - necessárias à recuperação do ativo de um desastre, descrevendo o tipo do ativo, formato, localização, informações sobre cópias de segurança, informações sobre licenças, versão do aplicativo, configurações necessárias para seu funcionamento, etc;

IV - identificar os ativos de informação considerados críticos, bem como identificar as interfaces e as interdependências internas e externas destes; e

V - identificar impactos quando da indisponibilidade ou destruição de tais ativos de informação, seja no caso de incidentes ou de desastres, visando atender os processos de negócios do Departamento Nacional de Infraestrutura de Transportes - DNIT.

CAPÍTULO VIII
DA ETAPA DE IDENTIFICAÇÃO DO(S) RESPONSÁVEL(IS) - PROPRIETÁRIO(S) E CUSTODIANTE(S) - DE CADA ATIVO DE INFORMAÇÃO

Art. 16. O proprietário do ativo de informação é a parte interessada do Departamento Nacional de Infraestrutura de Transportes - DNIT, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

Art. 17. O proprietário do ativo de informação assume, no mínimo, as seguintes responsabilidades:

I - de descrever o ativo de informação;

II - de comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários.

§1º O proprietário do ativo de informação pode delegar a um custodiante as tarefas consideradas de rotina. Porém a responsabilidade sobre o ativo permanece com o proprietário.

§2º Quando de sistemas de informação complexos, pode-se definir um grupo de ativos que juntos fornecem um serviço. Neste caso, o proprietário do serviço é o responsável (área de negócios) pela entrega do serviço, incluindo o funcionamento dos ativos que provê os serviços.

CAPÍTULO IX
DA ETAPA DE CARACTERIZAÇÃO DOS CONTÊINERES DOS ATIVOS DE INFORMAÇÃO

Art. 18. Serão definidos os limites do ambiente que devem ser examinados para o risco, quanto a descrever os relacionamentos que devem ser compreendidos para atendimento das exigências de segurança da informação e comunicações, bem como caracterizar também o(s) contêiner(s) do(s) ativo(s) de informação.

CAPÍTULO X
DAS RESPONSABILIDADES

Art. 19. A Coordenação de Infraestrutura de Tecnologia da Informação - COINF/CGTI, no âmbito de suas atribuições, é responsável pela coordenação do Inventário e Mapeamento de Ativos de Informação do DNIT, bem como pela indicação de Agente Responsável pela gerência de tais atividades.

Parágrafo único. A COINF 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 consequente, proposição de ajustes e de medidas preventivas e pró ativas à Alta Direção.

CAPÍTULO XI
DAS DISPOSIÇÕES GERAIS

Art. 20. A Coordenação de Infraestrutura de Tecnologia da Informação - COINF, deverá disponibilizar um banco de dados específico para armazenar o inventário de ativos, bem como uma aplicação especializada para permitir sua gestão.

Art. 21. Esta norma deverá ser revisada anualmente, ou por deliberação do Comitê de Segurança da Informação e Comunicação do Departamento Nacional de Infraestrutura de Transportes.

Art. 22. O Comitê de Segurança da Informação e o Departamento Nacional de Infraestrutura de Transportes formalizará a proposta de revisão desta norma por meio de instrumento legal, o qual deve ser aprovado pelo Diretor-Geral do DNIT.

Art. 23. Os casos omissos serão analisados pelo Comitê de Segurança Institucional, presidido pelo Diretor-Geral ou pela autoridade a que esta atribuição seja delegada.

Art. 24. Fica revogada a Portaria nº 1.953, de 12 de dezembro de 2014, publicada no Boletim Administrativo nº 050 de 08 a 12/12/2014.

Art. 25. Esta Instrução Normativa entra em vigor em 1º de junho de 2021.

ANTÔNIO LEITE DOS SANTOS FILHO
Diretor-Geral