MINISTÉRIO DA INFRAESTRUTURA
DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES

PORTARIA Nº 1745, DE 29 DE MARÇO DE 2021

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES – DNIT, no uso das atribuições que lhe conferem o art. 173 do Regimento Interno aprovado pela Resolução/CONSAD nº 39, de 17 de novembro de 2020, publicada no DOU de 19 de novembro de 2020, e

Considerando as recomendações constantes do Acórdão nº 866/2011 – TCU – Plenário e Acórdão nº 1221/2014 – TCU-Monitoramento sobre a implantação de uma completa Gestão de Segurança da Informação no DNIT;

Considerando a Portaria nº 982/DG, de 18 de outubro de 2013 e suas alterações, que institui o Comitê Gestor de Segurança da Informação e Comunicações (COSIC) e suas atribuições, e

Considerando a reunião do Comitê de Segurança da Informação e Comunicações realizada no dia 10 de março de 2021, que aprovou por unanimidade a terceira versão da Política de Segurança da Informação e Comunicações, resolve:

Art. 1º ESTABELECER a Política de Segurança da Informação e Comunicações (POSIC) do DNIT.

Art. 2º A Política de Segurança da Informação e Comunicações (POSIC) poderá ser revista, sempre que necessário, a fim de assegurar seu alinhamento às prioridades e estratégias institucionais, à disponibilidade financeira e orçamentária, e às mudanças na legislação pertinente.

CAPÍTULO I

DA FINALIDADE, DO OBJETIVO E DA ABRANGÊNCIA

Art. 3º A Política de Segurança da Informação e Comunicações - POSIC tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, pelos sistemas de informação a serem, obrigatoriamente, observadas na definição de regras operacionais e procedimentos no âmbito do Departamento Nacional de Infraestrutura de Transportes - DNIT.

Art. 4º O objetivo é estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações, no DNIT.

Art. 5º As diretrizes, instruções normativas complementares e manuais de procedimentos da POSIC do DNIT aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, bolsistas de iniciação ao trabalho, consultores externos e a quem, de alguma forma, execute atividades vinculadas a esta Autarquia.

Art. 6º Todos são responsáveis e devem estar comprometidos com a segurança da informação e comunicações.

Art. 7º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo DNIT devem atender a esta POSIC.

Art. 8º Esta política também se aplica, no que couber, ao relacionamento do DNIT com terceiros.

CAPÍTULO II

DOS CONCEITOS, DEFINIÇÕES E REFERÊNCIAS

Art. 9º No âmbito da POSIC considera-se:

I - **Agente responsável pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR:** servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal incumbido de chefiar e gerenciar a ETIR;

II - **Ameaça:** conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III - **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;

IV - **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;

V - **Capacitação em Segurança da Informação e Comunicações - SIC:** saber o que é segurança da informação e comunicações, aplicando em sua rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SIC;

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 proteção necessários a cada uma delas;

VII - **Comitê de Segurança da Informação e Comunicações - COSIC:** colegiado com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do DNIT;

VIII - **Confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

IX - **Conscientização em SIC**: atividade que tem por finalidade orientar sobre o que é Segurança da Informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros;

X - **Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

XI - **Credencial (ou conta de acesso)**: permissão, concedida por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha);

XII - **CTIR GOV:** Centro de Tratamento e Resposta a Incidentes Cibernéticos da Administração Pública Federal - APF, subordinado ao Departamento de Segurança da Informação - DSI do Gabinete de Segurança Institucional da Presidência da República - GSI;

XIII - **Custodiante:** aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia;

XIV - **Custodiante da Informação:** - qualquer indivíduo ou estrutura de órgão, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de SI comunicadas pelo proprietário da informação;

XV - **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;

XVI - **Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR:** grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do DNIT;

XVII - **Estrutura de GSIC:** grupo responsável pela gestão e execução da SIC;

XVIII - **Gestão de ativos:** processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XIV - **Gestão de continuidade:** processo abrangente de gestão 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;

XX - **Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC:** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;

XXI - **Gestão de Segurança da Informação e Comunicações - GSIC:** ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

XXII - **Gestor de Ativos de Informação:** chefe da unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

XXIII - **Gestor de SIC:** servidor nomeado pelo Diretor Geral do DNIT como responsável pela gestão de segurança da informação e comunicações no âmbito do órgão;

XXVI - **Incidente de SIC:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXV - **Informação:** dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXVI - **Infraestrutura de Tecnologia da Informação - TI:** instalações prediais (energia, água, 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;

XXVII - **Integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVIII - **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXIV - **Recursos criptográficos:** sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXX - **Risco de SIC:** 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;

XXXI - **Sensibilização em SIC:** atividade que tem por objetivo atingir uma predisposição dos participantes para uma mudança de atitude sobre a SI, de tal forma que eles possam perceber em sua rotina pessoal e profissional ações que devem ser corrigidas. É uma etapa inicial da educação em SIC;

XXXII - **Sistema estruturante:** sistema com suporte de TIC fundamental e imprescindível para o planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações de Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos ou entidades da APF, direta ou indireta, e que necessitem de coordenação central;

XXXIII - **Terceiros:** quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao DNIT;

XXXIV - **Tratamento de incidentes Cibernéticos:** serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XXXV - **Tratamento da informação:** conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; e

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

Art. 10. O Anexo I desta PoSIC enumera o arcabouço de dispositivos legais, bem como a legislação específica, de caráter federal, relacionados e/ou aplicáveis à Segurança da Informação.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 11. Toda informação produzida ou recebida pelos agentes públicos, em resultado da função exercida e/ou atividade profissional contratada, pertence ao DNIT. As exceções devem ser explícitas e formalizadas entre as partes.

Art. 12. Todos os recursos de informação do DNIT devem ser projetados para que seu uso seja consciente e responsável. Os recursos comunicacionais e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalísticos.

Art. 13. O DNIT pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada na infraestrutura provida pela Autarquia.

Art. 14. Cada usuário é responsável pela segurança das informações dentro do DNIT, principalmente daquelas que estão sob sua responsabilidade.

Art. 15. Esta POSIC e os documentos elaborados a partir dela devem obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

Art. 16. Esta Política de Segurança da Informação será implementada no DNIT por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 17. Esta POSIC define as diretrizes para a segurança da informação e comunicações do DNIT e descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

Art. 18. O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas pela Auditoria Interna, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 19. Os sistemas, as informações e os serviços do DNIT utilizados pelos usuários, no exercício de suas atividades, são de exclusiva propriedade da autarquia, não podendo ser interpretados como de uso pessoal e devem ser protegidos, segundo as diretrizes descritas nesta Política e demais regulamentações em vigor.

Art. 20. Todos os ativos de informação estão sujeitos a monitoração e auditoria. Os registros obtidos poderão ser utilizados para detecção de violações da POSIC e demais regulamentações em vigor.

Art. 21. Os recursos de tecnologia da informação de propriedade do DNIT são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração. É considerada imprópria a utilização desses recursos para propósitos não institucionais ou não autorizados. Os usuários e visitantes que tomarem conhecimento dessa prática, ou qualquer outra prática em desacordo com esta POSIC, devem levá-la ao conhecimento imediato da Coordenação Geral de Tecnologia da Informação - CGTI por meio do e-mail abuse@dnit.gov.br ou outro meio estabelecido, para que sejam aplicadas as ações cabíveis.

Art. 22. A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o reconhecimento do envolvido.

Art. 23. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação. A não designação pressupõe que o gestor é o próprio custodiante.

Art. 24. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIC e de suas normas complementares.

Art. 25. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta POSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no DNIT.

Art. 26. Qualquer tipo de dúvida sobre a POSIC, as Normas Complementares - NCs e demais regulamentações de SIC deve ser imediatamente esclarecida com a área de Gestão de Segurança da Informação.

CAPÍTULO V

DAS DIRETRIZES ESPECÍFICAS

Seção I

Controle de Acesso Físico e Lógico

Art. 27. Diretrizes específicas e procedimentos próprios de controles de acesso lógico e físico deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - Os usuários do DNIT são responsáveis pelos atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital.

II - A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento;

III - Todos os sistemas de informação do DNIT, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações;

IV - As práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança;

V - A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação;

VI - Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do DNIT ou bloqueados em caso de afastamento;

VII - O ingresso de visitantes deve ser controlado de tal forma a impedir o acesso destes às áreas de armazenamento ou processamento de informações sensíveis, salvo acompanhados e com autorização do CGTI.

Parágrafo único. Os atos que comprovadamente não forem praticados pelos titulares de suas credenciais serão alvos de auditoria, objetivando análise do incidente e o devido esclarecimento. O titular da credencial utilizada indevidamente por terceiros não deverá ser responsabilizado, quando comprovar que vinha cumprido regularmente com todas as diretrizes e normativos de segurança, principalmente no período anterior e durante a ocorrência.

Seção II

Correio Eletrônico

Art. 28. Diretrizes específicas e procedimentos próprios ao serviço de correio eletrônico (e-mail) deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

I - O uso do correio eletrônico do DNIT destina-se a fins corporativos e relacionados às atividades do usuário no âmbito da autarquia;

II - O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do DNIT;

III - São usuários do serviço de correio eletrônico corporativo os membros e servidores do DNIT, seus órgãos e unidades, os estagiários e os demais agentes públicos que oficialmente executem atividade vinculada à atuação institucional do DNIT, e que receberem o acesso ao respectivo serviço de correio.

Seção III

Utilização da Internet e Intranet

Art. 29. Diretrizes específicas e procedimentos próprios de controles de uso e acesso à Internet e Intranet deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

I - Todas as regras corporativas sobre uso de Internet e Intranet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação do DNIT deverá sempre ser privilegiada.

II - Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo. Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um servidor do quadro permanente do órgão.

III - Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet e Intranet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, caixa postal de correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

IV - O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo órgão, observando-se sempre a conduta compatível com a moralidade administrativa;

V - Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

VI - Toda alteração de nível de acesso somente será realizada mediante solicitação formal, pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pela CGTI, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade a segurança e a integridade da rede do DNIT;

VII - É vedado contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do DNIT;

VIII - O usuário poderá solicitar liberação de determinada página, com a devida justificativa, mediante requerimento formal à CGTI, nos termos do inciso VI;

IX - Somente serão liberadas as páginas analisadas e autorizadas pela CGTI;

X - A ocorrência de qualquer hipótese de má utilização da internet deverá ser comunicada, de imediato à CGTI, por meio do e-mail abuse@dnit.gov.br ou outro meio estabelecido;

XI - Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet bloqueado pela CGTI, sendo comunicado o fato à chefia imediata, podendo haver repercussão disciplinar com a aplicação das sanções legalmente previstas, assegurados o contraditório e a ampla defesa;

XII - Os navegadores de Internet e Intranet utilizados no âmbito do DNIT deverão ser homologados pela CGTI;

XIII - Os problemas técnicos verificados pelos usuários, ocorridos durante o acesso aos serviços de Internet e Intranet, devem ser imediatamente comunicados a CGTI para que sejam solucionados.

Seção IV

Recursos Computacionais

Art. 30. Os usuários devem ter acesso unicamente àqueles recursos computacionais que forem indispensáveis à realização de suas atividades no DNIT.

Art. 31. Os usuários são responsáveis pelos recursos computacionais por eles utilizados, devendo preservar a sua integridade e continuidade.

Art. 32. É vedado aos usuários do DNIT utilizar a identificação e/ou senha de outro usuário para acessar ou utilizar um recurso computacional.

Art. 33. É vedado aos usuários fazer uso de exploração de falhas de configuração, falhas de segurança ou tentar obter conhecimento de senhas especiais para alterar um Recurso Computacional.

Art. 34. Tendo em vista a preservação do ambiente computacional do DNIT, é vedado aos usuários o fornecimento de informações a terceiros sobre características, funcionalidades e configurações dos recursos de tecnologia da informação disponíveis, ressalvada a possibilidade de disposição de tais informações pela CGTI, quando o desempenho de atividades institucionais assim exigir.

Subseção I

Estações de Trabalho

Art. 35. É vedado ao usuário abrir as estações de trabalho ou modificar a configuração do hardware.

Art. 36. O usuário deve informar imediatamente à CGTI, assim como a área responsável pela gestão do patrimônio, quando identificada violação da integridade do equipamento por ele utilizado.

Art. 37. O usuário não deve cancelar o processo de verificação de vírus quando este for iniciado automaticamente na sua estação de trabalho.

Art. 38. Não é permitida a conexão de estações de trabalho particulares à rede cabeada do DNIT, portáteis ou não, à rede do DNIT, exceto em casos de comprovada necessidade, situações nas quais deverá ser assegurada a devida adoção de padrões de segurança compatíveis com o disposto nessa norma, devendo a estação de trabalho ser objeto de verificação de conformidade pela CGTI.

Art. 39. Arquivos salvos na unidade de disco local não terão garantia de *backup* e recuperação.

Art. 40. As credenciais de administrador do equipamento deverão ficar sob a guarda e responsabilidade da CGTI, restando ao usuário, ao qual se destina o equipamento, utilizá-lo mediante credenciais de "usuário comum". Ressalva-se o caso de usuários da área técnica, devidamente autorizados pela CGTI, que por força de suas funções e conhecimento técnico, se reservam ao direito de efetuar suas próprias instalações, bem como, a guarda e o uso oportuno das credenciais de administrador.

Art. 41. O compartilhamento de diretórios e arquivos em estações de trabalho somente deve ser realizado quando estritamente necessário para execução das atividades do usuário mediante solicitação formal à CGTI, devidamente justificada.

Subseção II

Servidor de Arquivos

Art. 42. Nos servidores de arquivos locais devem ser gravados:

I - Documentos relacionados ao trabalho cotidiano e à produção jurídica e administrativa local, que demande compartilhamento ou resguardo institucional;

II - Pastas particulares de correio eletrônico e das contas corporativas da unidade.

Art. 43. As permissões de acesso deverão ser concedidas em nível de grupos.

Art. 44. É proibida a gravação de material classificado como:

I - Jogos e apostas;

II - Pornografia, pedofilia, sexo, nudez, e de conteúdo adulto similar;

III - Maliciosos e/ou pirataria;

IV - Anonimadores e proxys de navegação;

V - Atividades ilegais, terroristas e violência; e

VI - Transferência ou cópia não autorizadas de material protegido por direito autoral.

Art. 45. Quando identificado pelas ferramentas de segurança, o material classificado nas categorias listadas nos incisos do artigo anterior será automaticamente bloqueado e não poderá ser objeto de pedido de liberação de acesso.

Art. 46. É obrigatório armazenar os arquivos inerentes ao serviço de cada setor em suas respectivas pastas de rede, para garantir o backup desses arquivos.

Art. 47. Não é permitido criar ou remover arquivos e pastas fora da área alocada ao respectivo Setor ou Unidade. Caso esteja em desacordo, o arquivo ou pasta será excluído sem aviso prévio.

Art. 48. É vedada a gravação de dados e informações de natureza particular.

Art. 49. Identificada ocorrência em desacordo com o disposto nos itens antecedentes, a CGTI poderá, após notificar o responsável pelo ato infracional e resguardar as evidências necessárias, excluir ou isolar arquivos, revogar acessos ou requisitar o equipamento, devendo representar acerca do fato imediatamente à autoridade responsável pela apuração da infração, nos termos do art. 116, XII, da Lei

nº 8.112, de 11 de dezembro de 1990, que estabelece que um dos deveres do servidor público federal é o de representar contra ilegalidade, omissão ou abuso de poder.

Parágrafo único. A representação de que trata este artigo deve ir acompanhada de todos os elementos probatórios obtidos pela CGTI .

Subseção III

Utilização de Software

Art. 50. No DNIT, só será permitida a utilização de softwares homologados pela CGTI, respeitando os direitos autorais e contratuais dos fabricantes, e que sejam necessários para a execução das atividades dos usuários.

Art. 51. O registro dos softwares homologados, do número de licenças disponíveis e dos softwares instalados nas estações de trabalho deve ser mantido atualizado pela CGTI.

Art. 52. O processo de homologação de software deve avaliar, sobretudo, o impacto da utilização desta na segurança da informação do DNIT e o suporte para o mesmo.

Art. 53. É vedado ao usuário efetuar réplicas dos softwares adquiridos pelo DNIT.

Art. 54. A instalação de software de outras categorias, tais como freeware (software gratuito), de domínio público (não protegido por copyright) e/ou cópias de demonstração que não sofram ação de direitos autorais, deve ser previamente requerida à CGTI.

Art. 55. A CGTI poderá remover programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa norma.

Subseção IV

Manutenção e Configuração

Art. 56. Toda solicitação de atendimento para instalação, suporte e configuração dos recursos computacionais deve ser efetuada mediante abertura de chamado à CGTI.

Art. 57. Nas dependências físicas do DNIT somente é permitida a execução dos serviços de suporte técnico nos equipamentos de propriedade da instituição ou cedidos formalmente, sendo proibida a assistência técnica em equipamentos particulares.

Art. 58. Todo equipamento que tiver a necessidade de ser deslocado para manutenção ou configuração, deverá estar devidamente identificado.

Art. 59. O usuário deve estar ciente da saída do equipamento das dependências físicas do DNIT, caso seja necessária a retirada para manutenção.

Art. 60. A saída do equipamento das dependências físicas do DNIT deverá ser autorizada pela área responsável pela gestão do patrimônio.

Subseção V

Criptografia

Art. 61. O uso de recursos criptográficos interfere na Disponibilidade, Integridade, Confidencialidade, Autenticidade - DICA, sendo, portanto, responsabilidade do Gestor de SIC a implementação dos procedimentos relativos ao seu uso, no âmbito das informações produzidas e custodiadas no DNIT, em conformidade com as orientações contidas em norma específica.

Art. 62. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade pelo seu uso.

Subseção VI

Ativos de Rede

Art. 63. As portas dos switches somente devem estar ativas se utilizadas e inventariadas.

Art. 64. Os switches e access points devem possuir controle de acesso.

Art. 65. Todo roteador utilizado na rede do DNIT deve prover, no mínimo, o uso de ACLs (Access lists) e o filtro de pacotes.

Art. 66. Todo ativo de rede deve estar em local seguro. Os switches departamentais devem estar instalados em racks devidamente fechados e seguros.

Art. 67. Os ativos de rede somente devem ser liberados para uso após a efetiva homologação, realizada em ambiente apropriado, distinto do ambiente de produção, e devidamente documentado.

Art. 68. As intervenções no ambiente de rede somente serão permitidas mediante supervisão pelos técnicos autorizados pela CGTI.

Art. 69. A CGTI reserva o direito de realizar investigações em qualquer dos equipamentos que integrem a sua rede local.

Subseção VII

Rede Wireless

Art. 70. Diretrizes específicas e procedimentos próprios referentes a utilização da Rede Wireless deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - O acesso a Rede Wireless Corporativa somente poderá ocorrer por meio dos recursos providos pelo DNIT, sendo vedado o uso de pontos de acesso particulares ou pertecentes às empresas prestadoras de serviço;

II - O acesso a Rede Wireless Corporativa realizar-se-á por credencial de acesso utilizando usuário e senha para autenticação, geridos pela CGTI;

III - Ao utilizar rede de computadores externa por meio de dispositivos portáteis de propriedade do DNIT, o usuário deve obedecer também às normas e às diretrizes daquelas redes. Em caso de divergência entre as normas das redes externas e a POSIC/DNIT, prevalece o definido nas normas do DNIT.

Seção V

Aquisição, Desenvolvimento e Manutenção de Sistemas

Art. 71. Diretrizes específicas e procedimentos próprios da aquisição, desenvolvimento e manutenção de Sistemas deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - A Estrutura de SIC deve estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção;

II - O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

Seção VI

Gestão de Ativos de Informação

Art. 72. Os ativos de informação devem:

I - Ser inventariados e protegidos;

II - Ter identificados os seus proprietários e custodiantes;

III - Ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - Ter a sua entrada e saída nas dependências do DNIT autorizadas e registradas por autoridade competente;

V - Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI - Ser regulamentados por norma específica quanto a sua utilização; e

VII - Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 73. O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo, conforme disposto em normas e legislação específica de classificação de informação.

Art. 74. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

Art. 75. É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo DNIT.

Seção VII

Gestão de Riscos de Segurança da Informação e Comunicações

Art. 76. Diretrizes e princípios específicos, acerca dos procedimentos, definições preliminares, análise/avaliação dos riscos e formulação de Plano de Tratamento dos Riscos devem ser fixados em norma complementar, em observância ao estabelecido pela Norma Complementar Nº 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, em especial:

I - Convém que o processo de Gestão de Riscos de Segurança da Informação e Comunicações esteja alinhado ao planejamento estratégico e também, com o processo maior de gestão de riscos corporativos, se esse existir;

II - Os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco;

III - A GRSIC é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações, levando em consideração o planejamento, execução, análise crítica e melhoria da SIC no DNIT;

IV - O Gestor de Segurança da Informação e Comunicações, no âmbito de suas atribuições, é responsáveis pela coordenação da Gestão de Riscos de Segurança da Informação e Comunicações no DNIT.

Seção VIII

Tratamento de Incidentes

Art. 77. A CGTI deverá manter Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), instituída pelo Comitê da Segurança da Informação e Comunicações (COSIC), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas à incidentes de segurança em rede de computadores:

I - Deverá ser elaborado documento de constituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, o qual designará suas atribuições e seu escopo de atuação;

II - A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos será composta, preferencialmente, por servidores públicos ocupantes de cargo efetivo, com perfil técnico adequado com as atividades dessa equipe;

III - O Agente responsável pela ETIR deverá ser servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, em atuação no DNIT, formalmente designado para chefiar e gerenciar a ETIR.

Art. 78. Os eventos e incidentes de SIC devem ser tratados de acordo com um Plano de Gerenciamento de Incidentes específico, comunicados e registrados.

Art. 79. No tratamento de incidentes cibernéticos, a ETIR, responsável pelo tratamento e resposta ao incidente, deverá considerar, no mínimo, as seguintes diretrizes:

I - Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas;

II - O tratamento da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;

III - Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, o Gestor de Segurança da Informação ou membros do COSIC tem como dever, sem prejuízo de suas demais atribuições, providenciar o acionamento das autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços do DNIT;

IV - A atuação da Equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo, sem prejuízo das demais metodologias e padrões conhecidos;

V - A ocorrência de incidentes de segurança em redes de computadores do DNIT poderá ser comunicada ao Centro de Tratamento de Incidentes Cibernéticos da Administração Pública Federal (CTIR.Gov), conforme procedimentos a serem definidos pelo próprio centro, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas.

VI - As notificações enviadas pela Equipe ao Centro de Tratamento e Resposta à Incidentes Cibernéticos de Governo, bem como a troca de informações entre as Equipes existentes, devem seguir os formatos e os procedimentos que serão estabelecidos pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo.

Seção IX

Gestão de Continuidade

Art. 80. Objetivando a implantação do processo de Gestão de Continuidade de Negócios, visando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, o DNIT deverá manter um Programa de Gestão da Continuidade de Negócios, conforme a Norma Complementar nº 06/IN01/DSIC/GSI/PR de 11 de novembro de 2009.

Art. 81. A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional do DNIT.

Art. 82. As medidas constantes do Plano de Gerenciamento de Incidentes deverão assegurar a disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o

objetivo de minimizar o impacto sofrido diante do acontecimento situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

Seção X

Avaliação de Conformidade

Art. 83. A Auditoria Interna do DNIT deverá avaliar, periodicamente, por meio de verificações de conformidade das práticas de SIC, a aderência desta POSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC, no âmbito das responsabilidades de cada unidade administrativa da Autarquia:

Art. 84. A Estrutura de GSIC do DNIT deverá avaliar, periodicamente, por meio de verificação de conformidade das práticas de SIC, a aderência desta POSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC, no âmbito das atividades e dos serviços sob a responsabilidade da CGTI:

I - A execução da verificação de conformidade será realizada pela Estrutura de GSIC, podendo, com a prévia aprovação do COSIC, ser subcontratada no todo ou em parte;

II - É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados;

III - A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pela Estrutura de GSIC e aprovado pelo COSIC;

IV - O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos;

V - A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 85. Os resultados de cada ação de verificação de conformidade descritas nos Art. 82 e Art. 83 serão documentados em relatório de avaliação de conformidade, o qual será encaminhado ao Gestor de SIC e, por ele ao Gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

Art. 86. As não-conformidades relativas ao descumprimento de legislações, normas e procedimentos serão consideradas riscos de SIC e devem ser tratadas.

Seção XI

Plano de Investimento em Segurança da Informação e Comunicação

Art. 87. Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos, que poderá estar contido no plano de investimentos geral da TI.

Art. 88. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 89. O plano de investimentos, assim como a correspondente proposta orçamentária, será aprovado pelo COSIC, mediante recomendação elaborada pela Estrutura de GSIC.

Art. 90. Caso haja limitação na execução orçamentária ou força de trabalho considerada insuficiente para cumprir o plano, caberá ao COSIC realizar a correspondente revisão do plano de investimentos, considerando os riscos a serem tratados.

Seção XII

Propriedade Intelectual

Art. 91. As informações produzidas por usuários no exercício de suas funções, são patrimônio intelectual do DNIT e não cabe a seus criadores qualquer forma de direito autoral.

Art. 92. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do DNIT em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela Autarquia, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Diretor Geral, nos demais casos, observando a legislação em vigor.

Art. 93. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 94. Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos desde que expressamente autorizadas pelo DNIT.

Seção XIII

Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 95. Os contratos, convênios, acordos e instrumentos congêneres que não estejam em conformidade com o exposto nos Art. 23 e Art. 24 desta POSIC, devem fazê-lo no próximo aditivo a ser lavrado.

Art. 96. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

CAPÍTULO VI

DA RESPONSABILIZAÇÃO

Art. 97. Ações que violem a POSIC ou a inobservância de quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SIC serão devidamente apuradas e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor, assegurados a ampla defesa e o contraditório.

Art. 98. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor.

Art. 99. O uso de qualquer recurso em inobservância das normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos administrativo, civil e criminal, em que a instituição cooperará ativamente com as autoridades competentes.

Art. 100. Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o DNIT e/ou terceiros. Portanto, o usuário vinculado a tais dispositivos identificadores será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal), sendo que o uso dos dispositivos e/ou senhas de identificação de outra pessoa viola as regras de segurança e poderá resultar na aplicação de medidas administrativas, cíveis e judiciais cabíveis.

CAPÍTULO VII

DA COMPOSIÇÃO E COMPETÊNCIA

Seção I

Do Gestor de Segurança da Informação

Art. 101. O gestor de segurança da informação será designado dentre os servidores públicos civis ocupantes de cargo efetivo e militares de carreira do órgão ou entidade, com formação ou capacitação técnica compatível às suas atribuições.

Art. 102. Compete ao gestor de segurança da informação:

I - Coordenar o Comitê de Segurança da Informação;

II - Coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do DNIT, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - Assessorar a alta administração na implementação da Política de Segurança da Informação;

IV - Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - Promover a divulgação da política e das normas internas de segurança da informação do DNIT a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

VI - Incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - Propor recursos necessários às ações de segurança da informação;

VIII - Acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX - Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - Manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Seção II

Do Comitê de Segurança da Informação

Art. 103. O Comitê de Segurança da Informação e Comunicações terá, no mínimo, a seguinte composição:

I - o gestor de segurança da informação, que o coordenará;

II - um representante da DIREX;

III - um representante de cada unidade finalística do DNIT; e

IV - o Coordenador-Geral de Tecnologia da Informação.

Art. 104. O Comitê de Segurança da Informação e Comunicações possui as seguintes atribuições:

I - Assessorar a implementação das ações de segurança da informação;

II - Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV - Propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V - Avaliar, revisar e analisar criticamente a POSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais do DNIT e às legislações vigentes;

VI - Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIC do DNIT;

VII - Deliberar sobre normas internas de segurança da informação.

Art. 105. O COSIC poderá estabelecer a periodicidade de suas reuniões, bem como a realização de reuniões extraordinárias, garantindo a frequência mínima anual.

Seção III

Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

Art. 106. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos tem como atribuições:

I - Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

II - Promover a recuperação de sistemas;

III - Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

IV - Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

V - Analisar ataques e intrusões na rede do DNIT;

VI - Executar as ações necessárias para tratar quebras de segurança;

VII - Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

VIII - Cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

IX - Participar em fóruns, redes nacionais e internacionais relativas à SIC.

Seção IV

Dos Gestores dos Ativos de Informação e dos Custodiantes

Art. 107. Cabe ao Gestor do Ativo de Informação:

I - Garantir a segurança dos ativos de informação sob sua responsabilidade;

II - Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta POSIC;

III - Conceder e revogar acessos aos ativos de informação;

IV - Comunicar à ETIR a ocorrência de incidentes de SIC; e

V - Designar custodiante do ativo de informação, quando aplicável.

Art. 108. Cabe ao custodiante do ativo de informação proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta POSIC.

Seção V

Das competências e responsabilidades dos demais envolvidos

Art. 109. Cabe ao titular de cada unidade administrativa do DNIT:

I - Corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua responsabilidade;

II - Conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

III - Incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

IV - Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

V - Informar à CGGP a movimentação de servidores de sua unidade;

VI - Informar à CGTI a movimentação de funcionários terceirizado de sua unidade;

VII - Realizar o tratamento e a classificação da informação;

VIII - Autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;

IX - Comunicar à ETIR os casos de quebra de segurança; e

X - Manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

Art. 110. Cabe aos terceiros e fornecedores, conforme previsto em contrato:

I - Tomar conhecimento desta POSIC;

II - Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

III - Fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Art. 111. Cabe aos usuários:

I - Conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta POSIC, bem como os demais normativos e resoluções relacionados à SIC;

II - Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e

III - Comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à ETIR.

CAPÍTULO VIII

DA ESTRUTURA NORMATIVA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 112. Os documentos que comporão a estrutura normativa de gestão de segurança da informação serão divididos em três categorias:

I - Política (POSIC) – nível estratégico: constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o DNIT decidiu incorporar à sua gestão de acordo

com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados;

II - Normas complementares à POSIC – nível tático: portarias, instruções normativas ou resoluções que especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar o cenário definido estrategicamente nas diretrizes da política;

III - Procedimentos Complementares à POSIC e às suas Normas Complementares – nível operacional: ofícios-circulares, procedimentos operacionais padrão e manuais que instrumentalizam o disposto nas normas e na política, permitindo sua direta aplicação nas atividades do DNIT.

Seção I

Atualização

Art. 113. A SIC, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

Art. 114. Os instrumentos normativos gerados a partir desta POSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal, ou conforme os seguintes critérios:

I - Política de Segurança da Informação e Comunicações (POSIC):

a) Nível de Aprovação: Diretoria Geral;

b) Periodicidade de Revisão: A periodicidade para a revisão da Política de Segurança da Informação não deve exceder 4 (quatro) anos.

II - Normas complementares à POSIC:

a) Nível de Aprovação: Comitê de Segurança da Informação e Comunicações (COSIC);

b) Periodicidade de Revisão: não deve exceder 4 (quatro) anos.

III - Procedimentos complementares à POSIC e às suas Normas Complementares:

a) Nível de Aprovação: Coordenação Geral de Tecnologia da Informação – CGTI;

b) Periodicidade de Revisão: não deve exceder 4 (quatro) anos.

Seção II

Divulgação e acesso à estrutura normativa

Art. 115. Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados a todos os agentes públicos e prestadores de serviços do DNIT e também publicadas na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 116. Fica revogada a Portaria/DG nº 721, de 27 de Abril de 2016, publicada no Boletim Administrativo nº 077, de 28 de Abril de 2016.

Art. 117. Esta Portaria entra em vigor em 03 de maio de 2021.

ANTÔNIO LEITE DOS SANTOS FILHO
Diretor-Geral

ANEXO

1. Dispositivos legais de caráter federal, aplicáveis à Segurança da Informação:

I - Constituição Federal, art. 5º, inciso X. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.

II - Constituição Federal, art. 5º, inciso XII. Sigilo dos dados telemáticos e das comunicações privadas.

III - Constituição Federal, art. 5º, inciso XIV. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.

IV - Constituição Federal, art. 5º, inciso XXXIII e art. 37, § 3º, inciso II. Disponibilidade das informações constantes nos órgãos públicos.

V - Constituição Federal, art. 5º, inciso XXXIV. Disponibilidade das informações constantes nos órgãos públicos.

VI - Constituição Federal, art. 23, incisos III e IV. Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.

VII - Constituição Federal, art. 216, § 2º. Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.

VIII - Constituição Federal, art. 37, caput. Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.

IX - Constituição Federal, art. 37, § 6º e Código Civil, art. 43. Responsabilidade objetiva do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.

X - Constituição Federal, art. 37, § 7º. Necessidade de regulamentação do acesso a informações privilegiadas.

XI - Consolidação das Leis do Trabalho - CLT, art. 482, alínea "g". Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).

XII - Código de Conduta da Alta Administração, art. 5º, § 4º. Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública).

XIII - Código de Conduta da Alta Administração, art.14, inciso II. Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.

XIV - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "h" do inciso XV da Seção II. Proteção da integridade das informações públicas.

XV - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "l" do inciso XV da Seção II. Proteção da disponibilidade das informações públicas.

XVI - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso X da Seção I. Proteção da disponibilidade das informações públicas.

XVII - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso VII da Seção I. Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.

XVIII - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso IX da Seção I. Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.

XIX - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "e" do inciso XIV da Seção II. Disponibilidade das comunicações.

XX - Código de Propriedade Industrial, art. 75. Sigilo das patentes de interesse da defesa nacional.

XXI - Código de Defesa do Consumidor, arts. 43 e 44. Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.

XXII - Código Penal, art. 151. Proteção do sigilo, integridade e disponibilidade das informações de caráter pessoal veiculadas através dos meios de comunicação.

XXIII - Código Penal, art. 152. Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.

XXIV - Código Penal, art. 153. Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.

XXV - Código Penal, art. 154. Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.

XXVI - Código Penal, art. 184, § 3º. Proteção da autenticidade.

XXVII - Código Penal, art. 297. Proteção da integridade e autenticidade dos documentos públicos.

XXVIII - Código Penal, art. 298. Proteção da integridade e autenticidade dos documentos particulares.

XXIX - Código Penal, art. 305. Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.

XXX - Código Penal, art. 307. Proteção da autenticidade.

XXXI - Código Penal, art. 313-A. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.

XXXII - Código Penal, art. 313-B. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.

XXXIII - Código Penal, art. 314. Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.

XXXIV - Código Penal, art. 325. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

XXXV - Código Processo Penal, art. 20. Proteção de informações sigilosas.

XXXVI - Código Processo Penal, art. 207. Proteção do sigilo profissional.

XXXVII - Código Processo Penal, art. 745. Proteção de informações sigilosas relacionadas ao condenado.

XXXVIII - Código Tributário Nacional, art. 198. Proteção do sigilo fiscal.

XXXIX - Código de Processo Civil, art. 388, inciso II, c/c art. 404, inciso IV. Proteção da privacidade de seus clientes.

XL - Código de Processo Civil, art. 448, inciso II c/c art. 457, §3º. Proteção da privacidade de seus clientes.

XLI - Instrução Normativa nº 1/2019 - Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e integrantes do Sistema de Administração dos Recursos de Informação (SISP) do Poder Executivo Federal.

XLII - Lei nº 6.538/1978, art. 41. Proteção da privacidade de correspondência.

XLIII - Lei nº 7.170/1983, art. 13. Proteção das informações sigilosas relacionadas à segurança nacional.

XLIV - Lei nº 7.232/1984, art. 2º, inciso VIII. Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.

XLV - Lei nº 7.492/1986, art. 18. Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.

XLVI - Lei nº 8.027/1990, artigo 5º, inciso I. Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.

XLVII - Lei nº 8.027/1990, artigo 5º, parágrafo único, inciso V. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

XLVIII - Lei nº 8.112/1990, art. 116, inciso VIII. Sigilo das informações produzidas ou conhecidas no exercício de cargo ou função pública.

XLIX - Lei nº 8.112/1990, art. 132, inciso IX. Proteção das informações sigilosas acessadas no exercício de cargo ou função pública.

L - Lei nº 8.137/1990, art. 3º, inciso I. Proteção da disponibilidade de informações para manutenção da ordem tributária.

LI - Lei nº 8.429/1992, art.11, incisos III, IV e VII. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público, bem como garantia de publicidade das informações de interesse coletivo ou geral que devem ser divulgadas por ato oficial.

LII - Lei nº 8.429/1992, art. 13. Disponibilidade de informações pessoais do agente público para o Poder Público e veracidade dos dados.

LIII - Lei nº 8.443/1992, art. 86, inciso IV. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

LIV - Lei Complementar nº 75/1993, art. 8º incisos II e VIII, §§ 1º e 2º. Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

LV - Lei nº 8.625/1993, art. 26, inciso I, alínea "b" e inciso II. Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

LVI - Lei nº 8.906/1994, art. 7º, inciso XIX. Proteção da privacidade do cliente do advogado.

LVII - Lei nº 9.100/1995, art. 67, incisos VII e VIII. Proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas.

LVIII - Lei nº 9.279/1996, art. 195, inciso XI. Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.

LIX - Lei nº 9.296/1996, art. 10. Sigilo dos dados e das comunicações privadas.

LX - Lei nº 9.472/1997, art. 3º, inciso V. Sigilo das comunicações.

LXI - Lei nº 9.472/1997, art. 3º, inciso VI. Proteção de informações pessoais de caráter sigiloso.

LXII - Lei nº 9.472/1997, art. 3º, inciso IX. Proteção de informações pessoais de caráter sigiloso.

LXIII - Lei nº 9.504/1997, art. 72. Proteção da integridade das informações de caráter eleitoral e dos equipamentos.

LXIV - Lei nº 9.605/1998, art. 62. Disponibilidade e integridade de dados e informações.

LXV - Lei nº 10.683/2003, art. 6º. Todos os aspectos da segurança da informação.

LXVI - Lei nº 10.703/2003, arts. 1º , 2º e 3º. Disponibilidade de dados cadastrais para fins de investigação criminal e sigilo nas demais hipóteses.

LXVII - Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

LXVIII - Decreto 9.819/2019 art. 2º, inciso II, alínea “j”.

LXIX - Decreto nº 5.483/2005, arts. 3º e 11. Disponibilidade de informações pessoais do agente público para o Poder Público e dever de sigilo por parte da Controladoria-Geral da União.

LXX - Decreto nº 5.687/2006, arts.10 e 13 do Anexo. Disponibilidade das informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos.

LXXI - Decreto nº 6.029/2007, inciso II do art. 1º. Disponibilidade das informações constantes nos registros públicos.

LXXII - Decreto nº 6.029/2007, art. 10. Sigilo da identidade do denunciante e sigilo do processo para proteção da honra e da imagem do investigado antes da prolação da decisão pela Comissão de Ética.

LXXIII - Decreto nº 6.029/2007, art. 13. Sigilo do processo administrativo por infração ética antes da prolação da decisão e publicidade após o término e aplicação das penalidades.

LXXIV - Decreto nº 6.029/2007, art. 22. Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética Pública.

Art. 116. Legislação específica de caráter federal relacionada à Segurança da Informação:

I - Lei nº 7.232/1984 Dispõe sobre a Política Nacional de Informática, e dá outras providências.

II - Lei nº 8.248/1991 Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências, observada suas atualizações.

III - Lei nº 9.296/1996 Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.

IV - Lei nº 9.472/1997 Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.

V - Lei nº 9.507/1997 Regula o direito de acesso a informações e disciplina o rito processual do habeas data.

VI - Lei nº 9.609/1998 Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.

VII - Lei nº 9.883/1999 Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.

VIII - Lei nº 8.159/1991 Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.

IX - Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

X - Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

XI - Lei nº 10.973, de 02 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.

XII - Lei nº 12.527, de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

XIII - Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil; e dá outras providências.

XIV - Decreto nº 2.295, de 04 de agosto de 1997. Regulamenta o disposto no art. 24, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Neste caso o processo deverá ser sigiloso, excetuando-se a publicidade das compras governamentais.

XV - Decreto nº 2.556, de 20 de abril de 1998. Regulamenta o registro previsto no art. 3º da Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.

XVI - Decreto nº 3.294, de 15 de dezembro de 1999. Institui o Programa Sociedade da Informação, com objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira.

XVII - Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

XVIII - Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.

XIX - Decreto nº 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

XX - Decreto nº 4.073, de 03 de janeiro de 2002. Regulamenta a Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados, observadas as suas atualizações.

XXI - Decreto nº 4.376, de 13 de setembro de 2002. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.

XXII - Decreto nº 4.522, de 17 de dezembro de 2002. Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.

XXIII - Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento, observadas as suas atualizações.

XXIV - Decreto nº 8,985, de 2017. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Instituto Nacional de Tecnologia da Informação - ITI, remaneja cargos em comissão e substitui cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS por Funções Comissionadas do Poder Executivo - FCPE.

XXV - Decreto nº 4.829, de 03 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.

XXVI - Decreto nº 5.450, de 31 de maio de 2005. Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.

XXVII - Decreto nº 9.283, de 2018. Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, a Lei nº 13.243, de 11 de janeiro de 2016, o art. 24, § 3º, e o art. 32, § 7º, da Lei nº 8.666, de 21 de junho de 1993, o art. 1º da Lei nº 8.010, de 29 de março de 1990, e o art. 2º, caput, inciso I, alínea "g", da Lei nº 8.032, de 12 de abril de 1990, e altera o Decreto nº 6.759, de 5 de fevereiro de 2009, para estabelecer medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação tecnológica, ao alcance da autonomia tecnológica e ao desenvolvimento do sistema produtivo nacional e regional.

XXVIII - Decreto nº 9.668, de 2019. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República e altera o quantitativo de Gratificações de Exercício de Cargo em Confiança devida a Militares - RMP.

XXIX - Decreto nº 6.605, de 14 de outubro de 2008. Dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.

XXX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética.114

XXXI - Instrução Normativa GSI Nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, observadas as suas atualizações e normas complementares.

XXXII - Resolução nº 338 do STF, de 11 de abril de 2007. Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do STF, alterada pela Resolução nº 579, de 25 de maio de 2016.

XXXIII - Portaria nº 93, de 26 de setembro de 2019. Aprova o Glossário de Segurança da Informação.

2. Normas técnicas relacionadas à segurança da informação:

I - ISO/IEC TR 13335-3:1998. Esta norma fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1 e TR ISO/IEC 13335-2. As orientações são projetadas para auxiliar o incremento da segurança na TI.

II - ISO/IEC GUIDE 51:1999. Esta norma fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos. É aplicável a qualquer aspecto de segurança relacionado a pessoas, propriedades, ao ambiente, ou a uma combinação de um ou mais destes (por exemplo, somente pessoas; pessoas e propriedades; pessoas, propriedades e o ambiente).

III - ISO/IEC GUIDE 73:2002. Esta norma fornece definições genéricas de termos de gestão de riscos para a elaboração de normas. Seu propósito é ser um documento genérico de alto nível voltado para a preparação ou revisão de normas que incluam aspectos de gestão de riscos.

IV - ABNT NBR ISO IEC 17799: 2005. Esta norma é equivalente à ISO/IEC 17799:2005. Consiste em um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.

V - ABNT NBR ISO/IEC 27001:2013. Esta norma é usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Aplicável a qualquer organização, independentemente do seu ramo de atuação, define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.

VI - ABNT NBR ISO/IEC 27002:2013. Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

Documento assinado eletronicamente por **Antônio Leite dos Santos Filho**, **Diretor-Geral**, em 29/03/2021, às 13:51, 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 **7832269** e o código CRC **7BB5E22B**.

Referência: Processo nº 50600.019695/2020-64 SEI nº 7832269

Setor de Autarquias Norte | Quadra 3 | Lote A
CEP 70040-902
Brasília/DF |

DIREÇÃO SUPERIOR

ATOS DA DIRETORIA-GERAL

PORTARIA Nº 1745, DE 29 DE MARÇO DE 2021

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES – DNIT, no uso das atribuições que lhe conferem o art. 173 do Regimento Interno aprovado pela Resolução/CONSAD nº 39, de 17 de novembro de 2020, publicada no DOU de 19 de novembro de 2020, e

Considerando as recomendações constantes do Acórdão nº 866/2011 – TCU – Plenário e Acórdão nº 1221/2014 – TCU-Monitoramento sobre a implantação de uma completa Gestão de Segurança da Informação no DNIT;

Considerando a Portaria nº 982/DG, de 18 de outubro de 2013 e suas alterações, que institui o Comitê Gestor de Segurança da Informação e Comunicações (COSIC) e suas atribuições, e

Considerando a reunião do Comitê de Segurança da Informação e Comunicações realizada no dia 10 de março de 2021, que aprovou por unanimidade a terceira versão da Política de Segurança da Informação e Comunicações, resolve:

Art. 1º **ESTABELECER** a Política de Segurança da Informação e Comunicações (POSIC) do DNIT.

Art. 2º A Política de Segurança da Informação e Comunicações (POSIC) poderá ser revista, sempre que necessário, a fim de assegurar seu alinhamento às prioridades e estratégias institucionais, à disponibilidade financeira e orçamentária, e às mudanças na legislação pertinente.

CAPÍTULO I
DA FINALIDADE, DO OBJETIVO E DA ABRANGÊNCIA

Art. 3º A Política de Segurança da Informação e Comunicações - POSIC tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, pelos sistemas de informação a serem, obrigatoriamente, observadas na definição de regras operacionais e procedimentos no âmbito do Departamento Nacional de Infraestrutura de Transportes - DNIT.

Art. 4º O objetivo é estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações, no DNIT.

Art. 5º As diretrizes, instruções normativas complementares e manuais de procedimentos da POSIC do DNIT aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, bolsistas de iniciação ao trabalho, consultores externos e a quem, de alguma forma, execute atividades vinculadas a esta Autarquia.

Art. 6º Todos são responsáveis e devem estar comprometidos com a segurança da informação e comunicações.

Art. 7º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo DNIT devem atender a esta POSIC.

Art. 8º Esta política também se aplica, no que couber, ao relacionamento do DNIT com terceiros.

CAPÍTULO II
DOS CONCEITOS, DEFINIÇÕES E REFERÊNCIAS

Art. 9º No âmbito da POSIC considera-se:

I - Agente responsável pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal incumbido de chefiar e gerenciar a ETIR;

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

III - 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;

IV - 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;

V - Capacitação em Segurança da Informação e Comunicações - SIC: saber o que é segurança da informação e comunicações, aplicando em sua rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SIC;

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 proteção necessários a cada uma delas;

VII - Comitê de Segurança da Informação e Comunicações - COSIC: colegiado com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do DNIT;

VIII - Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

IX - Conscientização em SIC: atividade que tem por finalidade orientar sobre o que é Segurança da Informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros;

X - Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

XI - Credencial (ou conta de acesso): permissão, concedida por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha);

XII - CTIR GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos da Administração Pública Federal - APF, subordinado ao Departamento de Segurança da Informação - DSI do Gabinete de Segurança Institucional da Presidência da República - GSI;

XIII - Custodiante: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia;

XIV - Custodiante da Informação: - qualquer indivíduo ou estrutura de órgão, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de SI comunicadas pelo proprietário da informação;

XV - 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;

XVI - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do DNIT;

XVII - Estrutura de GSIC: grupo responsável pela gestão e execução da SIC;

XVIII - Gestão de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XIV - Gestão de continuidade: processo abrangente de gestão 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;

XX - Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;

XXI - Gestão de Segurança da Informação e Comunicações - GSIC: ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

XXII - Gestor de Ativos de Informação: chefe da unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

XXIII - Gestor de SIC: servidor nomeado pelo Diretor Geral do DNIT como responsável pela gestão de segurança da informação e comunicações no âmbito do órgão;

XXVI - Incidente de SIC: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXV - Informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXVI -**Infraestrutura de Tecnologia da Informação - TI:** instalações prediais (energia, água, 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;

XXVII - **Integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVIII - **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXIV - **Recursos criptográficos:** sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXX - **Risco de SIC:** 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;

XXXI - **Sensibilização em SIC:** atividade que tem por objetivo atingir uma predisposição dos participantes para uma mudança de atitude sobre a SI, de tal forma que eles possam perceber em sua rotina pessoal e profissional ações que devem ser corrigidas. É uma etapa inicial da educação em SIC;

XXXII - **Sistema estruturante:** sistema com suporte de TIC fundamental e imprescindível para o planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações de Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos ou entidades da APF, direta ou indireta, e que necessitem de coordenação central;

XXXIII - **Terceiros:** quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao DNIT;

XXXIV - **Tratamento de incidentes Cibernéticos:** serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XXXV - **Tratamento da informação:** conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; e

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

Art. 10. O Anexo I desta PoSIC enumera o arcabouço de dispositivos legais, bem como a legislação específica, de caráter federal, relacionados e/ou aplicáveis à Segurança da Informação.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 11. Toda informação produzida ou recebida pelos agentes públicos, em resultado da função exercida e/ou atividade profissional contratada, pertence ao DNIT. As exceções devem ser explícitas e formalizadas entre as partes.

Art. 12. Todos os recursos de informação do DNIT devem ser projetados para que seu uso seja consciente e responsável. Os recursos comunicacionais e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalísticos.

Art. 13. O DNIT pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada na infraestrutura provida pela Autarquia.

Art. 14. Cada usuário é responsável pela segurança das informações dentro do DNIT, principalmente daquelas que estão sob sua responsabilidade.

Art. 15. Esta POSIC e os documentos elaborados a partir dela devem obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

Art. 16. Esta Política de Segurança da Informação será implementada no DNIT por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 17. Esta POSIC define as diretrizes para a segurança da informação e comunicações do DNIT e descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

Art. 18. O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas pela Auditoria Interna, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 19. Os sistemas, as informações e os serviços do DNIT utilizados pelos usuários, no exercício de suas atividades, são de exclusiva propriedade da autarquia, não podendo ser interpretados como de uso pessoal e devem ser protegidos, segundo as diretrizes descritas nesta Política e demais regulamentações em vigor.

Art. 20. Todos os ativos de informação estão sujeitos a monitoração e auditoria. Os registros obtidos poderão ser utilizados para detecção de violações da POSIC e demais regulamentações em vigor.

Art. 21. Os recursos de tecnologia da informação de propriedade do DNIT são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração. É considerada imprópria a utilização desses recursos para propósitos não institucionais ou não autorizados. Os usuários e visitantes que tomarem conhecimento dessa prática, ou qualquer outra prática em desacordo com esta POSIC, devem levá-la ao conhecimento imediato da Coordenação Geral de Tecnologia da Informação - CGTI por meio do e-mail abuse@dnit.gov.br ou outro meio estabelecido, para que sejam aplicadas as ações cabíveis.

Art. 22. A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o reconhecimento do envolvido.

Art. 23. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação. A não designação pressupõe que o gestor é o próprio custodiante.

Art. 24. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIC e de suas normas complementares.

Art. 25. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta POSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no DNIT.

Art. 26. Qualquer tipo de dúvida sobre a POSIC, as Normas Complementares - NCs e demais regulamentações de SIC deve ser imediatamente esclarecida com a área de Gestão de Segurança da Informação.

CAPÍTULO V
DAS DIRETRIZES ESPECÍFICAS

Seção I
Controle de Acesso Físico e Lógico

Art. 27. Diretrizes específicas e procedimentos próprios de controles de acesso lógico e físico deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - Os usuários do DNIT são responsáveis pelos atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital.

II - A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento;

III - Todos os sistemas de informação do DNIT, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações;

IV - As práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança;

V - A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação;

VI - Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do DNIT ou bloqueados em caso de afastamento;

VII - O ingresso de visitantes deve ser controlado de tal forma a impedir o acesso destes às áreas de armazenamento ou processamento de informações sensíveis, salvo acompanhados e com autorização do CGTI.

Parágrafo único. Os atos que comprovadamente não forem praticados pelos titulares de suas credenciais serão alvos de auditoria, objetivando análise do incidente e o devido esclarecimento. O titular da credencial utilizada indevidamente por terceiros não deverá ser responsabilizado, quando comprovar que vinha cumprido regularmente com todas as diretrizes e normativos de segurança, principalmente no período anterior e durante a ocorrência.

Seção II
Correio Eletrônico

Art. 28. Diretrizes específicas e procedimentos próprios ao serviço de correio eletrônico (e-mail) deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

I - O uso do correio eletrônico do DNIT destina-se a fins corporativos e relacionados às atividades do usuário no âmbito da autarquia;

II - O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do DNIT;

III - São usuários do serviço de correio eletrônico corporativo os membros e servidores do DNIT, seus órgãos e unidades, os estagiários e os demais agentes públicos que oficialmente executem atividade vinculada à atuação institucional do DNIT, e que receberem o acesso ao respectivo serviço de correio.

Seção III
Utilização da Internet e Intranet

Art. 29. Diretrizes específicas e procedimentos próprios de controles de uso e acesso à Internet e Intranet deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

I - Todas as regras corporativas sobre uso de Internet e Intranet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação do DNIT deverá sempre ser privilegiada.

II - Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo. Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um servidor do quadro permanente do órgão.

III - Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet e Intranet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, caixa postal de correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

IV - O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo órgão, observando-se sempre a conduta compatível com a moralidade administrativa;

V - Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

VI - Toda alteração de nível de acesso somente será realizada mediante solicitação formal, pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pela CGTI, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade a segurança e a integridade da rede do DNIT;

VII - É vedado contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do DNIT;

VIII - O usuário poderá solicitar liberação de determinada página, com a devida justificativa, mediante requerimento formal à CGTI, nos termos do inciso VI;

IX - Somente serão liberadas as páginas analisadas e autorizadas pela CGTI;

X - A ocorrência de qualquer hipótese de má utilização da internet deverá ser comunicada, de imediato à CGTI, por meio do e-mail abuse@dnit.gov.br ou outro meio estabelecido;

XI - Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet bloqueado pela CGTI, sendo comunicado o fato à chefia imediata, podendo haver repercussão disciplinar com a aplicação das sanções legalmente previstas, assegurados o contraditório e a ampla defesa;

XII - Os navegadores de Internet e Intranet utilizados no âmbito do DNIT deverão ser homologados pela CGTI;

XIII - Os problemas técnicos verificados pelos usuários, ocorridos durante o acesso aos serviços de Internet e Intranet, devem ser imediatamente comunicados a CGTI para que sejam solucionados.

Seção IV
Recursos Computacionais

Art. 30. Os usuários devem ter acesso unicamente àqueles recursos computacionais que forem indispensáveis à realização de suas atividades no DNIT.

Art. 31. Os usuários são responsáveis pelos recursos computacionais por eles utilizados, devendo preservar a sua integridade e continuidade.

Art. 32. É vedado aos usuários do DNIT utilizar a identificação e/ou senha de outro usuário para acessar ou utilizar um recurso computacional.

Art. 33. É vedado aos usuários fazer uso de exploração de falhas de configuração, falhas de segurança ou tentar obter conhecimento de senhas especiais para alterar um Recurso Computacional.

Art. 34. Tendo em vista a preservação do ambiente computacional do DNIT, é vedado aos usuários o fornecimento de informações a terceiros sobre características, funcionalidades e configurações dos recursos de tecnologia da informação disponíveis, ressalvada a possibilidade de disposição de tais informações pela CGTI, quando o desempenho de atividades institucionais assim exigir.

Subseção I
Estações de Trabalho

Art. 35. É vedado ao usuário abrir as estações de trabalho ou modificar a configuração do hardware.

Art. 36. O usuário deve informar imediatamente à CGTI, assim como a área responsável pela gestão do patrimônio, quando identificada violação da integridade do equipamento por ele utilizado.

Art. 37. O usuário não deve cancelar o processo de verificação de vírus quando este for iniciado automaticamente na sua estação de trabalho.

Art. 38. Não é permitida a conexão de estações de trabalho particulares à rede cabeada do DNIT, portáteis ou não, à rede do DNIT, exceto em casos de comprovada necessidade, situações nas quais deverá ser assegurada a devida adoção de padrões de segurança compatíveis com o disposto nessa norma, devendo a estação de trabalho ser objeto de verificação de conformidade pela CGTI.

Art. 39. Arquivos salvos na unidade de disco local não terão garantia de *backup* e recuperação.

Art. 40. As credenciais de administrador do equipamento deverão ficar sob a guarda e responsabilidade da CGTI, restando ao usuário, ao qual se destina o equipamento, utilizá-lo mediante credenciais de "usuário comum". Ressalva-se o caso de usuários da área técnica, devidamente autorizados pela CGTI, que por força de suas funções e conhecimento técnico, se reservam ao direito de efetuar suas próprias instalações, bem como, a guarda e o uso oportuno das credenciais de administrador.

Art. 41. O compartilhamento de diretórios e arquivos em estações de trabalho somente deve ser realizado quando estritamente necessário para execução das atividades do usuário mediante solicitação formal à CGTI, devidamente justificada.

Subseção II
Servidor de Arquivos

Art. 42. Nos servidores de arquivos locais devem ser gravados:

I - Documentos relacionados ao trabalho cotidiano e à produção jurídica e administrativa local, que demande compartilhamento ou resguardo institucional;

II - Pastas particulares de correio eletrônico e das contas corporativas da unidade.

Art. 43. As permissões de acesso deverão ser concedidas em nível de grupos.

Art. 44. É proibida a gravação de material classificado como:

I - Jogos e apostas;

II - Pornografia, pedofilia, sexo, nudez, e de conteúdo adulto similar;

III - Maliciosos e/ou pirataria;

IV - Anonimadores e proxys de navegação;

V - Atividades ilegais, terroristas e violência; e

VI - Transferência ou cópia não autorizadas de material protegido por direito autoral.

Art. 45. Quando identificado pelas ferramentas de segurança, o material classificado nas categorias listadas nos incisos do artigo anterior será automaticamente bloqueado e não poderá ser objeto de pedido de liberação de acesso.

Art. 46. É obrigatório armazenar os arquivos inerentes ao serviço de cada setor em suas respectivas pastas de rede, para garantir o backup desses arquivos.

Art. 47. Não é permitido criar ou remover arquivos e pastas fora da área alocada ao respectivo Setor ou Unidade. Caso esteja em desacordo, o arquivo ou pasta será excluído sem aviso prévio.

Art. 48. É vedada a gravação de dados e informações de natureza particular.

Art. 49. Identificada ocorrência em desacordo com o disposto nos itens antecedentes, a CGTI poderá, após notificar o responsável pelo ato infracional e resguardar as evidências necessárias, excluir ou isolar arquivos, revogar acessos ou requisitar o equipamento, devendo representar acerca do fato imediatamente à autoridade responsável pela apuração da infração, nos termos do art. 116, XII, da Lei nº 8.112, de 11 de dezembro de 1990, que estabelece que um dos deveres do servidor público federal é o de representar contra ilegalidade, omissão ou abuso de poder.

Parágrafo único. A representação de que trata este artigo deve ir acompanhada de todos os elementos probatórios obtidos pela CGTI.

Subseção III
Utilização de Software

Art. 50. No DNIT, só será permitida a utilização de softwares homologados pela CGTI, respeitando os direitos autorais e contratuais dos fabricantes, e que sejam necessários para a execução das atividades dos usuários.

Art. 51. O registro dos softwares homologados, do número de licenças disponíveis e dos softwares instalados nas estações de trabalho deve ser mantido atualizado pela CGTI.

Art. 52. O processo de homologação de software deve avaliar, sobretudo, o impacto da utilização desta na segurança da informação do DNIT e o suporte para o mesmo.

Art. 53. É vedado ao usuário efetuar réplicas dos softwares adquiridos pelo DNIT.

Art. 54. A instalação de software de outras categorias, tais como freeware (software gratuito), de domínio público (não protegido por copyright) e/ou cópias de demonstração que não sofram ação de direitos autorais, deve ser previamente requerida à CGTI.

Art. 55. A CGTI poderá remover programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa norma.

Subseção IV
Manutenção e Configuração

Art. 56. Toda solicitação de atendimento para instalação, suporte e configuração dos recursos computacionais deve ser efetuada mediante abertura de chamado à CGTI.

Art. 57. Nas dependências físicas do DNIT somente é permitida a execução dos serviços de suporte técnico nos equipamentos de propriedade da instituição ou cedidos formalmente, sendo proibida a assistência técnica em equipamentos particulares.

Art. 58. Todo equipamento que tiver a necessidade de ser deslocado para manutenção ou configuração, deverá estar devidamente identificado.

Art. 59. O usuário deve estar ciente da saída do equipamento das dependências físicas do DNIT, caso seja necessária a retirada para manutenção.

Art. 60. A saída do equipamento das dependências físicas do DNIT deverá ser autorizada pela área responsável pela gestão do patrimônio.

Subseção V
Criptografia

Art. 61. O uso de recursos criptográficos interfere na Disponibilidade, Integridade, Confidencialidade, Autenticidade - DICA, sendo, portanto, responsabilidade do Gestor de SIC a implementação dos procedimentos relativos ao seu uso, no âmbito das informações produzidas e custodiadas no DNIT, em conformidade com as orientações contidas em norma específica.

Art. 62. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade pelo seu uso.

Subseção VI
Ativos de Rede

Art. 63. As portas dos switches somente devem estar ativas se utilizadas e inventariadas.

Art. 64. Os switches e access points devem possuir controle de acesso.

Art. 65. Todo roteador utilizado na rede do DNIT deve prover, no mínimo, o uso de ACLs (Access lists) e o filtro de pacotes.

Art. 66. Todo ativo de rede deve estar em local seguro. Os switches departamentais devem estar instalados em racks devidamente fechados e seguros.

Art. 67. Os ativos de rede somente devem ser liberados para uso após a efetiva homologação, realizada em ambiente apropriado, distinto do ambiente de produção, e devidamente documentado.

Art. 68. As intervenções no ambiente de rede somente serão permitidas mediante supervisão pelos técnicos autorizados pela CGTI.

Art. 69. A CGTI reserva o direito de realizar investigações em qualquer dos equipamentos que integrem a sua rede local.

Subseção VII
Rede Wireless

Art. 70. Diretrizes específicas e procedimentos próprios referentes a utilização da Rede Wireless deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - O acesso a Rede Wireless Corporativa somente poderá ocorrer por meio dos recursos providos pelo DNIT, sendo vedado o uso de pontos de acesso particulares ou pertecentes às empresas prestadoras de serviço;

II - O acesso a Rede Wireless Corporativa realizar-se-á por credencial de acesso utilizando usuário e senha para autenticação, geridos pela CGTI;

III - Ao utilizar rede de computadores externa por meio de dispositivos portáteis de propriedade do DNIT, o usuário deve obedecer também às normas e às diretrizes daquelas redes. Em caso de divergência entre as normas das redes externas e a POSIC/DNIT, prevalece o definido nas normas do DNIT.

Seção V
Aquisição, Desenvolvimento e Manutenção de Sistemas

Art. 71. Diretrizes específicas e procedimentos próprios da aquisição, desenvolvimento e manutenção de Sistemas deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - A Estrutura de SIC deve estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção;

II - O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

Seção VI
Gestão de Ativos de Informação

Art. 72. Os ativos de informação devem:

I - Ser inventariados e protegidos;

II - Ter identificados os seus proprietários e custodiantes;

III - Ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - Ter a sua entrada e saída nas dependências do DNIT autorizadas e registradas por autoridade competente;

V - Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI - Ser regulamentados por norma específica quanto a sua utilização; e

VII - Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 73. O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo, conforme disposto em normas e legislação específica de classificação de informação.

Art. 74. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

Art. 75. É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo DNIT.

Seção VII
Gestão de Riscos de Segurança da Informação e Comunicações

Art. 76. Diretrizes e princípios específicos, acerca dos procedimentos, definições preliminares, análise/avaliação dos riscos e formulação de Plano de Tratamento dos Riscos devem ser fixados em norma complementar, em observância ao estabelecido pela Norma Complementar Nº 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, em especial:

I - Convém que o processo de Gestão de Riscos de Segurança da Informação e Comunicações esteja alinhado ao planejamento estratégico e também, com o processo maior de gestão de riscos corporativos, se esse existir;

II - Os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco;

III - A GRSIC é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações, levando em consideração o planejamento, execução, análise crítica e melhoria da SIC no DNIT;

IV – O Gestor de Segurança da Informação e Comunicações, no âmbito de suas atribuições, é responsáveis pela coordenação da Gestão de Riscos de Segurança da Informação e Comunicações no DNIT.

Seção VIII
Tratamento de Incidentes

Art. 77. A CGTI deverá manter Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), instituída pelo Comitê da Segurança da Informação e Comunicações (COSIC), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas à incidentes de segurança em rede de computadores:

I - Deverá ser elaborado documento de constituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, o qual designará suas atribuições e seu escopo de atuação;

II - A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos será composta, preferencialmente, por servidores públicos ocupantes de cargo efetivo, com perfil técnico adequado com as atividades dessa equipe;

III - O Agente responsável pela ETIR deverá ser servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, em atuação no DNIT, formalmente designado para chefiar e gerenciar a ETIR.

Art. 78. Os eventos e incidentes de SIC devem ser tratados de acordo com um Plano de Gerenciamento de Incidentes específico, comunicados e registrados.

Art. 79. No tratamento de incidentes cibernéticos, a ETIR, responsável pelo tratamento e resposta ao incidente, deverá considerar, no mínimo, as seguintes diretrizes:

I - Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas;

II - O tratamento da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;

III - Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, o Gestor de Segurança da Informação ou membros do COSIC tem como dever, sem prejuízo de suas demais atribuições, providenciar o acionamento das autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços do DNIT;

IV - A atuação da Equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo, sem prejuízo das demais metodologias e padrões conhecidos;

V - A ocorrência de incidentes de segurança em redes de computadores do DNIT poderá ser comunicada ao Centro de Tratamento de Incidentes Cibernéticos da Administração Pública Federal (CTIR.Gov), conforme procedimentos a serem definidos pelo próprio centro, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas.

VI - As notificações enviadas pela Equipe ao Centro de Tratamento e Resposta à Incidentes Cibernéticos de Governo, bem como a troca de informações entre as Equipes existentes, devem seguir os formatos e os procedimentos que serão estabelecidos pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo.

Seção IX
Gestão de Continuidade

Art. 80. Objetivando a implantação do processo de Gestão de Continuidade de Negócios, visando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, o DNIT deverá manter um Programa de Gestão da Continuidade de Negócios, conforme a Norma Complementar nº 06/IN01/DSIC/GSI/PR de 11 de novembro de 2009.

Art. 81. A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional do DNIT.

Art. 82. As medidas constantes do Plano de Gerenciamento de Incidentes deverão assegurar a disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto sofrido diante do acontecimento situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

Seção X
Avaliação de Conformidade

Art. 83. A Auditoria Interna do DNIT deverá avaliar, periodicamente, por meio de verificações de conformidade das práticas de SIC, a aderência desta POSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC, no âmbito das responsabilidades de cada unidade administrativa da Autarquia:

Art. 84. A Estrutura de GSIC do DNIT deverá avaliar, periodicamente, por meio de verificação de conformidade das práticas de SIC, a aderência desta POSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC, no âmbito das atividades e dos serviços sob a responsabilidade da CGTI:

I - A execução da verificação de conformidade será realizada pela Estrutura de GSIC, podendo, com a prévia aprovação do COSIC, ser subcontratada no todo ou em parte;

II - É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados;

III - A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pela Estrutura de GSIC e aprovado pelo COSIC;

IV - O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos;

V - A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 85. Os resultados de cada ação de verificação de conformidade descritas nos Art. 82 e Art. 83 serão documentados em relatório de avaliação de conformidade, o qual será encaminhado ao Gestor de SIC e, por ele ao Gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

Art. 86. As não-conformidades relativas ao descumprimento de legislações, normas e procedimentos serão consideradas riscos de SIC e devem ser tratadas.

Seção XI
Plano de Investimento em Segurança da Informação e Comunicação

Art. 87. Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos, que poderá estar contido no plano de investimentos geral da TI.

Art. 88. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 89. O plano de investimentos, assim como a correspondente proposta orçamentária, será aprovado pelo COSIC, mediante recomendação elaborada pela Estrutura de GSIC.

Art. 90. Caso haja limitação na execução orçamentária ou força de trabalho considerada insuficiente para cumprir o plano, caberá ao COSIC realizar a correspondente revisão do plano de investimentos, considerando os riscos a serem tratados.

Seção XII
Propriedade Intelectual

Art. 91. As informações produzidas por usuários no exercício de suas funções, são patrimônio intelectual do DNIT e não cabe a seus criadores qualquer forma de direito autoral.

Art. 92. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do DNIT em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela Autarquia, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Diretor Geral, nos demais casos, observando a legislação em vigor.

Art. 93. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 94. Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos desde que expressamente autorizadas pelo DNIT.

Seção XIII
Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 95. Os contratos, convênios, acordos e instrumentos congêneres que não estejam em conformidade com o exposto nos Art. 23 e Art. 24 desta POSIC, devem fazê-lo no próximo aditivo a ser lavrado.

Art. 96. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

CAPÍTULO VI
DA RESPONSABILIZAÇÃO

Art. 97. Ações que violem a POSIC ou a inobservância de quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SIC serão devidamente apuradas e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor, assegurados a ampla defesa e o contraditório.

Art. 98. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor.

Art. 99. O uso de qualquer recurso em inobservância das normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos administrativo, civil e criminal, em que a instituição cooperará ativamente com as autoridades competentes.

Art. 100. Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o DNIT e/ou terceiros. Portanto, o usuário vinculado a tais dispositivos identificadores será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal), sendo que o uso dos dispositivos e/ou senhas de identificação de outra pessoa viola as regras de segurança e poderá resultar na aplicação de medidas administrativas, cíveis e judiciais cabíveis.

CAPÍTULO VII
DA COMPOSIÇÃO E COMPETÊNCIA

Seção I
Do Gestor de Segurança da Informação

Art. 101. O gestor de segurança da informação será designado dentre os servidores públicos civis ocupantes de cargo efetivo e militares de carreira do órgão ou entidade, com formação ou capacitação técnica compatível às suas atribuições.

Art. 102. Compete ao gestor de segurança da informação:

I - Coordenar o Comitê de Segurança da Informação;

II - Coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do DNIT, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - Assessorar a alta administração na implementação da Política de Segurança da Informação;

IV - Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - Promover a divulgação da política e das normas internas de segurança da informação do DNIT a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

VI - Incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - Propor recursos necessários às ações de segurança da informação;

VIII - Acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX - Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - Manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Seção II
Do Comitê de Segurança da Informação

Art. 103. O Comitê de Segurança da Informação e Comunicações terá, no mínimo, a seguinte composição:

I - o gestor de segurança da informação, que o coordenará;

II - um representante da DIREX;

III - um representante de cada unidade finalística do DNIT; e

IV - o Coordenador-Geral de Tecnologia da Informação.

Art. 104. O Comitê de Segurança da Informação e Comunicações possui as seguintes atribuições:

I - Assessorar a implementação das ações de segurança da informação;

II - Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV - Propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V - Avaliar, revisar e analisar criticamente a POSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais do DNIT e às legislações vigentes;

VI - Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIC do DNIT;

VII - Deliberar sobre normas internas de segurança da informação.

Art. 105. O COSIC poderá estabelecer a periodicidade de suas reuniões, bem como a realização de reuniões extraordinárias, garantindo a frequência mínima anual.

Seção III
Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

Art. 106.A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos tem como atribuições:

I - Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

II - Promover a recuperação de sistemas;

III - Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

IV - Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

V - Analisar ataques e intrusões na rede do DNIT;

VI - Executar as ações necessárias para tratar quebras de segurança;

VII - Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

VIII - Cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

IX - Participar em fóruns, redes nacionais e internacionais relativas à SIC.

Seção IV
Dos Gestores dos Ativos de Informação e dos Custodiantes

Art. 107.Cabe ao Gestor do Ativo de Informação:

I - Garantir a segurança dos ativos de informação sob sua responsabilidade;

II - Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta POSIC;

III - Conceder e revogar acessos aos ativos de informação;

IV - Comunicar à ETIR a ocorrência de incidentes de SIC; e

V - Designar custodiante do ativo de informação, quando aplicável.

Art. 108. Cabe ao custodiante do ativo de informação proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta POSIC.

Seção V
Das competências e responsabilidades dos demais envolvidos

Art. 109. Cabe ao titular de cada unidade administrativa do DNIT:

I - Corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua responsabilidade;

II - Conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

III - Incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

IV - Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

V - Informar à CGGP a movimentação de servidores de sua unidade;

VI - Informar à CGTI a movimentação de funcionários terceirizado de sua unidade;

VII - Realizar o tratamento e a classificação da informação;

VIII - Autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;

IX - Comunicar à ETIR os casos de quebra de segurança; e

X - Manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

Art. 110. Cabe aos terceiros e fornecedores, conforme previsto em contrato:

I - Tomar conhecimento desta POSIC;

II - Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

III - Fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Art. 111. Cabe aos usuários:

I - Conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta POSIC, bem como os demais normativos e resoluções relacionados à SIC;

II - Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e

III - Comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à ETIR.

CAPÍTULO VIII
DA ESTRUTURA NORMATIVA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 112. Os documentos que comporão a estrutura normativa de gestão de segurança da informação serão divididos em três categorias:

I - Política (POSIC) – nível estratégico: constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o DNIT decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados;

II - Normas complementares à POSIC – nível tático: portarias, instruções normativas ou resoluções que especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar o cenário definido estrategicamente nas diretrizes da política;

III - Procedimentos Complementares à POSIC e às suas Normas Complementares – nível operacional: ofícios-circulares, procedimentos operacionais padrão e manuais que instrumentalizam o disposto nas normas e na política, permitindo sua direta aplicação nas atividades do DNIT.

Seção I
Atualização

Art. 113. A SIC, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

Art. 114. Os instrumentos normativos gerados a partir desta POSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal, ou conforme os seguintes critérios:

I - Política de Segurança da Informação e Comunicações (POSIC):
a) Nível de Aprovação: Diretoria Geral;

b) Periodicidade de Revisão: A periodicidade para a revisão da Política de Segurança da Informação não deve exceder 4 (quatro) anos.

II - Normas complementares à POSIC:

a) Nível de Aprovação: Comitê de Segurança da Informação e Comunicações (COSIC);

b) Periodicidade de Revisão: não deve exceder 4 (quatro) anos.

III - Procedimentos complementares à POSIC e às suas Normas Complementares:

a) Nível de Aprovação: Coordenação Geral de Tecnologia da Informação – CGTI;

b) Periodicidade de Revisão: não deve exceder 4 (quatro) anos.

Seção II
Divulgação e acesso à estrutura normativa

Art. 115.Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados a todos os agentes públicos e prestadores de serviços do DNIT e também publicadas na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 116. Fica revogada a Portaria/DG nº 721, de 27 de abril de 2016, publicada no Boletim Administrativo nº 077, de 28 de abril de 2016.

Art. 117. Esta Portaria entra em vigor em 03 de maio de 2021.

ANTÔNIO LEITE DOS SANTOS FILHO
Diretor-Geral

Anexo

1. Dispositivos legais de caráter federal, aplicáveis à Segurança da Informação:

I - Constituição Federal, art. 5º, inciso X. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.

II - Constituição Federal, art. 5º, inciso XII. Sigilo dos dados telemáticos e das comunicações privadas.

III - Constituição Federal, art. 5º, inciso XIV. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.

IV - Constituição Federal, art. 5º, inciso XXXIII e art. 37, § 3º, inciso II. Disponibilidade das informações constantes nos órgãos públicos.

V - Constituição Federal, art. 5º, inciso XXXIV. Disponibilidade das informações constantes nos órgãos públicos.

VI - Constituição Federal, art. 23, incisos III e IV. Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.

VII - Constituição Federal, art. 216, § 2º Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.

VIII - Constituição Federal, art. 37, caput. Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.

IX - Constituição Federal, art. 37, § 6º e Código Civil, art. 43. Responsabilidade objetiva do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.

X - Constituição Federal, art. 37, § 7º Necessidade de regulamentação do acesso a informações privilegiadas.

XI - Consolidação das Leis do Trabalho - CLT, art. 482, alínea "g". Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).

XII - Código de Conduta da Alta Administração, art. 5º, § 4º Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública).

XIII - Código de Conduta da Alta Administração, art.14, inciso II. Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.

XIV - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "h" do inciso XV da Seção II. Proteção da integridade das informações públicas.

XV - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "l" do inciso XV da Seção II. Proteção da disponibilidade das informações públicas.

XVI - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso X da Seção I. Proteção da disponibilidade das informações públicas.

XVII - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso VII da Seção I. Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.

XVIII - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso IX da Seção I. Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.

XIX - Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "e" do inciso XIV da Seção II. Disponibilidade das comunicações.

XX - Código de Propriedade Industrial, art. 75. Sigilo das patentes de interesse da defesa nacional.

XXI - Código de Defesa do Consumidor, arts. 43 e 44. Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.

XXII - Código Penal, art. 151. Proteção do sigilo, integridade e disponibilidade das informações de caráter pessoal veiculadas através dos meios de comunicação.

XXIII - Código Penal, art. 152. Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.

XXIV - Código Penal, art. 153. Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.

XXV - Código Penal, art. 154. Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.

XXVI - Código Penal, art. 184, § 3º Proteção da autenticidade.

XXVII - Código Penal, art. 297. Proteção da integridade e autenticidade dos documentos públicos.

XXVIII - Código Penal, art. 298. Proteção da integridade e autenticidade dos documentos particulares.

XXIX - Código Penal, art. 305. Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.

XXX - Código Penal, art. 307. Proteção da autenticidade.

XXXI - Código Penal, art. 313-A. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.

XXXII - Código Penal, art. 313-B. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.

XXXIII - Código Penal, art. 314. Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.

XXXIV - Código Penal, art. 325. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

XXXV - Código Processo Penal, art. 20. Proteção de informações sigilosas.

XXXVI - Código Processo Penal, art. 207. Proteção do sigilo profissional.

XXXVII - Código Processo Penal, art. 745. Proteção de informações sigilosas relacionadas ao condenado.

XXXVIII - Código Tributário Nacional, art. 198. Proteção do sigilo fiscal.

XXXIX - Código de Processo Civil, art. 388, inciso II, c/c art. 404, inciso IV. Proteção da privacidade de seus clientes.

XL - Código de Processo Civil, art. 448, inciso II c/c art. 457, §3º Proteção da privacidade de seus clientes.

XLI - Instrução Normativa nº 1/2019 - Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e integrantes do Sistema de Administração dos Recursos de Informação (SISP) do Poder Executivo Federal.

XLII - Lei nº 6.538/1978, art. 41. Proteção da privacidade de correspondência.

XLIII - Lei nº 7.170/1983, art. 13. Proteção das informações sigilosas relacionadas à segurança nacional.

XLIV - Lei nº 7.232/1984, art. 2º, inciso VIII. Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.

XLV - Lei nº 7.492/1986, art. 18. Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.

XLVI - Lei nº 8.027/1990, artigo 5º, inciso I. Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.

XLVII - Lei nº 8.027/1990, artigo 5º, parágrafo único, inciso V. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

XLVIII - Lei nº 8.112/1990, art. 116, inciso VIII. Sigilo das informações produzidas ou conhecidas no exercício de cargo ou função pública.

XLIX - Lei nº 8.112/1990, art. 132, inciso IX. Proteção das informações sigilosas acessadas no exercício de cargo ou função pública.

L - Lei nº 8.137/1990, art. 3º, inciso I. Proteção da disponibilidade de informações para manutenção da ordem tributária.

LI - Lei nº 8.429/1992, art.11, incisos III, IV e VII. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público, bem como garantia de publicidade das informações de interesse coletivo ou geral que devem ser divulgadas por ato oficial.

LII - Lei nº 8.429/1992, art. 13. Disponibilidade de informações pessoais do agente público para o Poder Público e veracidade dos dados.

LIII - Lei nº 8.443/1992, art. 86, inciso IV. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

LIV - Lei Complementar nº 75/1993, art. 8º incisos II e VIII, §§ 1º e 2º Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

LV - Lei nº 8.625/1993, art. 26, inciso I, alínea "b" e inciso II. Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

LVI - Lei nº 8.906/1994, art. 7º, inciso XIX. Proteção da privacidade do cliente do advogado.

LVII - Lei nº 9.100/1995, art. 67, incisos VII e VIII. Proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas.

LVIII - Lei nº 9.279/1996, art. 195, inciso XI. Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.

LIX - Lei nº 9.296/1996, art. 10. Sigilo dos dados e das comunicações privadas.

LX - Lei nº 9.472/1997, art. 3º, inciso V. Sigilo das comunicações.

LXI - Lei nº 9.472/1997, art. 3º, inciso VI. Proteção de informações pessoais de caráter sigiloso.

LXII - Lei nº 9.472/1997, art. 3º, inciso IX. Proteção de informações pessoais de caráter sigiloso.

LXIII - Lei nº 9.504/1997, art. 72. Proteção da integridade das informações de caráter eleitoral e dos equipamentos.

LXIV - Lei nº 9.605/1998, art. 62. Disponibilidade e integridade de dados e informações.

LXV - Lei nº 10.683/2003, art. 6º Todos os aspectos da segurança da informação.

LXVI - Lei nº 10.703/2003, arts. 1º, 2º e 3º Disponibilidade de dados cadastrais para fins de investigação criminal e sigilo nas demais hipóteses.

LXVII - Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

LXVIII - Decreto 9.819/2019 art. 2º, inciso II, alínea “j”.

LXIX - Decreto nº 5.483/2005, arts. 3º e 11. Disponibilidade de informações pessoais do agente público para o Poder Público e dever de sigilo por parte da Controladoria-Geral da União.

LXX - Decreto nº 5.687/2006, arts.10 e 13 do Anexo. Disponibilidade das informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos.

LXXI - Decreto nº 6.029/2007, inciso II do art. 1º Disponibilidade das informações constantes nos registros públicos.

LXXII - Decreto nº 6.029/2007, art. 10. Sigilo da identidade do denunciante e sigilo do processo para proteção da honra e da imagem do investigado antes da prolação da decisão pela Comissão de Ética.

LXXIII - Decreto nº 6.029/2007, art. 13. Sigilo do processo administrativo por infração ética antes da prolação da decisão e publicidade após o término e aplicação das penalidades.

LXXIV - Decreto nº 6.029/2007, art. 22. Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética Pública.

Art. 116. Legislação específica de caráter federal relacionada à Segurança da Informação:

I - Lei nº 7.232/1984 Dispõe sobre a Política Nacional de Informática, e dá outras providências.

II - Lei nº 8.248/1991 Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências, observada suas atualizações.

III - Lei nº 9.296/1996 Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.

IV - Lei nº 9.472/1997 Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.

V - Lei nº 9.507/1997 Regula o direito de acesso a informações e disciplina o rito processual do habeas data.

VI - Lei nº 9.609/1998 Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.

VII - Lei nº 9.883/1999 Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.

VIII - Lei nº 8.159/1991 Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.

IX - Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

X - Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

XI - Lei nº 10.973, de 02 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.

XII - Lei nº 12.527, de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

XIII - Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil; e dá outras providências.

XIV - Decreto nº 2.295, de 04 de agosto de 1997. Regulamenta o disposto no art. 24, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Neste caso o processo deverá ser sigiloso, excetuando-se a publicidade das compras governamentais.

XV - Decreto nº 2.556, de 20 de abril de 1998. Regulamenta o registro previsto no art. 3º da Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.

XVI - Decreto nº 3.294, de 15 de dezembro de 1999. Institui o Programa Sociedade da Informação, com objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira.

XVII - Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

XVIII - Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.

XIX - Decreto nº 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

XX - Decreto nº 4.073, de 03 de janeiro de 2002. Regulamenta a Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados, observadas as suas atualizações.

XXI - Decreto nº 4.376, de 13 de setembro de 2002. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.

XXII - Decreto nº 4.522, de 17 de dezembro de 2002. Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.

XXIII - Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento, observadas as suas atualizações.

XXIV - Decreto nº 8,985, de 2017. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Instituto Nacional de Tecnologia da Informação - ITI, remaneja cargos em comissão e substitui cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS por Funções Comissionadas do Poder Executivo - FCPE.

XXV - Decreto nº 4.829, de 03 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.

XXVI - Decreto nº 5.450, de 31 de maio de 2005. Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.

XXVII - Decreto nº 9.283, de 2018. Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, a Lei nº 13.243, de 11 de janeiro de 2016, o art. 24, § 3º, e o art. 32, § 7º, da Lei nº 8.666, de 21 de junho de 1993, o art. 1º da Lei nº 8.010, de 29 de março de 1990, e o art. 2º, caput, inciso I, alínea "g", da Lei nº 8.032, de 12 de abril de 1990, e altera o Decreto nº 6.759, de 5 de fevereiro de 2009, para estabelecer medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação tecnológica, ao alcance da autonomia tecnológica e ao desenvolvimento do sistema produtivo nacional e regional.

XXVIII - Decreto nº 9.668, de 2019. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República e altera o quantitativo de Gratificações de Exercício de Cargo em Confiança devida a Militares - RMP.

XXIX - Decreto nº 6.605, de 14 de outubro de 2008. Dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.

XXX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética.114

XXXI - Instrução Normativa GSI Nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, observadas as suas atualizações e normas complementares.

XXXII - Resolução nº 338 do STF, de 11 de abril de 2007. Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do STF, alterada pela Resolução nº 579, de 25 de maio de 2016.

XXXIII - Portaria nº 93, de 26 de setembro de 2019. Aprova o Glossário de Segurança da Informação.

2. Normas técnicas relacionadas à segurança da informação:

I - ISO/IEC TR 13335-3:1998. Esta norma fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1 e TR ISO/IEC 13335-2. As orientações são projetadas para auxiliar o incremento da segurança na TI.

II - ISO/IEC GUIDE 51:1999. Esta norma fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos. É aplicável a qualquer aspecto de segurança relacionado a pessoas, propriedades, ao ambiente, ou a uma combinação de um ou mais destes (por exemplo, somente pessoas; pessoas e propriedades; pessoas, propriedades e o ambiente).

III - ISO/IEC GUIDE 73:2002. Esta norma fornece definições genéricas de termos de gestão de riscos para a elaboração de normas. Seu propósito é ser um documento genérico de alto nível voltado para a preparação ou revisão de normas que incluam aspectos de gestão de riscos.

IV - ABNT NBR ISO IEC 17799: 2005. Esta norma é equivalente à ISO/IEC 17799:2005. Consiste em um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.

V - ABNT NBR ISO/IEC 27001:2013. Esta norma é usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Aplicável a qualquer organização, independentemente do seu ramo de atuação, define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.

VI - ABNT NBR ISO/IEC 27002:2013. Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.