SERVIÇOS PRESTADOS

17. A ETIR prestará os seguintes serviços:

a) condução do tratamento de Incidentes de Segurança em ambientes cibernéticos;

b) promoção do tratamento de artefatos maliciosos;

c) promoção do tratamento de vulnerabilidades;

d) emissão de alertas e advertências relacionados a incidentes de segurança da informação;

e) prospecção ou monitoração de novas tecnologias;

f) avaliação de segurança do ambiente de tecnologia da informação; e

g) disseminação de informações relacionadas à segurança da informação.

INSTRUÇÃO NORMATIVA Nº 23/DNIT SEDE, DE 12 DE MAIO DE 2021

Disciplina a utilização dos recursos de Tecnologia da Informação, bem como estabelecer regras gerais para controles de acesso relativo à Segurança da Informação e Comunicações no âmbito do Departamento de Nacional de Infraestrutura e Transportes - DNIT, abrangendo suas Superintendências e unidades locais.

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 17/11/2020, publicada no DOU de 19/11/2020, a aprovação do Relato nº 100/2021/DAF/DNIT SEDE, o qual foi incluído na Ata da 18ª Reunião Ordinária da Diretoria Colegiada, realizada em 11/05/2021, e tendo em vista o constante no **Processo nº 50600.000763/2021-01**, resolve:

Art. 1º **DISCIPLINAR** a utilização dos recursos de Tecnologia da Informação, bem como estabelecer regras gerais para controles de acesso relativo à Segurança da Informação e Comunicações no âmbito do Departamento de Nacional de Infraestrutura e Transportes - DNIT, abrangendo suas Superintendências e unidades locais.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 2º As disposições desta Instrução Normativa são válidas para todos os usuários de recursos de tecnologia da informação do Departamento Nacional de Infraestrutura de Transportes, a saber: servidores ocupantes de cargo efetivo ou cargo em comissão e os ocupantes de emprego público, em exercício na autarquia, bem como funcionários de empresas prestadoras de serviços terceirizados e ainda os estagiários em atividade no órgão.

Art. 3º As disposições desta Instrução Normativa são válidas também para outras pessoas que se encontrem a serviço do DNIT, como consultores externos e demais agentes públicos ou particulares que, por força de convênios, contratos, acordos de cooperação e instrumentos congêneres, executem atividades vinculadas ao DNIT, como responsáveis pela proteção e preservação do ativo de informação, e que estejam autorizadas a utilizar os recursos de tecnologia da informação mediante solicitação de dirigente de unidade da autarquia à Diretoria de Administração e Finanças - DAF, por meio da sua Divisão de Segurança da Informação - DSINF da Coordenação-Geral de Tecnologia da Informação - CGTI.

Art. 4º As regras gerais para controle de acesso relativo à Segurança da Informação e Comunicações, cujo objetivo é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações, estão em consonância com o disposto na Política de Segurança da Informação e Comunicações - PoSIC do DNIT .

Art. 5º Os contratos de prestação de serviço celebrados com o DNIT devem conter cláusula específica exigindo da empresa contratada o cumprimento da presente Instrução Normativa pelos prepostos por ela alocados, bem como prevendo as penalidades decorrentes da sua inobservância.

Parágrafo único. Os contratos de prestação de serviço já celebrados pelo DNIT, e em vigor na data de publicação desta Instrução Normativa, deverão, oportunamente, em seus aditivos/renovações, proceder a inclusão da cláusula obrigatória no caput do artigo.

Art. 6º 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 constituem ativos de informação do DNIT.

Art. 7º O ativo de informação é um bem de valor e deverá ser protegido, guardado, cuidado e gerenciado adequadamente com o objetivo de garantir a sua Disponibilidade, Integridade, Confidencialidade e Autenticidade - DICA, independente do meio de suporte, armazenamento, processamento ou transmissão que for utilizado.

CAPÍTULO II
DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 8º Os recursos de tecnologia da informação são:

I - os microcomputadores de mesa e portáteis e seus dispositivos periféricos, como teclado, mouse, caixa de som, microfone, leitoras, gravadoras e demais acessórios conectados ao computador;

II - os scanners, impressoras laser, impressoras jato de tinta, webcams e demais equipamentos relacionados à tecnologia da informação;

III - os programas de computador adquiridos e os sistemas desenvolvidos na autarquia;

IV - os equipamentos e serviços da Rede DNIT, que compreende as redes locais do Órgão Central e das Unidades Regionais, bem como a rede de comunicação que as interliga (**storages**, **switches** e servidores);

V - os suprimentos e bens de consumo relacionados à tecnologia da informação; e

VI - os dados armazenados em equipamentos, dispositivos e periféricos.

Art. 9º Os recursos de tecnologia da informação pertencentes às unidades do DNIT e que estão disponíveis para o usuário devem ser usados em atividades estritamente relacionadas às funções institucionais desempenhadas pela autarquia.

Art. 10. O usuário responsável pelo uso e guarda do recurso de tecnologia da informação deve zelar pelo seu estado, integridade e funcionamento, comunicando qualquer defeito ou anormalidade à CGTI.

§ 1º Para formalização da responsabilidade, o usuário de recurso de tecnologia da informação deve assinar Termo de Responsabilidade, na forma do Anexo I desta Instrução Normativa.

§ 2º Caberá ao dirigente a indicação dos responsáveis pelos equipamentos de uso compartilhado que estejam disponíveis na sua unidade.

Art. 11. Tendo em vista a preservação do ambiente informacional 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.

Art. 12. É vedada a utilização dos recursos informacionais disponíveis com o objetivo de praticar ações indevidas contra outros recursos da rede de computadores do DNIT ou redes externas, dentre os quais: equipamentos servidores, estações de mesa, estações portáteis, equipamentos de rede, serviços de segurança e sistemas de informação.

CAPÍTULO III
DAS ESTAÇÕES DE TRABALHO

Art. 13. São estações de trabalho os microcomputadores de mesa, bem como os portáteis do DNIT.

Art. 14. A estação de trabalho deve manter o padrão estabelecido pela CGTI, no tocante ao sistema operacional e aos demais programas de computador instalados.

Art. 15. É vedada a alteração, pelo usuário, da configuração do ambiente operacional da estação de trabalho, procedimento que só pode ser realizado por técnico qualificado da CGTI, ou por empresa prestadora de serviço por ela autorizada, diretamente na referida estação de trabalho ou automaticamente por meio da rede.

Art. 16. É vedada a instalação, pelo usuário, de programas de computador nas estações de trabalho, à exceção dos softwares disponibilizados, em caráter específico, na central de software.

§ 1º 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, pelo Portal de Atendimento da referida Coordenação.

§ 2º A CGTI poderá remover, sem notificação prévia, qualquer programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa norma.

§ 3º Os programas de computador adquiridos pelo DNIT e os sistemas desenvolvidos no órgão somente podem ser instalados nas estações de trabalho por técnico qualificado da CGTI, ou por pessoa por ela autorizada, diretamente nas estações de trabalho ou automaticamente por meio da rede, devendo aqueles constarem, obrigatoriamente, de relação de programas de computador homologados pela referida Coordenação.

§ 4º É vedada, ao usuário, a cópia de programas de computador, licenças de software e sistemas implantados nas estações de trabalho, quer seja para uso externo ao DNIT, quer seja para uso em outra estação de trabalho do órgão.

§ 5º A simples presença do programa de computador na relação mencionada no parágrafo primeiro deste artigo não constitui autorização prévia para a sua instalação em qualquer estação de trabalho, devendo-se considerar o número de licenças disponíveis, bem como autorização da CGTI, observado o procedimento no parágrafo anterior.

§ 6º É vedada a utilização de ferramentas nas estações de trabalho que não possuam o devido licenciamento (softwares piratas), ou que possam comprometer a segurança dos recursos de rede, tais como coletores de tráfego (sniffers), mapeadores de portas (port scans) e softwares de acesso remoto (TeamViewer, AnyDesk, AeroAdmin, TightVNC e Supremo), dentre outros.

§ 7º Aplica-se a vedação do parágrafo anterior a qualquer equipamento conectado à rede do DNIT.

Art. 17. É vedada a instalação e utilização de quaisquer periféricos, componentes ou placas de hardware na rede e equipamentos do DNIT que não tenham sido adquiridos pelo órgão.

Art. 18. Somente em casos especiais será concedido privilégio de administrador da máquina para os usuários das estações de trabalho, por meio de prévia solicitação, mediante formalização de processo no Sistema Eletrônico de Informações - SEI, o qual será analisado pela CGTI.

Parágrafo único. É vedado aos usuários com privilégio de administrador da máquina o compartilhamento de recursos ou ativação de serviços de rede nas estações de trabalho.

Art. 19. É vedada a utilização de microcomputadores particulares, portáteis ou não, na rede do DNIT, exceto em casos de comprovada necessidade, e mediante anuência da CGTI. Nestes casos, a referida Coordenação velará para que sejam, obrigatoriamente, adotados os padrões de segurança compatíveis com o disposto nesta Instrução Normativa.

Parágrafo único. Em se tratando de equipamentos de empresas contratadas e/ou colaboradoras do DNIT, caberá solicitação junto à CGTI para análise do atendimento.

Art. 20. É vedada a conexão de equipamentos de rede sem fio (Wireless) na rede do DNIT, exceto aqueles homologados pela CGTI.

Parágrafo único. As diretrizes específicas e procedimentos próprios referentes a utilização da Rede Wireless estão fixados em norma complementar.

Art. 21. Compete à CGTI o processamento de software antivírus nas estações de trabalho, definindo, inclusive, sua periodicidade, podendo, antecipadamente, realizar varredura nos equipamentos em que julgar necessária a realização do referido procedimento.

Art. 22. É de responsabilidade do usuário a realização de cópias de segurança dos dados armazenados no disco rígido de sua estação de trabalho.

CAPÍTULO IV
DO ACESSO FÍSICO

Art. 23. Quaisquer movimentações de equipamentos de informática no âmbito do DNIT devem ser comunicadas à CGTI para atualização dos respectivos controles.

Art. 24. Previamente ao envio de equipamentos para manutenção ou alienação, a CGTI deverá ser comunicada a fim de que realize procedimento para remoção de informações relevantes.

Art. 25. É de responsabilidade do usuário a guarda e adequada utilização de dispositivos de armazenamento externos (disquetes, pendrives, CDs, DVDs, etc.).

Art. 26. Em viagens, as estações portáteis devem ser transportadas como bagagem pessoal.

Art. 27. Usuários que lidam com informações confidenciais devem utilizar, em suas estações de trabalho, sistema de criptografia homologado pela CGTI para armazenar ou enviar seus documentos.

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

Art. 28. A retirada de equipamentos de informática da autarquia seguirá a normatização vigente, devendo ser previamente autorizada pela DAF, e mantendo-se registro informatizado de saída e posterior devolução, quando for o caso.

§ 1º A movimentação interna de equipamento também deve ser objeto de controle.

§ 2º No caso das estações portáteis utilizados por servidor do DNIT, deverá ser utilizado o termo de responsabilidade como documento de autorização.

§ 3º No caso de equipamentos retirados para manutenção, por empresa contratada pelo DNIT, para tal finalidade, deverá ser utilizado documento de autorização fornecido pela CGTI, mediante formalização de SEI.

Art. 29. O ambiente físico em que se encontram os equipamentos servidores e equipamentos de rede é de acesso exclusivo ao pessoal da CGTI, ou a quem for por ela autorizado.

Seção I
Do acesso às Instalações Físicas

Art. 30. O acesso às dependências do DNIT deverá ser feito, preferencialmente, por portarias que contemplem catracas, vigilantes armados, sistemas de inspeção de bagagens de mão e recepção e será realizado por:

I - servidores e colaboradores, por meio de identificação pessoal na catraca; e
II - visitantes, após o devido registro na recepção.

§ 1º É obrigatória a identificação pessoal dos servidores e colaboradores por meio de crachás, contendo:

I - foto;
II - matrícula; e
III - cargo/Função.

§ 2º O visitante, após identificado, receberá um crachá provisório.

§ 3º Na identificação, o visitante deverá informar:

I - seu nome;
II - o número de um documento de identificação; e
III - a área que pretende visitar e a pessoa que irá recebê-lo, a qual deverá ser previamente contatada para autorização de acesso.

§ 4º Deverá ser registrado o horário de ingresso do visitante.

§ 5º O servidor ou colaborador que, por qualquer motivo, não tiver o crachá, no ato de entrada, deverá ser identificado na portaria, como qualquer outro visitante e receberá um crachá provisório.

§ 6º O crachá deverá ser usado a todo momento por todas as pessoas nas dependências do DNIT.

Art. 31. O acesso às dependências por portadores de bagagem é condicionado, preferencialmente, à inspeção por meio de sistema de raios X, na portaria, restando proibida a entrada de:

I - armas de fogo;
II - armas brancas;
III - substâncias tóxicas, radioativas, explosivas ou inflamáveis;
IV - bebidas alcoólicas;
V - drogas ilícitas.

§ 1º Os itens elencados no caput deste artigo, excepcionalmente, podem ingressar nas dependências quando expressamente autorizados, via correspondência oficial expedida e assinada pelo responsável pela segurança.

§ 2º O parágrafo anterior não se aplica aos agentes públicos que possuem porte de arma de fogo em razão de suas funções, previstas em lei.

Art. 32. O acesso ao Centro de Processamento de Dados (CPD) será feito, estritamente, por:

I - servidor e colaborador, desde que cadastrado em bancos de dados, autorizado pela Equipe de Segurança da Informação, com o apoio da Coordenação de Infraestrutura de Tecnologia da Informação e Comunicações - COINF, por meio dos crachás;
II - por prestador de serviço ou visitante, desde que identificado e autorizado, acompanhado por servidor ou colaborador da COINF.

Art. 33. Os corredores e pátios próximos às portarias deverão ser monitorados por sistema de CFTV.

Parágrafo único. Outros locais considerados como de riscos também poderão ser monitorados. O acesso ao CPD do DNIT é tratado de forma específica no anexo II desta norma.

Seção II
Da Classificação de Ativos e Perímetro de Segurança

Art. 34. Os ativos de Informação devem ser classificados quanto à sua criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, de acordo com o anexo II.

Art. 35. Os ativos de Nível 1 de criticidade devem ser armazenados, preferencialmente, em tipos de salas seguras, com mecanismos de proteção contra desastres naturais, vandalismo, sabotagens e outras catástrofes.

Art. 36. Os ativos de Nível 1 e 2 de criticidade devem ser alocados em ambientes restritos aos colaboradores que operam os ativos.

Art. 37. Não será permitida a entrada de dispositivos eletrônicos, incluindo mídias removíveis, computadores, celulares e smartphones, e equipamentos fotográficos de qualquer natureza nos ambientes seguros descritos no Art. 33, a menos que autorizado por um colaborador operador do ativo protegido em questão.

Parágrafo único. É de responsabilidade do colaborador que acompanha os visitantes solicitar-lhes que guardem seus dispositivos eletrônicos fora do ambiente seguro.

Art. 38. As informações serão classificadas de acordo com o disposto na Lei 12.527 - Lei de Acesso à Informação, de 18 de novembro de 2011, Capítulo IV.

CAPÍTULO V
DAS UNIDADES DE ARMAZENAMENTO DE REDE

Art. 39. São de responsabilidade da CGTI as unidades de armazenamento de rede para os usuários do DNIT e a execução de cópia de segurança delas.

Art. 40. O usuário deve manter, preferencialmente, os arquivos de trabalho nas unidades de armazenamento de rede que possuem cópia de segurança.

§ 1º O usuário deve manter nas unidades de armazenamento de rede apenas arquivos que estejam estritamente relacionados às atividades desempenhadas pela autarquia, sendo vedada a gravação de arquivos de música, fotos, vídeos, e outros que não atendam tal finalidade.

§ 2º A restrição citada no parágrafo anterior deste artigo é válida para qualquer unidade de rede, portanto, extensiva à pasta pessoal do usuário.

§ 3º Fica autorizada a CGTI, quando verificado armazenamento indevido na forma do caput do artigo, a proceder, sem necessidade prévia de comunicação ao usuário, a eliminação dos arquivos indevidos.

Art. 41. A CGTI pode prover, adicionalmente às unidades descritas no Art. 39, unidades de armazenamento de rede públicas, com direito de acesso a todos os usuários de uma rede local, para compartilhamento temporário de arquivos entre diferentes unidades ou áreas.

§ 1º A CGTI efetuará limpeza periódica nas unidades de rede descritas no **caput,** conforme critérios a serem divulgados aos usuários.

§ 2º Não serão realizadas cópias de segurança das unidades de armazenamento de rede descritas no caput.

Art. 42. A capacidade das unidades de armazenamento de rede será limitada, segundo definições estabelecidas pela CGTI, que considerará a disponibilidade de espaço no equipamento servidor e as atividades inerentes às unidades ou áreas.

CAPÍTULO VI
DAS IDENTIFICAÇÕES DE USUÁRIOS E SENHAS DE ACESSO

Art. 43. A identificação, a autorização, a autenticação, o interesse do serviço, a utilização de credenciais pessoais de acesso e a necessidade de conhecer são condicionantes prévias para concessão de acesso aos ativos de informação no DNIT.

Art. 44. Para utilização das estações de trabalho do DNIT será necessária a autenticação do usuário, mediante identificação (login) e senha de acesso.

Art. 45. A identificação do usuário e a senha inicial de acesso são fornecidas pela CGTI por solicitação do dirigente responsável pela unidade ou área de lotação do usuário, mediante fornecimento da cópia do CPF do credenciando.

§ 1º A senha de acesso é de uso pessoal e intransferível, e sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio usuário no primeiro acesso.

§ 2º Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário ao qual as informações estão vinculadas.

§ 3º A utilização da identificação e da senha de acesso concedidas a estagiário e a funcionário de empresa prestadora de serviços terceirizados é de responsabilidade do dirigente da respectiva unidade ou área em que ele estiver alocado.

§ 4º Ao ser credenciado para uso dos recursos de tecnologia da informação, é atribuído ao usuário um perfil, que corresponde a seus direitos e privilégios para acesso a serviços e informações, que não podem, em hipótese alguma, ser transferidos a terceiros.

§ 5º Poderão ser disponibilizadas permissões de acesso distintas daquelas definidas nos critérios citados no parágrafo anterior, desde que devidamente autorizadas pelo dirigente da unidade ou área a que a referida unidade de armazenamento de rede se referir.

§ 6º Os dirigentes de cada unidade ou área devem comunicar por escrito à CGTI o afastamento definitivo de usuários lotados em seus setores, solicitando o seu descredenciamento do acesso aos recursos de tecnologia da informação de suas respectivas unidades ou áreas.

§ 7º 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.

§ 8º A área de recursos humanos do DNIT deve comunicar à CGTI os desligamentos, as aposentadorias, os afastamentos e as movimentações de usuários que impliquem em mudanças de lotação.

§ 9º O acesso aos sistemas de informação pode exigir a concessão de identificação de usuário e senha específica, que somente são fornecidas mediante critérios, específicos e objetivos, estabelecidos pelos gestores dos sistemas.

§ 10. Usuários em trânsito pela Sede ou por quaisquer entidades vinculadas ao DNIT nos Estados poderão utilizar os recursos de tecnologia da informação das unidades em que estiverem trabalhando.

§ 11. Os direitos de acesso dos usuários devem ser revisados pela CGTI, por amostragem, em intervalos regulares de 6 (seis) meses, ou quando aquela Coordenação julgar conveniente para manter a segurança do ambiente do DNIT.

Art. 46. Será solicitada ao usuário uma troca de sua senha, que deve ser realizada, no máximo, a cada 90 (noventa) dias.

§ 1º O usuário terá seu acesso temporariamente bloqueado caso não execute uma modificação da senha mencionada no caput.

§ 2º A CGTI poderá alterar o prazo para modificação da senha estabelecida no caput.

§ 3º A CGTI deve determinar um padrão a ser seguido quanto à definição da senha, incluindo tamanho mínimo de caracteres, utilização de caracteres alfanuméricos e símbolos, à proibição de repetição de senhas anteriores e à quantidade permitida de, além de outras medidas que visem ao aumento da privacidade da senha.

Art. 47. Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada à CGTI.

Art. 48. No caso de ausência do local de trabalho, mesmo que temporariamente, o usuário deve bloquear o acesso à sua estação de trabalho, devendo informar novamente sua senha para efetuar o desbloqueio.

Art. 49. Os equipamentos servidores, switches, firewalls e roteadores deverão ser protegidos por senha, que será de conhecimento exclusivo da CGTI, e de quem por ela autorizada.

Art. 50. A conta que permanecerá sem registro de acesso, por período superior a 06 (seis) meses, será desativada pela CGTI.

Parágrafo único. A reativação será efetivada com observância do contido no Art. 45.

CAPÍTULO VII
DO ACESSO A REDES EXTERNAS E A INTERNET PELOS USUÁRIOS DO DNIT

Art. 51. O acesso a redes externas ao DNIT ou à Internet dá-se, exclusivamente, por intermédio dos meios autorizados e configurados pela COINF/CGTI, sendo vedado o uso de qualquer forma de conexão alternativa como: ADSL, Proxy externo, conexão discada via fax, ou conexão de dados via telefonia celular, dentre outras.

Art. 52. O acesso à Internet provido pela rede do DNIT deve restringir-se às páginas com conteúdo estritamente relacionado com as atividades desempenhadas pelo Órgão.

Art. 53. A navegação na internet estará sujeita a monitoramento por parte da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR do DNIT e será passível de investigação, caso se faça necessário.

Art. 54. Constitui utilização indevida do serviço de acesso à Internet qualquer das seguintes ações:

I - Acesso a páginas com conteúdo que envolva:

a) pornografia, pedofilia, sexo, nudez e de conteúdo similar adulto;

b) racismo ou preconceitos de qualquer natureza;

c) bate-papo (chats), exceto aquele definido como ferramenta de trabalho homologada pela CGTI;

d) rádio e TV em tempo real, exceto os canais identificados como corporativos e de interesse ao serviço;

e) jogos e apostas;

f) sites de streaming e IPTV

g) sites maliciosos e pirataria;

h) anonimizadores e proxys de navegação;

i) atividades ilegais, terroristas e violência;

j) transferência ou cópia não autorizada de material protegido por direito autoral;

k) outros conteúdos notadamente fora do contexto do trabalho desenvolvido; e

l) conexões de p2p (peer-to-peer*).*

II - Obter na Internet arquivos (download) de imagens, áudio, vídeo, jogos, programas que não estejam relacionados com suas atividades; e

III - Utilizar mecanismos com o objetivo de descaracterizar o acesso indevido a páginas ou serviços vedados neste artigo.

§ 1º As categorias classificadas no inciso I serão automaticamente bloqueadas e não poderão ser objeto de pedido de liberação de acesso, exceto casos pontuais para treinamentos e/ou conferências, a serem solicitados via portal de atendimento;

§ 2º O Comitê de Segurança da Informação e Comunicações - COSIC pode definir outras categorias de sítios de internet e critérios adicionais para bloqueio automático.

§ 3º Não constitui utilização indevida o acesso a sítios que possam ser úteis ao desenvolvimento das atividades administrativas ou funcionais do usuário, tais como: bancos, jornais e revistas, pesquisa e busca, instituições de ensino, etc.

§ 4º O acesso permanente aos sítios e serviços que estejam enquadrados nos casos do parágrafo anterior, será liberado mediante solicitação, via processo SEI, por solicitação do dirigente da unidade ou área, com a devida justificativa.

Art. 55. A transferência de arquivos será monitorada e controlada conforme critérios estabelecidos pelo COSIC.

§1º A transferência de arquivos poderá ser autorizada mediante solicitação justificada.

§2º Os arquivos a serem transferidos serão analisados por software antivírus homologado pelo DNIT.

Art. 56. Poderá ser autorizado o uso de áreas de armazenamento virtuais, como discos e caixas hospedadas na internet, desde que em conformidade com a legislação brasileira vigente, através de pedido de liberação de acesso na ferramenta do portal de atendimento.

Art. 57. Havendo necessidade de restrição, bloqueio ou liberação de acesso a determinados conteúdos, o gestor dos ativos de informação da unidade administrativa deverá formalizar a sua intenção ao DNIT, por meio de pedido devidamente justificado.

Art. 58. Deverão ser adquiridos e mantidos, na rede corporativa do DNIT, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

CAPÍTULO VIII
DO ACESSO À REDE INTERNA DO DNIT

Art. 59. O acesso à rede interna do DNIT, se dará mediante concessão de credenciais de uso pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento, desde que autorizado pela chefia imediata, e solicitado via portal de atendimento da CGTI.

Art. 60. As credenciais de acesso obedecerão os critérios definidos pelo COSIC, no tocante à estrutura dos nomes de usuário e senhas de acesso.

Art. 61. O número de tentativas de logon (acesso) deve ser limitado, e todas as tentativas deverão ser registradas contendo no mínimo data e hora.

Art. 62. O primeiro acesso à rede interna do DNIT estará condicionado à ciência, por parte do usuário, das disposições estabelecidas na PoSIC, bem como das disposições desta norma, atestando sua ciência e concordância.

Art. 63. A autorização, o acesso e o uso das informações e dos recursos computacionais da rede interna estarão sujeitos a monitoramento e deverão ser controlados e limitados ao necessário, considerando as atribuições de cada usuário.

Art. 64. Sempre que houver mudança nas atribuições de determinado usuário da rede interna, os seus privilégios de acesso às informações e aos recursos computacionais deverão ser readequados imediatamente, devendo ser cancelados em caso de desligamento do DNIT ou bloqueados em caso de afastamento.

Parágrafo único. Será responsável pelo fornecimento de informações à COINF/CGTI:

I - o chefe imediato que solicitou o credenciamento, sobre as mudanças de registro e desligamentos de seus respectivos usuários; e

II - a Coordenação-Geral de Gestão de Pessoas, nos casos de desligamento de servidores e estagiários do DNIT.

Art. 65. Os usuários do DNIT serão responsáveis pelos atos praticados na rede interna com suas identificações, tais como: nome de usuário/senha, correio eletrônico e certificado digital.

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.

Art. 66. A rede interna do DNIT ou de suas unidades administrativas poderá ser acessada via serviço de comunicação remota segura homologado e fornecido pelas respectivas áreas de TI, mediante justificação e autorização concedida pela área de segurança da informação do DNIT, através de pedido formalizado via processo SEI.

Parágrafo único. O acesso remoto a serviços autorizados na intranet do DNIT ou de suas unidades administrativas por parte de empresas prestadoras de serviço será concedido mediante solicitação formal justificada da subunidade gestora do contrato e condicionado ao mesmo procedimento do caput deste artigo.

Art. 67. No caso de prestadores de serviço externos que realizarem atividades eventuais ou continuadas no DNIT, o login na rede e o acesso ao domínio do DNIT ou de suas unidades administrativas poderão ser solicitados pelo gestor da respectiva unidade administrativa à área de infraestrutura com avaliação da área de segurança da informação.

Art. 68. O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade pública será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.

CAPÍTULO IX
DAS VEDAÇÕES

Art. 69. Os recursos computacionais do DNIT não poderão ser utilizados para:

I - constranger, assediar ou ameaçar qualquer pessoa;

II - tentar causar, ou permitir que terceiro cause, alteração ou destruição de dados, equipamentos de processamento ou de comunicações ou ambientes operacionais;

III - obter benefícios financeiros diretos, próprios ou de terceiros;

IV - introduzir códigos maliciosos nos sistemas de informática;

V - divulgar ou comercializar produtos, itens ou serviços;

VI - sobrecarregar, desativar ou tentar de alguma forma interferir, sem autorização, em um sistema, programa ou serviço, inclusive cooperando com ataques de negação de serviços internos e externos;

VII - obter acesso não autorizado a dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de informática, exceto no caso das equipes de TI internas criadas para este fim;

VIII - violar medida de segurança ou de autenticação;

IX - fornecer informações a terceiros sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto com permissão de autoridade competente; e

X - armazenar ou utilizar jogos de computador e entretenimento.

CAPÍTULO X
DA ADMINISTRAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 70. Os administradores dos sistemas computacionais do DNIT são responsáveis pelo uso adequado dos recursos sob sua responsabilidade, devendo zelar pela integridade e confidencialidade dos sistemas e dos dados sob seus cuidados.

Parágrafo único. Entende-se por administradores de sistemas computacionais quaisquer pessoas do quadro funcional ou não, lotadas na CGTI, ou por ela autorizadas, que tenham conhecimento autorizado do código de acesso e senha de administração dos recursos de tecnologia da informação, sejam eles de uso geral, ou de uso restrito a uma unidade, grupo de pessoas, ou de uso individual.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 71. É atribuição da CGTI prover os instrumentos tecnológicos necessários ao cumprimento das normas estabelecidas nesta Instrução Normativa, bem como zelar pela manutenção, devidamente atualizada, de sistemas operacionais, navegadores e quaisquer programas de detecção e eliminação de códigos e/ou programas indevidos nas estações de trabalho dos usuários.

Art. 72. É atribuição da CGTI gerir a infraestrutura de hardware e software necessária à prestação dos serviços de acesso à rede interna, a redes externas e à Internet, sendo vedada a instalação de qualquer equipamento neste ambiente, salvo prévia autorização e homologação daquela Coordenação.

Art. 73. A CGTI, em conjunto com a Coordenação-Geral de Gestão de Pessoas, promoverá, periodicamente, cursos, palestras e/ou informativos sobre assuntos relacionados ao uso de recursos de informática, com vistas a manter os usuários dos recursos de tecnologia da informação informados e atualizados.

Art. 74. A CGTI poderá realizar monitoramento da utilização dos serviços de rede e acesso à Internet, podendo, ainda, exercer fiscalização nos casos de apuração de uso indevido desses recursos.

Parágrafo único. A CGTI poderá bloquear temporariamente, sem aviso prévio, acesso a rede, estação de trabalho, e-mail, SEI ou qualquer outro recurso tecnológico ou sistema, caso o usuário esteja realizando atividades que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do DNIT.

Art. 75. O usuário que fizer uso de forma indevida ou não-autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos desta Instrução Normativa, fica sujeito à aplicação das penalidades previstas no art. 117, incisos XVI e XVIII da Lei nº 8.112, de 11 de dezembro de 1990.

Art. 76. Os casos omissos e as dúvidas suscitadas na aplicação desta Instrução Normativa serão dirimidos pela DAF e, quando couber, pelo COSIC.

Art. 77. O descumprimento ou violação desta Instrução Normativa pode resultar na aplicação de sanções administrativas, penais e cíveis.

Art. 78. REVOGAR as Portarias/DG nº 1.347, de 21/08/2007, publicada no Boletim Administrativo nº 034, de 20 a 24/08/2007, e nº 1.954/DIREX, de 12/12/2014, publicada no Boletim Administrativo nº 050, de 08 a 12/12/2014.

Art. 79. Esta Instrução Normativa entra em vigor no dia 1º de junho de 2021.

ANTÔNIO LEITE DOS SANTOS FILHO
Diretor-Geral

ANEXOS

ANEXO I
Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL
Departamento Nacional de Infraestrutura de Transportes

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ deste Departamento Nacional de Infraestrutura de Transportes - DNIT, DECLARO, sob pena das sanções cabíveis nos termos da legislação e normatização vigente, que assumo a responsabilidade por:

I) tratar o(s) ativo(s) de informação como patrimônio do DNIT (equipamentos físicos, sistemas, **software**, dados e informações, etc.);

II) utilizar as informações sob minha custódia, exclusivamente no interesse do serviço do DNIT;

III) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI Nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV) utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do DNIT; e

V) responder, perante o DNIT, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Local, UF, _____de _____de _____.

_____
Assinatura
Nome do usuário e seu setor

_____
Assinatura
Nome da autoridade responsável pela autorização do acesso

ANEXO II
Tabela de Classificação de Ativos de Informação

Grau de criticidade	Ativos de informação	Impacto
Nível 1 – Alto	Data-center, servidores, central telefônica, recursos criptológicos, cópias de segurança, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de primeiro escalão.	Interrompe a missão do órgão ou provoca grave dano à imagem institucional, à segurança do estado ou sociedade.
Nível 2 – Médio	Computadores com dados e informações únicas, de grande relevância, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de segundo escalão.	Degrada o serviço do órgão ou provoca dano à imagem institucional, à segurança do estado ou sociedade.
Nível 3 – Baixo	Os demais ativos de informação	Compromete planos ou provoca danos aos ativos de informação.

ANEXO III
Procedimentos de Controle de Acesso ao CPD (Central de Processamento de Dados) do DNIT

1 - Aplicação

Referem-se aos procedimentos relacionados ao controle de Acesso em áreas críticas da sede do DNIT e o procedimento de cadastro, descadastro e alteração de permissão de acesso às áreas críticas do DNIT. O sistema de controle de acesso será implantado inicialmente nas seguintes áreas:

- CGTI - 1º subsolo

- Controle de acesso por meio de leitura de crachá

- CPD - Dentro da área da CGTI 1º subsolo

- Controle de acesso por meio de leitura de crachá

- Sala de equipamentos de Telecomunicações - Mezanino

- Controle de acesso por meio de leitura de crachá

No caso específico da CGTI no 1º subsolo, considerando a importância estratégica da operação do CPD/Datacenter, o acesso de pessoas estranhas ao setor somente será permitido mediante acompanhamento por pessoal autorizado pela COINF/CGTI. Assim, não haverá instalação de interfone nem autorização para que o vigilante abra a porta de acesso. Caso uma pessoa não autorizada requeira acesso ao local, o vigilante da área deverá contatar a COINF/CGTI por ramal, para providenciar o acompanhamento durante todo o tempo de permanência do visitante no local.

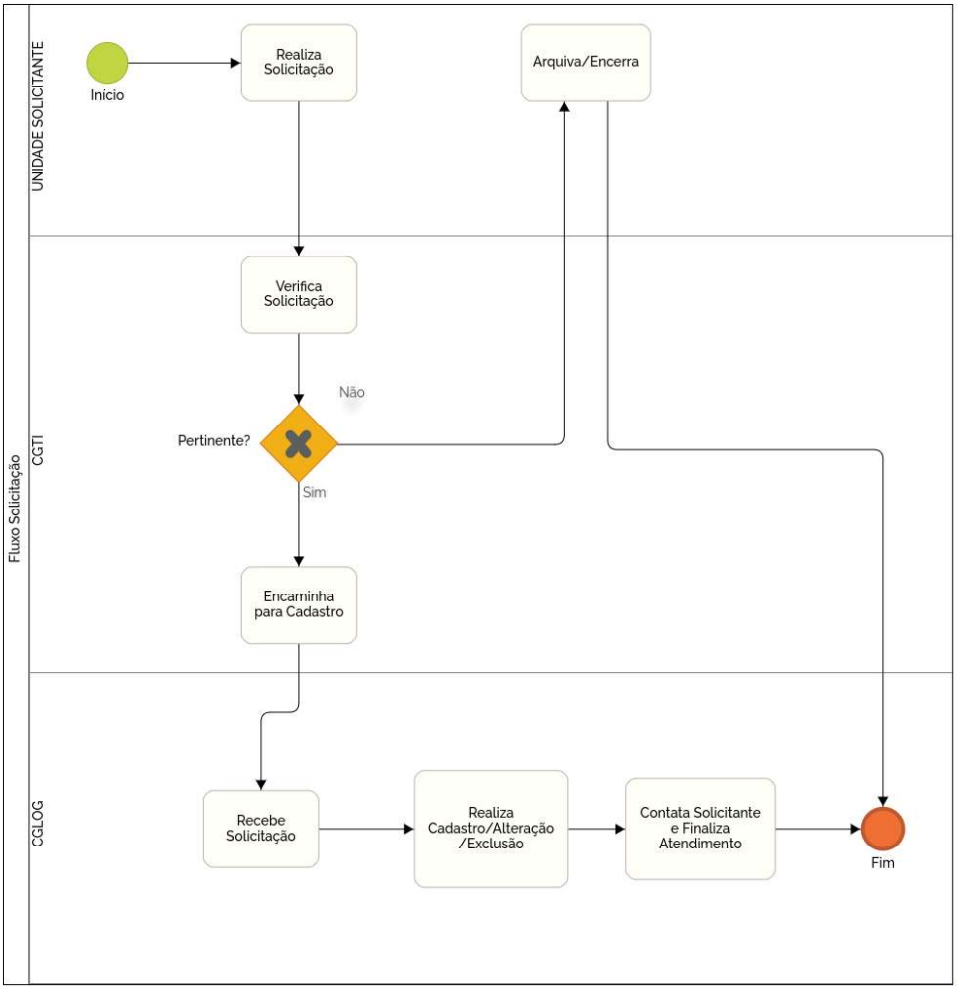
2 - Modalidades

Os controles do acesso dos funcionários aos setores críticos são executados com 2 procedimentos principais:

- Ativação, desativação e alteração de permissões;
- Verificação Periódica dos servidores/colaboradores cadastrados;

2.1 - Ativação, desativação e alteração de permissões

2.1.1 - Fluxograma



2.1.2 - Processamento da solicitação

2.1.2.1 - O processo é iniciado, via SEI, pela unidade solicitante que necessite acesso às áreas críticas, informando:

- Nome do Servidor/Colaborador
- Empresa (caso não seja servidor do DNIT)
- CPF
- Áreas que ele deve ter acesso

2.1.2.2 - O processo é remetido à CGTI, que:

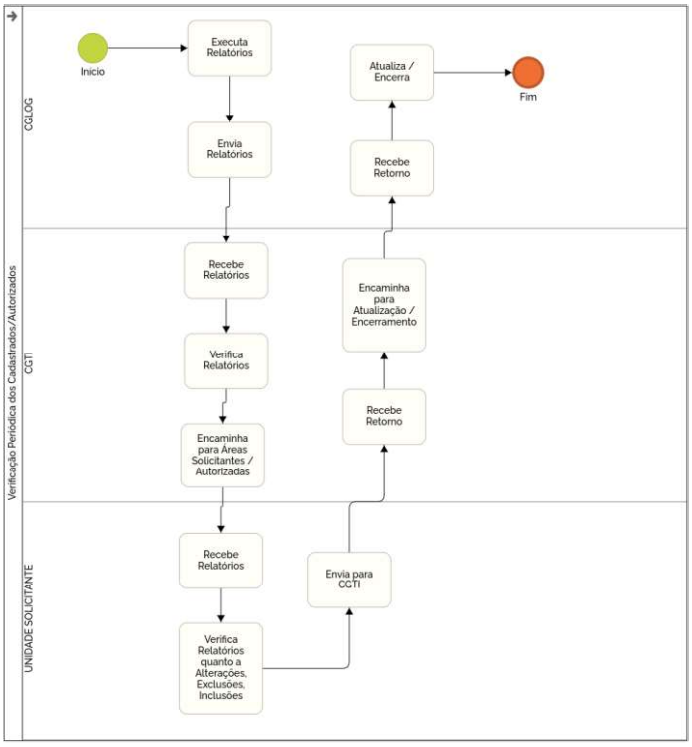
- recebe o processo de solicitação;
- verifica a pertinência técnica da solicitação;
- encaminha o documento de solicitação com a autorização.

2.1.2.3 - O Processo é remetido à CGLOG, que:

- recebe o documento de solicitação;
- solicita a presença do servidor/colaborador para que seja feito o cadastro/alteração, a confecção e a conferência do crachá;
- efetiva o cadastramento;
- contacta o servidor/colaborador quanto ao atendimento do cadastramento e entrega do crachá.
- encerra o atendimento.

2.2 - Verificação Periódica dos funcionários cadastrados

2.2.1 - Fluxograma



2.2.2 - Procedimento de verificação

2.2.2.1 - A CGLOG:

- executa relatório periódico listando os dispositivos de controle de acesso, listando os servidores/colaboradores que têm acesso e as atividades registradas nos dispositivos, contendo histórico com data e hora de acesso de cada servidor/colaborador listado;
- executa relatório listando histórico de acessos nos dispositivos de controle de acesso;
- envia relatório, via SEI, para avaliação da CGTI.

2.2.2.2 - O processo é remetido à CGTI:

- recebe o processo com os relatórios;
- verifica os relatórios;
- encaminha para as áreas correspondentes/ unidades solicitantes;

2.2.2.3 - A Unidade Solicitante:

- recebe o processo;
- remete ao responsável por cada setor para verificação pertinente a cada servidor/colaborador listado;
- verifica a relação de seus servidores/colaboradores que têm acesso a áreas críticas, podendo solicitar alterações/exclusões devidas;
- assinala/ cientifica o relatório recebido e devolve à CGTI.

2.2.2.4 - A CGTI:

- recebe a relação com as alterações;
- analisa e encaminha à CGLOG.

2.2.2.6 - A CGLOG:

- recebe o relatório com as observações feitas pelas unidades;
- confere as informações e processa as devidas alterações;
- encerra a verificação.

3 - Critérios de Aplicação

O responsável pela área solicitante será integralmente responsável por quaisquer ocorrências cometidas pelos funcionários indicados, que tenham como consequência:

- Quebra de sigilo de informações críticas;
- Procedimentos que coloquem em risco a integridade física de equipamentos do DNIT;
- Mal uso do privilégio de acesso para atividades não relacionadas ao setor;

Não serão aceitas solicitações de permissão de acesso a funcionários:

- Funcionários afastados com licença;
- Funcionários que não desempenham mais atividades internas.

INSTRUÇÃO NORMATIVA Nº 24/DNIT SEDE, DE 12 DE MAIO DE 2021

Altera a Instrução Normativa nº 13, de 23 de abril de 2021, do Departamento Nacional de Infraestrutura de Transportes, a qual dispõe sobre o planejamento, a coordenação, o desenvolvimento e o controle de sistemas de Tecnologia da Informação.

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 17/11/2020, publicada no DOU, de 19/11/2020, a aprovação do Relato nº 101/2021/DAF/DNIT SEDE, o qual foi incluído na Ata da 18ª Reunião Ordinária da Diretoria Colegiada, realizada em 11/05/2021, e tendo em vista o constante no **Processo nº 50600.002307/2021-97**, resolve:

Art. 1º A Instrução Normativa nº 13, de 23 de abril de 2021, do Departamento Nacional de Infraestrutura de Transportes, passa a vigorar com as seguintes alterações:

"Art. 4º O desenvolvimento de qualquer sistema/software no âmbito do DNIT será realizado após solicitação por escrito da área requisitante e a aprovação da Coordenação de Sistemas - COSIS, que indicará quais tecnologias devem ser empregadas, no que diz respeito à linguagem de programação, banco de dados, servidor de aplicação e afins, ou avaliará as que forem sugeridas, ficando a seu critério a sua aceitação.

Parágrafo único. O desenvolvimento de sistema/software poderá ser realizado no âmbito de qualquer outra setorial, desde que a Unidade interessada assuma a inteira responsabilidade pelo projeto, e observe:

I - o ambiente de infraestrutura do DNIT;

II - os padrões e tecnologias de linguagem e programação adotados pelo DNIT;