MINISTÉRIO DOS TRANSPORTES
DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES

PORTARIA Nº 1.954 , DE 12 DE DEZEMBRO DE 2014.

O DIRETOR-EXECUTIVO SUBSTITUTO DO DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES - DNIT, no uso das atribuições regimentais que lhe foram delegadas pela Portaria/DG nº 1.708, de 21/10/2014, publicada no D.O.U., de 22/10/2014, e nos Incisos III, IV e V do Art. 124, do Regimento Interno da Autarquia, aprovado pela Resolução nº 10 de 31 de Janeiro de 2007, publicado no D.O.U de 26/02/2007, resolve;

CAPÍTULO I - OBJETIVO

Art. 1º ESTABELECER regras gerais para controles de acesso relativos à Segurança da Informação e Comunicações no âmbito do Departamento de Nacional de Infraestrutura e transportes- DNIT, abrangendo suas Superintendências e unidades locais.

CAPÍTULO II - DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Ficam estabelecidas as regras gerais para controle de acesso relativos à Segurança da Informação e Comunicações, em consonância com o disposto na Política de Segurança da Informação e Comunicações - POSIC do DNIT, conforme disciplinado por esta Norma Operacional – NO.

Art. 3º O objetivo do controle é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações.

Art. 4º Aplicar-se-á esta norma aos servidores, estagiários, colaboradores, consultores externos e demais agentes públicos ou particulares que, por força de convênios, protocolos, acordos de cooperação e instrumentos congêneres, executem atividades vinculadas ao DNIT, como responsáveis pela proteção e preservação do ativo de informação.

Art. 5º Os dados, informações e conhecimentos produzidos, enviados, recebidos, transportados, armazenados ou manipulados por meio dos recursos computacionais, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso constituem ativos de informação do DNIT.

Art. 6º 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. 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 III - DIRETRIZES PARA CONTROLE DE ACESSO LÓGICO

Seção I

Do Acesso à Internet pelos Usuários Internos do DNIT

Art. 8º O acesso à internet será um recurso disponibilizado pelo DNIT e seu uso é exclusivo ao desempenho das atividades profissionais de seus servidores, colaboradores e usuários autorizados.

Art. 9º O acesso somente poderá ocorrer por meio dos recursos providos pelo DNIT, sendo vedado o uso de pontos de acesso ou modems particulares de rede celular conectados às estações de trabalho.

Parágrafo único. Os dispositivos de conexão citados no caput deste artigo poderão ser utilizados pelos custodiantes de dispositivos móveis corporativos, desde que:

I - o DNIT não forneça equipamento similar para conexão à internet; e

II - o usuário registre o equipamento junto à equipe de infraestrutura de TI.

Art. 10. A navegação na internet estará sujeita a monitoramento por parte da Equipes de Tratamento e Resposta a Incidentes em Rede Computacionais do DNIT e será passível de investigação, caso se faça necessário.

Art. 11. Serão vedados o acesso e a navegação aos sítios de internet classificados nas categorias de:

I - jogos e apostas;

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

III - sites maliciosos e pirataria;

IV - anonimizadores e proxys de navegação;

V - atividades ilegais, terroristas e violência; e

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

§ 1º As categorias listadas no caput serão automaticamente bloqueadas e não poderão ser objeto de pedido de liberação de acesso.

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

Art. 12. O acesso a sítios e serviços de internet das demais categorias não listadas no art. 11 terá sua liberação ou bloqueio efetuado pelas Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, mediante:

I - análise de viabilidade técnica, no tocante à capacidade operacional da rede de computadores e dos critérios de segurança da informação e comunicações; e

II - justificativa, considerando a avaliação da necessidade funcional do DNIT de suas Superintendências e Unidades Locais.

Art. 13. 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. 14. 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.

Art. 15. 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 a do DNIT, por meio de pedido justificado.

Art. 16. Deverá ser adquirido e mantido, na rede corporativa do DNIT, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

Seção II

Do Acesso a Rede Interna do DNIT

Art. 17. 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.

Art. 18. As credenciais de acesso obedecerão os critérios definidos pelo COSIC, no tocante à estrutura dos nomes de usuário e senhas de acesso.

Art. 19. O processo de identificação e autenticação na rede interna do DNIT é denominado logon, este processo deverá fornecer o mínimo de informações possíveis.

Parágrafo único. O número de tentativas de logon deverá ser limitada, todas as tentativas deverão ser registradas contendo no mínimo data e hora.

Art. 20. 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. 21. A solicitação de acesso deverá ser encaminhada à área responsável pela TI da respectiva unidade administrativa.

Art. 22. A autorização, o acesso e o uso das informações e dos recursos computacionais da intranet estarão sujeitos a monitoramento e deverão ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário dependerá de prévia autorização do gestor da área responsável pela informação.

Art. 23. 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.

Parágrafo único. Será responsável pelo fornecimento de informações à Coordenação Geral de Modernização de Informática - CGMI:

I - o chefe imediato que solicitou o credenciamento, sobre as mudanças de atribuição e de 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. 24. Os usuários do DNIT serão responsáveis por todos os atos praticados na intranet com suas identificações, tais como, nome de usuário e senha, correio eletrônico e certificado digital.

Art. 25. 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.

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

CAPÍTULO IV - DIRETRIZES PARA CONTROLE DE ACESSO FÍSICO

Sessão I

Acesso às Instalações Físicas

Art. 28. O acesso às dependências do DNIT deverá ser feito somente por portarias que contemplem catracas, vigilantes armados, sistemas de inspeção de bagagens de mão e recepção e será realizado por;

I - Colaboradores, por meio de identificação pessoal na catraca; e

II- Visitantes, após o devido registro na recepção.

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

I - Foto do colaborador;

II - Matrícula do Colaborador; e

III - Cargo/Função do Colaborador.

§ 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.

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

§ 5º O 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. 29. O acesso às dependências por portadores de bagagem é condicionado à inspeção por meio de sistema de raios X, na portaria.

§ 1º Fica proibida a entrada de;

I- Armas de fogo;

II- Armas brancas;

III- Substâncias tóxicas, radioativas, explosivas ou inflamáveis;

IV- Bebidas Alcoólicas;

V- Drogas ilícitas;

§ 2º Os artigos elencados no § 1º, excepcionalmente, podem ingressar nas dependências quando expressamente autorizados, via memorando expedito e assinado, pelo responsável pela segurança.

Art. 30. O Centro de Processamento de Dados é isolado por paredes, porta automatizada e portaria específica.

Art. 31. O acesso ao Centro de Processamento de Dados será feito:

I - Por colaborador cadastrado em bancos de dados, mantidos pela Equipe de Segurança da Informação, por meio dos crachás.

II - Por colaborador não cadastrado ou visitante, desde que identificado na portaria do Centro de Processamento de Dados e autorizado por um colaborador cadastrado.

Art. 32. O acesso à sala dos servidores será feito:

I - Por colaborador da COINF, cadastrado em bancos de dados, mantidos pela Equipe de Segurança da Informação, por meio dos crachás.

II - Por colaborador não cadastrado ou visitante, desde que por um colaborador da COINF cadastrado.

Art. 33. Os corredores, os 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 (Centro de Processamento de Dados) do DNIT é tratado de forma específica no anexo B desta norma.

Sessão II

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 A.

Art. 35. Os ativos de Nível 1 de criticidade devem ser armazenados em salas seguras, com mecanismos 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 nos ambientes seguros descritos no Art. 33, a menos que autorizado por um colaborador operador do ativo protegido e 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.

CAPITULO VI

DAS VEDAÇÕES

Art. 39. 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 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.

CAPITULO VII

Disposições Finais

Art. 40. Os casos omissos e as dúvidas suscitadas serão resolvidos pelo COSIC.

Art. 41. O descumprimento ou violação desta Norma Operacional poderá resultar na aplicação de sanções administrativas, penais e cíveis.

Art. 42. Esta norma entra em vigor na data de sua publicação.

ADAILTON CARDOSO DIAS
Diretor-Executivo Substituto

Publicado no
Boletim Administrativo nº 050
de 08 a 12 / 12 / 14

Carlos Augusto da Mota Gomes
Matr. DNIT nº 0185-6

ANEXOS

Anexo A - 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 B – Procedimentos de Controle de Aceso 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 as áreas críticas do DNIT. O sistema de controle de acesso será implantado inicialmente nas seguintes áreas:

- CGMI – 1º subsolo
  - Controle de acesso por meio de leitura de crachá
- CPD – dentro da área da CGMI 1º subsolo
  - Controle de acesso por meio de leitura de crachá e biometria
- TELECOM - Mezanino
  - Controle de acesso por meio de leitura de crachá
- OPERAÇÃO TELECOM – dentro da área da TELECOM no Mezanino
  - Controle de acesso por meio de leitura de crachá e biometria
- CMS –1º subsolo

- Controle de acesso por meio de leitura de crachá e biometria

No caso específico da CGMI no 1º subsolo, considerando a importância estratégica da operação do CPD, o acesso de pessoas estranhas ao setor somente será autorizado mediante acompanhamento de pessoal autorizado. 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 por ramal a pessoa desejada que deverá se dirigir à porta de acesso e acompanhar o visitante.

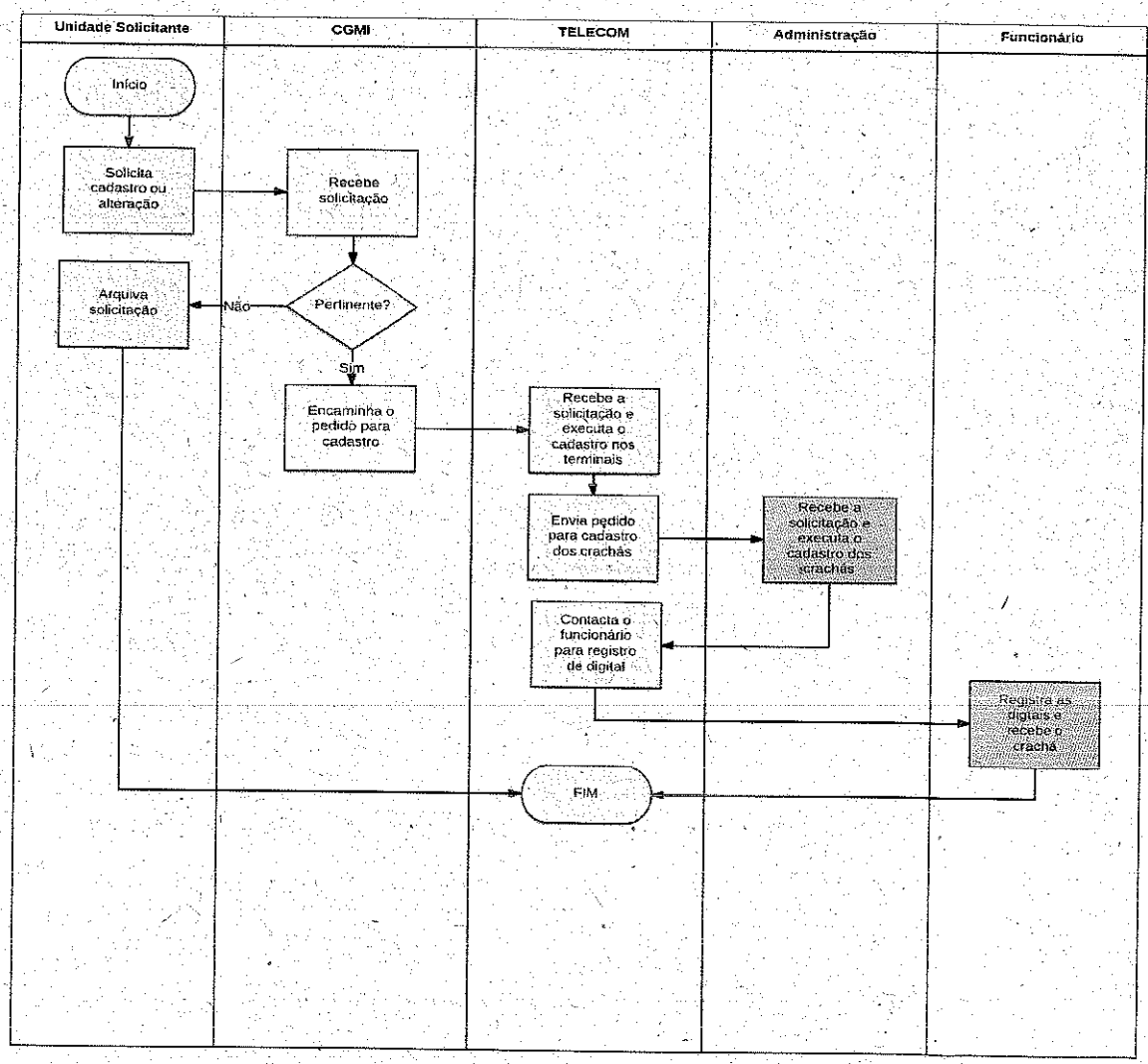
2 - Modalidades

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

- Ativação, desativação e alteração de permissões;
- Verificação Periódica dos funcionários cadastrados;

2.1 - Ativação, desativação e alteração de permissões

2.1.1 –



Fluxograma

2.1.2 - Documentos de apoio:

- Memorando de solicitação da Unidade Solicitante;

2.1.3 - Prazo de solicitação: 3 dias úteis;

2.1.4 – Processamento

2.1.4.1 - O processo é iniciado no momento em que a unidade solicitante necessita de acesso as áreas críticas aos seus funcionários, emitindo um memorando à CGMI contendo:

- Nome do Funcionário
- Empresa (caso não for servidor do DNIT)
- CPF
- Áreas que ele deve ter acesso

2.1.4.2 – A CGMI:

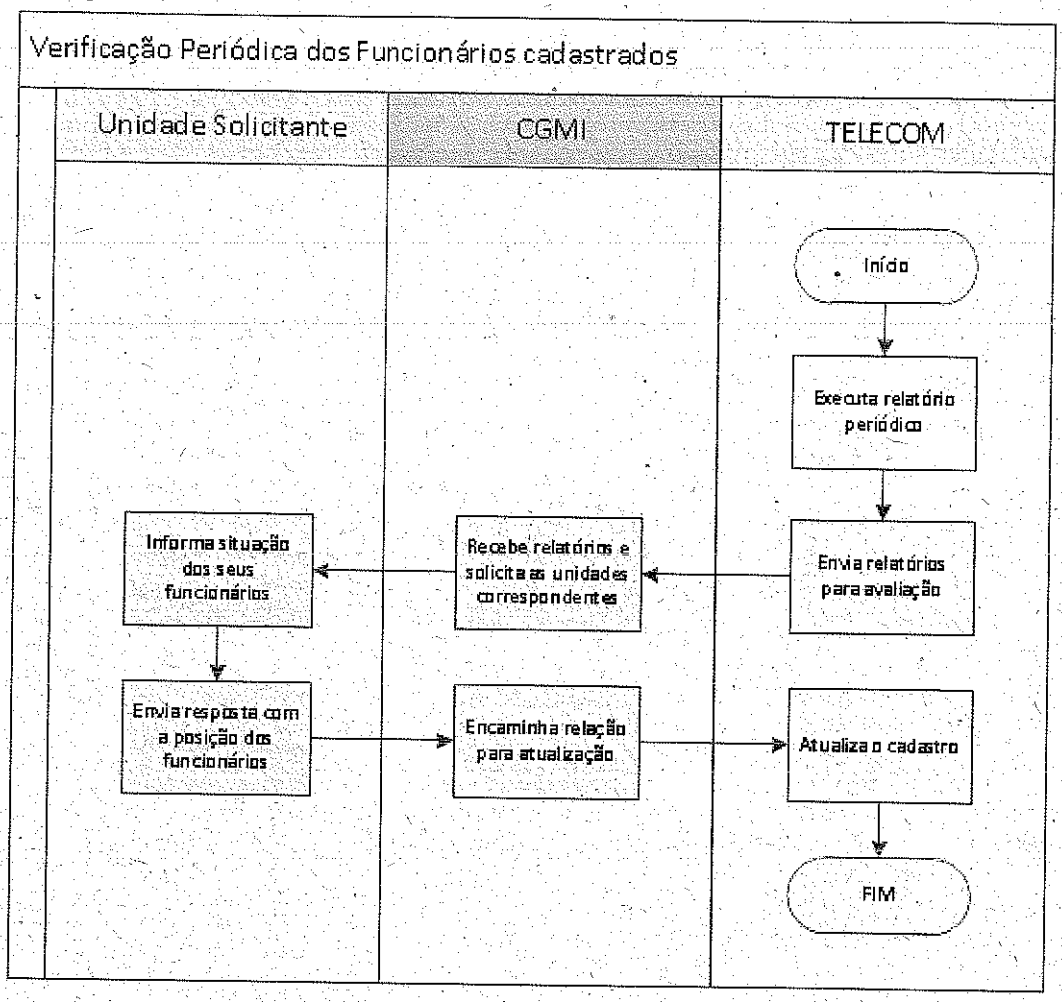
a) Recebe o Memorando de solicitação;
b) Verifica a pertinência técnica da solicitação;
c) Encaminha o Memorando de solicitação com a autorização da empresa ao Serviço de Telecomunicações;

2.1.4.3 – O Serviço de Telecomunicações:

a) Recebe o Memorando de solicitação;
b) Solicita a presença do funcionário para que seja feito o cadastro das impressões digitais, conferência do crachá e o cadastro da senha de acesso;
c) Efetiva o cadastramento.

2.2 – Verificação Periódica dos funcionários cadastrados

2.2.1 - Fluxograma



2.2.2 - Processamento

2.2.2.1 - O processo é iniciado periodicamente a cada 3 meses pelo Serviço de Telecomunicação, apresentando as seguintes atividades:

a) Executa o procedimento de verificação dos dispositivos de controle de acesso, listando os funcionários que tem acesso e a data/hora do último acesso.

b) Encaminha a CGMI o relatório atualizado com os funcionários, setores e suas permissões as áreas críticas,

2.2.2.2 – A CGMI analisa o processo e encaminha aos setores correspondentes;

2.2.2.3 - O responsável por cada setor faz a verificação correspondente a cada funcionário e devolve a CGMI. Portanto a Unidade Solicitante realiza as seguintes atividades:

a) Verifica a relação de seus funcionários que tem acesso a áreas criticas

b) Assinala no relatório recebido e devolve a CGMI com as seguintes identificações:

- Indicação de funcionário que não trabalha mais neste setor;
- Funcionários que não necessitam mais de ter acesso a determinadas áreas críticas;
- Funcionários que devem continuar a ter acesso às áreas críticas;

2.2.2.4 – A CGMI:

a) Recebe a relação com as alterações, analisa e encaminha ao Serviço de Telecomunicações.

2.2.2.5 - O Serviço de Telecomunicações:

a) Recebe o relatório com as observações feitas pelas unidades;

b) Confere as informações e processa as devidas alterações;

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.