MINISTÉRIO DA INFRAESTRUTURA

DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES

INSTRUÇÃO NORMATIVA Nº 22/DNIT SEDE, DE 12 DE MAIO DE 2021

Dispõe sobre a Estrutura de Gestão da Segurança da Informação no âmbito do Departamento Nacional de Infraestrutura de Transportes - DNIT.

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES-DNIT, no uso das atribuições que lhe conferem o art. 173 do Regimento Interno, aprovado pela Resolução nº 39, de 17/11/2020, publicada no DOU de 19/11/2020, em observância ao Decreto nº 9.637, de 26/12/2018 e ao Decreto nº 10.222, de 05/02/2020, bem como as normas NBR ISO/IEC 27.002; Instrução Normativa do Gabinete de Segurança Institucional - GSI Nº 1, de 27/05/2020, alterada pela Instrução Normativa GSI Nº 2, de 24/07/2020, c/c Norma Complementar 05/IN01/DSIC/GSIPR e a Portaria GSI/PR nº 93, de de 26/09/2019 e, consoante a aprovação do Relato nº. 99/2021/DAF/DNIT SEDE, o qual foi incluído na Ata da 18ª Reunião Ordinária da Diretoria Colegiada, realizada em 11/05/2021 e o constante no Processo nº 50600.003041/2021-08, resolve:

Art. 1º DISPOR sobre o Gestor de Segurança da Informação, o Comitê de Segurança da Informação e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Departamento Nacional de Infraestrutura de Transportes, bem como sobre as atribuições dessas estruturas.

CAPÍTULO I
DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

Art. 2º 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. 3º 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 - coordenar a instituição, implementação e manutenção da infraestrutura necessária à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

IX - acompanhar os trabalhos da ETIR;

X - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

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

XII - 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.

CAPÍTULO II
DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art. 4º O Comitê de Segurança da Informação - CoSIC do Departamento Nacional de Infraestrutura de Transportes está vinculado à Diretoria-Geral e será coordenado pelo Gestor de Segurança da Informação do DNIT, o qual, em seus afastamentos ou impedimentos legais, será representado pelo Diretor de Administração e Finanças.

Art. 5º O Comitê de Segurança da Informação deve conter, 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. 6º O Comitê de Segurança da Informação 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 - PoSIC 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.

Parágrafo único. O COSIC deverá realizar ao menos uma reunião semestral, podendo convocar reuniões extraordinárias para dar celeridade às deliberações que se fizerem necessárias.

CAPÍTULO III

DA EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS

Art. 7º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR do Departamento Nacional de Infraestrutura de Transportes está vinculada à Coordenação-Geral de Tecnologia da Informação e deve ser coordenada por um Agente responsável formalmente designado, o qual, em seus afastamentos ou impedimentos legais, será substituído pelo Chefe da Divisão de Segurança da Informação.

Art. 8º 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.

Art. 9º 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 Segurança da Informação e Comunicações - 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 Segurança da Informação e Comunicações - SIC.

Art. 10. O Anexo I desta Instrução Normativa regulamenta a Constituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR do Departamento Nacional de Infraestrutura de Transportes - DNIT.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 11. REVOGAR as Portarias/DG nº 982, de 18/10/2013, publicada no Boletim Administrativo nº 042, de 14 a 18/10/2013 e nº 1.952, de 12/12/2014, publicada no Boletim Administrativo nº 050, de 08 a 12/12/2014.

Art. 12. Esta Instrução Normativa entra em vigor em 1º de junho de 2021.

ANTÔNIO LEITE DOS SANTOS FILHO
Diretor-Geral

ANEXO I

DOCUMENTO DE CONSTITUIÇÃO DA ETIR

1. A ETIR do DNIT tem como missão prioritária facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, receber e notificar qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

2. A ETIR atuará, desejavelmente, também de forma proativa com o objetivo de minimizar o risco de que as vulnerabilidades sejam exploradas por ameaças e venham a comprometer o negócio da Instituição a fim de contribuir para a adequada prestação dos serviços do Departamento.

PÚBLICO ALVO DA ETIR

3. São considerados como **comunidade, ou público alvo**, o conjunto de pessoas, setores, órgãos ou entidades atendidas pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR do Departamento Nacional de Infraestrutura de Transporte ou das redes de terceiros as quais estão sendo usa das pela organização.

MODELO DE IMPLEMENTAÇÃO

4. O modelo de implementação no qual a ETIR se baseia é o “Modelo 1 - Utilizando a equipe de Tecnologia da Informação”, descrito na subseção 7.1 da Norma Complementar 5 da Instrução Normativa 1 do Gabinete de Segurança Institucional da Presidência da República.

5. No Modelo 1 - Utilizando a equipe de Tecnologia da Informação - TI, não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes cibernéticos. A Equipe será formada a partir dos membros das equipes de TI do próprio DNIT, que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes cibernéticos.

6. Neste modelo, as funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos em segurança.

7. A Equipe que utilizar este modelo desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades pró-ativas.

8. A ETIR poderá, a qualquer tempo, de acordo com sua necessidade e conveniência, migrar para outro modelo de implementação que melhor atenda as funções e serviços de tratamentos de incidentes e resposta a incidentes cibernéticos.

ESTRUTURA ORGANIZACIONAL

9. A ETIR ficará subordinada à Coordenação-Geral de Tecnologia da Informação - CGTI.

10. Para que seja efetiva em sua missão, a ETIR terá competência para solicitar informações e providências das empresas contratadas, prestadoras de serviços de TI, atuando assim como moderador e coordenador dos serviços.

11. Serão definidos em portaria o Agente Responsável, os membros titulares e substitutos da ETIR.

12. Compete ao Agente Responsável pela ETIR:

a) dimensionar a ETIR, de acordo com as necessidades institucionais;

b) submeter a indicação dos membros da ETIR e respectivos substitutos à aprovação do Gestor de Segurança da Informação;

c) coordenar as atividades da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

d) interagir com organismos externos de respostas a incidentes, principalmente com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV; e

e) assistir diretamente o Comitê de Segurança da Informação e o Gestor de Segurança da Informação.

13. Compete aos membros da ETIR e aos substitutos, quando necessário:

a) prestar os serviços aos quais a ETIR se propõe a prestar;

b) definir e documentar metodologia e procedimentos internos para o tratamento e resposta a incidentes;

c) criar as estratégias de resposta a incidentes de rede, elaborar procedimentos de resposta para incidentes previamente conhecidos, gerenciar e atribuir as atividades para a equipe distribuída;

d) auxiliar o Gestor de Segurança da Informação na tomada de decisões;

e) garantir que os incidentes na Rede de Computadores do DNIT sejam monitorados;

f) adotar procedimentos para assegurar que os usuários comuniquem incidentes de segurança da informação obtenham informações acerca das ações executadas;

g) auxiliar em treinamentos relacionados à Segurança da Informação, no que se refere à prevenção e combate a incidentes em redes computacionais;

h) recolher tempestivamente as provas quando da ocorrência de um incidente de rede computacional;

i) executar uma análise crítica sobre os registros de falha para assegurar que foram satisfatoriamente resolvidas;

j) investigar as causas dos incidentes nas redes computacionais e sistemas de informação; e

k) indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

14. Os membros da ETIR, bem como seu Agente Responsável, deverão destinar o tempo necessário para o desempenho das tarefas da Equipe e atuação nas ocorrências e incidências de riscos relacionadas a segurança da informação.

AUTONOMIA

15. A ETIR terá autonomia completa e poderá conduzir o seu público alvo para realizar ações ou medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança.

16. Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão, devendo ser homologadas pelo COSIC.

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.

Documento assinado eletronicamente por **Antônio Leite dos Santos Filho**, **Diretor-Geral**, em 13/05/2021, às 10:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Referência: Processo nº 50600.003041/2021-08 SEI nº 8149354

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