AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES

DELIBERAÇÃO Nº 364, DE 19 DE DEZEMBRO DE 2013

CAPÍTULO I
DO OBJETIVO E ABRANGÊNCIA

Art. 1° A Política de Segurança da Informação e Comunicações da Agência Nacional de Transportes Terrestres (PoSIC/ANTT) observará os princípios, objetivos e diretrizes estabelecidos nesta Portaria, bem como as disposições constitucionais, legais e regimentais vigentes.

Parágrafo único. As diretrizes da PoSIC aplicam-se ao ambiente informatizado e aos meios convencionais de processamento e comunicações da ANTT.

Art. 2° Integram a PoSIC normas gerais e específicas emanadas do Decreto nº 3505/00 que "Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal – APF", marco legal do assunto, da Lei nº 12527/11 (LAI), dos Decretos nº 7724/12 e 7845/2012, e das demais Instruções Normativas e Normas Complementares instituídas pelo Gabinete de Segurança Institucional da Presidência da República – GSI/PR "que regulamentam o assunto, no âmbito dos órgãos e entidades, da Administração Pública Federal – APF", bem como Normas e Procedimentos complementares que vierem a ser instituídos.

Art. 3° Esta PoSIC e as Normas e Procedimentos complementares, aplicam-se a todas as unidades da estrutura organizacional da ANTT, incluindo as Unidades Regionais, bem como a servidores, prestadores de serviço, colaboradores, fornecedores, estagiários, consultores externos e a quem, de alguma forma, execute atividades para a Agência.

§ 1º Os contratos, convênios, acordos, termos de cooperação e outros instrumentos congêneres celebrados pela ANTT devem atender aos preceitos desta PoSIC.

§ 2º Esta PoSIC também se aplica, no que couber, ao relacionamento da ANTT com outros órgãos e entidades públicas ou privadas.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 4° Para os fins desta Portaria entende-se por:

I – Política de Segurança da Informação e Comunicações (PoSIC): documento aprovado pela Diretoria Geral da ANTT, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
II – Comitê Gestor de Segurança da Informação e Comunicações (CGSIC): grupo de servidores com a responsabilidade de assessorar na implementação e acompanhamento das ações de segurança da informação e comunicações no âmbito da ANTT;

DELIBERAÇÃO Nº 364, DE 19 DE DEZEMBRO DE 2013

III – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de servidores com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes da rede que afetem a segurança da informação e comunicações;

IV – Agente Público: toda pessoa que, por força de lei, contrato ou de qualquer outro ato jurídico, com ou sem remuneração, preste serviços de natureza permanente, temporária, excepcional ou eventual;

V – informação - dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VI – ativo de informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma Unidade Organizacional;

VII – incidentes de segurança da informação e comunicações: ocorrências indesejadas ou inesperadas, que tenham uma grande probabilidade de comprometer a continuidade das operações do negócio e ameaçar a segurança da informação e comunicações;

VIII – gestão de riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos;

IX – infraestruturas críticas: são instalações, serviços, bens e sistemas cujas informações, se forem alvo de acesso, modificação, destruição ou divulgação não autorizada, resultarão em impactos na adequada prestação dos serviços públicos de transportes terrestres;

X – Termo de Responsabilidade: documento que tem por propósito sistematizar a concessão de acesso ao agente público, a fim de evitar a quebra de segurança da informação e comunicações; e

XI – Termo de Confidencialidade: documento que tem por propósito sistematizar os contratos, convênios, acordos e termos de cooperação e outros instrumentos congêneres celebrados pela ANTT, visando restringir a utilização dessas informações aos fins a que se destinam.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 5° Esta política abrange aspectos básicos da Segurança da Informação e Comunicações, especialmente:
I – disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

II – autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

III – integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino; e

DELIBERAÇÃO Nº 364, DE 19 DE DEZEMBRO DE 2013

IV – primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 6º Portarias, Normas e Procedimentos complementares serão elaboradas para a implantação e operacionalização das diretrizes previstas nos artigos 7º a 19 desta norma, cuja proposição competirá ao CGSIC e aprovação à Diretoria Geral da ANTT.

Seção I
Da Gestão da Segurança da Informação e Comunicações

Art. 7º A gestão da segurança da informação e comunicações compreende ações e métodos que vise à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional dos processos institucionais estratégicos, operacionais e táticos.

Seção II
Do Tratamento da Informação

Art. 8º Os ativos de informação devem ser inventariados e classificados, conforme o Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, o Decreto 7845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e demais exigências legais.

Art. 9º O uso de ativos de informação deve ser controlado e monitorado pela ANTT, respeitados os princípios legais, para garantir a utilização estrita e correta desses recursos, bem como minimizar riscos às atividades, aos serviços e à imagem institucional da Agência.

Seção III
Do Tratamento de Incidentes

Art. 10. Deverá ser estabelecido um plano de ação de resposta aos incidentes de segurança da informação e comunicações com o objetivo de interromper ou mitigar os impactos deles decorrentes.

DELIBERAÇÃO Nº 364, DE 19 DE DEZEMBRO DE 2013

Seção IV
Da Gestão de Riscos

Art. 11. Deverá ser implementado e mantido um processo de gestão de riscos com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações.

Parágrafo único. Os ativos de informação a serem protegidos deverão ser priorizados, bem como a definição e implantação de controles para a identificação e tratamento de problemas de segurança.

Seção V
Da Gestão de Continuidade de Negócios

Art. 12. O processo de gestão da continuidade de negócios deverá ser implementado, mantido e testado periodicamente visando reduzir, para um nível aceitável, o tempo de interrupção causado por incidentes e acidentes de segurança que afetem os ativos de informação e comunicações.

Seção VI
Das Infraestruturas Críticas

Art. 13. As informações referentes às infraestruturas críticas, tais como Plano de Continuidade de Negócios (PCN), Programa de Gerenciamento de Riscos (PGR) e as demais informações que possam comprometer a adequada prestação dos serviços públicos de transportes terrestres devem ser identificadas, classificadas e tratadas de forma a serem preservadas, e ter seu uso restrito às pessoas e áreas credenciadas.

Seção VII
Dos Controles de Acesso

Art. 14. Os recursos computacionais disponibilizados pela ANTT devem ser utilizados estritamente dentro do seu propósito institucional, sendo vedados para uso próprio ou de terceiros, entretenimento, veiculação de opiniões político-partidárias ou religiosas.

§ 1º A entrada e a saída de ativos de informação nas dependências da ANTT devem ser autorizadas e registradas por autoridade competente, conforme estabelecido por norma específica.

§ 2º É obrigatório o uso de crachá, que é pessoal e intransferível, o qual deve possibilitar de maneira clara e inequívoca o reconhecimento de seu portador, de acordo com o estabelecido por norma específica.

§ 3º 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 Agente Público.

DELIBERAÇÃO Nº 364, DE 19 DE DEZEMBRO DE 2013

§ 4º Os privilégios de acesso às informações devem ser definidos pelo gestor da área responsável pela informação.

§ 5º Em caso de desligamento da ANTT, os privilégios de acesso às informações e aos recursos computacionais devem ser cancelados imediatamente.

Seção VIII
Do uso de e-mail e acesso à Internet

Art. 15. O uso de e-mail e o acesso à Internet, no ambiente de trabalho da ANTT, devem ser para atender as necessidades de serviço.

Seção IX
Da capacitação e aperfeiçoamento

Art. 16. Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicações.

Seção X
Do patrimônio intelectual

Art. 17. As informações, os sistemas e os métodos criados pelos servidores da ANTT ou por prestadores de serviço, colaboradores, no exercício de suas funções, são patrimônios intelectuais da Instituição, não cabendo a seus criadores qualquer forma de direito autoral.

Parágrafo único. A utilização dessas informações, sistemas e métodos deve ser restrita aos fins a que se destinam, seu uso em eventos fora do âmbito da ANTT, do tipo apresentações em Seminários, Workshops, Foruns e demais eventos congêneres deverá ter autorização da Unidade Organizacional responsável e ciência do CGSIC.

Seção XI
Do Termo de Responsabilidade e Termo de Confidencialidade

Art. 18. Todo Agente Público em exercício na ANTT deve ter ciência e firmar o Termo de Responsabilidade.

Art. 19. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela ANTT, que necessitem ter informações da Agência, devem se comprometer a tratá-las de acordo com o Termo de Confidencialidade.

AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES

DELIBERAÇÃO Nº 364, DE 19 DE DEZEMBRO DE 2013

CAPITULO V
COMPETÊNCIAS E RESPONSABILIDADES

Art. 20. Compete a Diretoria da ANTT:

I – aprovar a Política de Segurança da Informação e Comunicações (PoSIC):

II – instituir o Comitê Gestor de Segurança da Informação e Comunicações (CGSIC); e

III – aprovar Normas e Procedimentos relativos à segurança da informação e comunicações no âmbito da ANTT.

Art. 21. Compete ao Comitê Gestor de Segurança da Informação e Comunicações (CGSIC):

I – coordenar e acompanhar a implementação da PoSIC e das Normas e Procedimentos complementares;

II – assessorar na implementação das ações de segurança da informação e comunicações na ANTT;

II – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

III – propor à Diretoria Geral Normas e Procedimentos complementares relativos à segurança da informação e comunicações no âmbito da ANTT;

IV – realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

V – monitorar e avaliar periodicamente as práticas de segurança da informação adotadas pela ANTT;
VI – acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

VII – propor programa orçamentário específico para as ações de segurança da informação e comunicações;

VIII – revisar e analisar periodicamente as diretrizes e normas estabelecidas nesta política visando a sua aderência e concordância aos objetivos estratégicos da ANTT e as legislações vigentes; e

IX – promover cultura de segurança da informação e comunicações.

Parágrafo único. O CGSIC será integrado por, pelo menos, 01 (um) representante das seguintes áreas funcionais da ANTT:

DELIBERAÇÃO Nº 364, DE 19 DE DEZEMBRO DE 2013

I – da Diretoria;
II – da Procuradoria Geral;
III – da Ouvidoria;
IV – da Assessoria de Comunicação Social;
V – do Centro de Documentação;
VI – da Corregedoria;
VII – de cada Superintendência Organizacional; e
VIII – de cada Unidade Regional.

Art. 22. Compete à Gerência de Tecnologia da Informação a elaboração e implementação de Normas e Procedimentos complementares, no âmbito da Tecnologia da Informação e em conformidade com as demais normas legais vigentes devendo, para isso:

I – Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) que deverá receber, analisar e responder notificações e atividades relacionadas a incidentes da rede de computadores que afetem a segurança das informações e tomar as providências de emergência pertinentes à segurança da informação e comunicações, imediatamente após detecção ou conhecimento de incidentes de segurança.

II – Prestar apoio técnico, administrativo e propor ao CGSIC as alterações nas normas e nos procedimentos de segurança da informação e comunicações, sempre que houver alteração no ambiente computacional ou atualizações tecnológicas, a fim de manter e melhorar o nível de segurança;

III – Avaliar o nível de segurança alcançado, emitindo relatórios periódicos de Análise de Riscos ao CGSIC;

IV – Definir as soluções técnicas necessárias para a implantação e adequação do ambiente da ANTT à PoSIC e garantir a disponibilidade de recursos tecnológicos necessários à implementação das ações de segurança da informação e comunicações.

Art. 23. Compete às demais Unidades Organizacionais da ANTT, a proposição ao CGSIC de Normas e Procedimentos complementares em seu âmbito de atuação, bem como a implementação desta PoSIC e demais normas legais vigentes.

Parágrafo único. A proposição de normas e procedimentos complementares deverá ser submetida ao CGSIC para avaliação.

Art. 24. Compete ao Agente Público:

I – A preservação da imagem institucional da ANTT;

II – Comunicar ao CGSIC os incidentes que afetam a segurança dos ativos de informação e comunicações ou ao descumprimento desta PoSIC; e

III – Comunicar à ETIR os incidentes da rede de computadores.

DELIBERAÇÃO Nº 364, DE 19 DE DEZEMBRO DE 2013

CAPITULO VI
PENALIDADES

Art. 25. O desrespeito ou violação dos termos contidos nesta Portaria será apurado em Processo Administrativo podendo resultar:

I – na suspensão temporária ou permanente de privilégios de acesso aos recursos que estiverem disponíveis;

II – em penas e sanções legais impostas por meio de medidas administrativas sem prejuízo das demais medidas penais e/ou cíveis;

III – na aplicação do disposto no Código de Ética da ANTT; e

IV – na aplicação das penalidades previstas na Lei 8112/90.

CAPITULO VII
VIGÊNCIA

Art. 26. Todos os instrumentos normativos gerados a partir da aprovação desta Portaria e a própria PoSIC, devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 02 anos.

CAPITULO VIII
DISPOSIÇÕES GERAIS

Art. 27. Todas as dúvidas ou casos porventura omissos desta PoSIC deverão ser reportados ao CGSIC.