AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES

PORTARIA Nº 559, DE 3 DE JULHO DE 2013

Aprova a Política de Segurança da Informação e Comunicações da Agência Nacional de Telecomunicações.

O CONSELHO DIRETOR DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, no uso das atribuições que lhe foram conferidas pelo art. 133, inciso XXII, do Regimento Interno da Agência, aprovado pela Resolução nº 612, de 29 de abril de 2013, e alterações posteriores;

CONSIDERANDO a Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República - GSIPR, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;

CONSIDERANDO a recomendação da Norma Complementar Nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que dispõe sobre as diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO o constante dos autos do Processo nº 53500.024990/2010,

R E S O L V E :

Art. 1º Aprovar a Política de Segurança da Informação e Comunicações da Agência Nacional de Telecomunicações, anexa a esta Portaria.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

JOÃO BATISTA DE REZENDE
Presidente do Conselho

.

ANEXO DA PORTARIA Nº 559, DE 3 DE JULHO DE 2013

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES

CAPÍTULO I

DO OBJETIVO E ABRANGÊNCIA

Art. 1º. A Política de Segurança da Informação e Comunicações da Agência Nacional de Telecomunicações (POSIC/Anatel) tem por finalidade estabelecer diretrizes para a segurança do manuseio, tratamento, controle e proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio, no âmbito da Anatel, observadas as diretrizes estabelecidas pelo poder público quanto à transparência e o acesso às informações públicas.

Art. 2º. Esta política se aplica às atividades de todo usuário de informação que venha a ter acesso aos ativos de informação protegidos por esse regulamento.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º. Para os fins desta Política, considera-se:

I. ativo de informação – patrimônio composto por todos os dados, informações e conhecimentos obtidos, gerados e utilizados durante a execução dos sistemas e processos de trabalho da Anatel;

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

III. classificação – atribuição, pela autoridade competente, de grau de sigilo a dado, informação, documento, material, área ou instalação;

IV. confidencialidade – propriedade de que o dado ou a informação não esteja disponível ou revelado a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

V. conhecimento – conhecimento é a soma da experiência das pessoas com as informações adquiridas ao longo do tempo, podendo ser tácito (cognitivo) ou explícito (formalizado);

VI. controle de acesso – procedimento destinado a conceder ou bloquear o acesso aos ativos de informação;

VII. dado – qualquer elemento identificado em sua forma bruta, que em determinado contexto não conduz, por si só, à compreensão de determinado fato ou situação;

VIII. direito de acesso – privilégio relacionado a um cargo ou pessoa para ter acesso a um determinado ativo de informação;

IX. disponibilidade – qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

X. documento – unidade de registro de informações, qualquer que seja o suporte ou formato;

XI. evento de segurança da informação – ocorrência identificada a partir de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou outra que possa ser relevante para a segurança da informação;

XII. gestor da informação – servidor responsável pela administração das informações geridas nos processos de trabalho de sua responsabilidade;

XIII. incidente de segurança da informação – evento de segurança da informação, indesejado ou inesperado, que comprometa ou ameace a integridade, a autenticidade, a confidencialidade ou a disponibilidade de qualquer ativo de informação da Anatel;

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

XV. informação pessoal – aquela relacionada à pessoa natural identificada ou identificável;

XVI. informação sigilosa – aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

XVII. instrumento de trabalho – recursos empregados no acesso, manuseio, proteção, transmissão e armazenamento dos ativos de informação, dentre outros: computadores, incluindo seus componentes, acessórios e periféricos, redes de dados, telefones, sistemas de processamento da informação (sistemas interativos da Anatel) e bancos de dados;

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

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

XX. responsabilidade – deveres de um usuário em relação ao ativo de informação ao qual ele tem direito de acesso;

XXI. Segurança da Informação e Comunicações (SIC) – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e das informações. Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

XXII. tratamento da informação – conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

XXIII. usuário – qualquer pessoa que utilize os ativos de informação da Anatel, de acordo com a seguinte classificação:

a. externo – qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada, aos ativos de informação produzidos ou custodiados pela Anatel e que não seja caracterizada como usuário interno;

b. interno – qualquer pessoa que, mesmo transitoriamente ou sem remuneração, exerça, na Anatel cargo, emprego, função pública, ou que trabalhe para empresa prestadora de serviço contratada ou conveniada para a execução de atividades da Agência.

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 4º. Na aplicação e interpretação das regras estabelecidas na POSIC/Anatel, devem ser observados os seguintes instrumentos legais e normativos, sem prejuízo do disposto em normas supervenientes que venham a regular a matéria:

I. Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais ;

II. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

III. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37, e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

IV. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal e dá outras providências;

V. Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil);

VI. Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VII. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

VIII. Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores – Internet;

IX. Portaria Interministerial nº 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores - internet e dá outras providências;

X. Portaria nº 24 da Anatel, de 7 de janeiro de 2010, que institui a Comissão de Segurança da Informação (CSI) no âmbito da Anatel;

XI. Decreto nº 6.029, de 1º de fevereiro de 2007, que institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;

XII. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

XIII. Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 13 de outubro de 2008, que estabelece a Metodologia de Gestão de Segurança da Informação e Comunicações para os órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XIV. Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XV. Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

XVI. Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XVII. Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009, que disciplina as Diretrizes para Gestão de Continuidade de Negócios nos aspectos relacionados à Segurança da Informação e Comunicações - GCN nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XVIII. Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 7 de maio de 2010, que disciplina as diretrizes para implementação de Controles de Acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XIX. Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XX. Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 22 de novembro de 2010, que estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

XXI. ABNT NBR ISO/IEC 27001, publicada em 31 de março de 2006, que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI) documentado dentro do contexto dos riscos de negócio globais da organização;

XXII. ABNT NBR ISO/IEC 27002, publicada em 31 de agosto de 2005, que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

XXIII. ABNT NBR ISO/IEC 27005, publicada em 17 de novembro de 2011, que fornece diretrizes para o processo de gestão de riscos de segurança da informação.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 5º. São princípios da POSIC/Anatel:

I. a legalidade, a impessoalidade, a moralidade, a publicidade, a eficiência, a celeridade e a ética na proteção do ativo de informação;

II. a preservação da disponibilidade, da integridade e da autenticidade do ativo de informação da Anatel;

III. a busca de melhores práticas e a atualização tecnológica na proteção dos ativos de informação;

IV. a responsabilidade individual na utilização dos ativos de informação;

V. a transparência no tratamento das informações institucionais e pessoais, respeitando-se a intimidade, a vida privada, a honra e a imagem das pessoas, bem como as liberdades e garantias individuais.

CAPÍTULO V
DAS DIRETRIZES GERAIS

Art. 6º. Serão elaboradas portarias específicas destinadas à implantação e operacionalização das diretrizes previstas nesta norma, cuja aprovação competirá ao Conselho Diretor.

Seção I
Da Gestão da Segurança da Informação e Comunicações

Art. 7º. A gestão da segurança da informação e comunicações compreende a preservação da informação da Anatel quanto aos aspectos de disponibilidade, autenticidade confidencialidade e integridade, independentemente do meio que se encontrem.

Parágrafo único. De forma a promover a gestão e fomentar os aspectos de segurança da informação, a Comissão de Segurança da Informação da Anatel, órgão colegiado, de natureza consultiva e de caráter permanente, atuará na proposição e condução das diretrizes da POSIC/Anatel, bem como no assessoramento do Conselho Diretor em matérias correlatas, conforme previsto na Portaria nº 24 da Anatel, de 7 de janeiro de 2010.

Seção II

Do Tratamento da Informação

Art. 8º. As informações de propriedade da Anatel devem ser utilizadas para os fins a que se destinam e não podem ser apropriadas pelos usuários.

§ 1º. O uso de ativos de informação e dos instrumentos de trabalho pode ser controlado e monitorado pela Anatel para garantir a utilização estrita e correta desses recursos, bem como minimizar riscos às atividades, aos serviços e à imagem da Agência.

§ 2º. A forma do tratamento e utilização dos dados e informações decorrentes das atividades de monitoramento será disciplinada em norma específica.

Art. 9º. Os ativos de informação devem ser inventariados e classificados, conforme exigências legais.

Seção III

Do Tratamento de Incidentes

Art. 10. Deve ser estabelecido um plano de ação de resposta aos incidentes de segurança da informação com o objetivo de interromper ou minimizar os impactos decorrentes dos incidentes de segurança da informação.

Parágrafo único. Todo usuário, ao tomar conhecimento de qualquer incidente ou suspeitar da possibilidade de ocorrência de um incidente de segurança da informação, deve notificar o fato imediatamente à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIS) da Anatel para as providências cabíveis.

Seção IV

Da Gestão de Riscos

Art. 11. Deve ser estabelecido um processo de gerenciamento de riscos com objetivo de identificar possíveis vulnerabilidades que podem implicar riscos para a segurança das informações.

Parágrafo único. Em suas atividades a Comissão de Segurança da Informação deverá considerar, principalmente, a identificação dos riscos mais relevantes aos quais a informação da Anatel está exposta e a priorização das ações voltadas ao tratamento dos riscos apontados, tais como implantação de novos controles, criação de novas regras e procedimentos, e reformulação de sistemas.

Seção V

.

Da Gestão de Continuidade

Art. 12. Deve ser estabelecido um plano para garantir a continuidade regular do exercício das funções institucionais sob a perspectiva da disponibilidade dos ativos de informação da Anatel.

Seção VI

Da Conformidade

Art. 13. O cumprimento da POSIC/Anatel, de suas normas e procedimentos será acompanhado pela Comissão de Segurança da Informação da Anatel.

Seção VII

Dos Controles de Acesso

Art. 14. Os ativos de informação, quando aplicável, devem ser submetidos ao controle de acesso, sendo protegidos contra perda e usos indevidos, conforme disposto em normas específicas.

Art. 15. O identificador pessoal de acesso aos ativos de informação é intransferível, não podendo ser compartilhado ou armazenado de forma visível e desprotegida.

Seção VIII

Uso de Correio Eletrônico (e-mail)

Art. 16. A Anatel deverá estabelecer, em norma específica, regras para o uso de Correio Eletrônico (*e-mail*).

Seção IX

Acesso à Internet

Art. 17. A Anatel deverá estabelecer, em norma específica, regras para o acesso à internet.

Seção X

.

Da Sensibilização, Conscientização e Capacitação

Art. 18. Deve ser estabelecido um programa de divulgação, sensibilização, conscientização e capacitação em segurança da informação e comunicações direcionado aos usuários internos da rede corporativa da Anatel.

§ 1º. Todos os usuários dos ativos de informação da Anatel devem ter ciência de que o uso das informações e dos sistemas corporativos pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da POSIC/Anatel e das normas de segurança da informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

CAPÍTULO VI
DA APURAÇÃO DAS IRREGULARIDADES E DAS PENALIDADES

Art. 19. A violação das normas e procedimentos relativos à POSIC/Anatel será avaliada pela Comissão de Segurança da Informação que tomará as medidas cabíveis e encaminhará os autos para a Corregedoria da Anatel, quando aplicável.

CAPÍTULO VII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 20. Compete à Comissão de Segurança da Informação:

I. propor ao Conselho Diretor, para aprovação, a Política de Segurança da Informação e Comunicações da Anatel

II. definir o modelo de gestão corporativa da segurança da informação e comunicações e fomentar sua aplicação;

III. propor a elaboração e a revisão de normas e procedimentos inerentes à segurança da informação;

IV. propor metas e ações corporativas em segurança da informação e comunicações;

V. coordenar as ações de segurança da informação e comunicações;

VI. propor as ações corretivas cabíveis nos casos de quebra de segurança;

VII. analisar incidentes de segurança da informação e encaminhar à Corregedoria aqueles passíveis de correição;

VIII. propor ajustes no modelo de gestão corporativa da segurança da informação e comunicações, e nas ações necessárias à sua implementação, com subsídio no monitoramento e avaliação periódica das práticas de segurança da informação e comunicações;

IX. elaborar proposta e promover atualização periódica de plano com medidas que garantam a continuidade das atividades da Anatel e o retorno à situação de normalidade em caso de desastre ou falha nos recursos que suportam os processos vitais de negócio da Agência;

X. manifestar-se sobre ações corporativas em segurança da informação e comunicações;

XI. requerer, às unidades administrativas da Anatel, informações que considerar necessárias ao acompanhamento das ações de gestão de segurança da informação e comunicações;

XII. promover a divulgação de boas práticas em segurança da informação e comunicações;

XIII. submeter à aprovação minutas de normativos e propostas de natureza estratégica ou que necessitem de cooperação intersetorial que versem sobre segurança da informação e comunicações;

XIV. instituir grupos de trabalho para tratar de temas específicos para as ações de segurança da informação e comunicações;

XV. interagir com as unidades administrativas da Agência ou entidades externas, objetivando o pleno atendimento ao objeto desta POSIC;

XVI. a edição das demais normas referentes ao seu funcionamento.

Parágrafo único. A Comissão de Segurança da Informação é presidida pelo Gestor de Segurança da Informação, composta nos termos da Portaria nº 24 da Anatel, de 7 de janeiro de 2010.

Art. 21. Compete à área de tecnologia da informação:

I. prestar apoio técnico e administrativo às atividades da Comissão de Segurança da Informação;

II. propor à Comissão de Segurança da Informação a atualização da Política, das normas e dos 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 à Comissão de Segurança da Informação;

IV. definir as soluções técnicas necessárias para a implantação e adequação do ambiente da Anatel à POSIC/Anatel;

V. garantir a disponibilidade de recursos tecnológicos necessários à implementação das ações de segurança da informação e comunicações.

Parágrafo único. As normas complementares definidas no Inciso I deste artigo deverão ser elaboradas e submetidas à aprovação em até 24 meses após a publicação desta Política.

Art. 22. Compete à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR):

I. tomar as providências de emergência pertinentes à segurança da informação e comunicações, imediatamente após detecção ou conhecimento de incidentes de segurança da informação no âmbito da Anatel;

II. analisar os incidentes de segurança da informação e encaminhar mensalmente relatório dos incidentes à Comissão de Segurança da Informação.

.

Parágrafo único. Os membros da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação serão indicados pela Comissão de Segurança da Informação e suas atribuições serão definidas em portaria específica.

Art. 23. Os usuários dos ativos de informação devem conhecer e cumprir a POSIC/Anatel, bem como os demais instrumentos normativos relacionados, sendo-lhes facultado o direito de propor alterações nesses documentos.

CAPÍTULO VIII
DA ATUALIZAÇÃO E VIGÊNCIA

Art. 24. A Política de Segurança da Informação e Comunicações e os documentos normativos gerados a partir dela devem ser revisados e atualizados no máximo a cada três anos, ou imediatamente, caso ocorram eventos ou fatos relevantes que exijam uma revisão extraordinária.

Art. 25. Esta Portaria entre em vigor na data da sua publicação.