SERVIÇO PÚBLICO FEDERAL
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
DO RIO GRANDE DO NORTE

RESOLUÇÃO Nº 99/2012-CONSUP **Natal (RN), 21 de dezembro de 2012.**

Aprova a Política de Segurança da Informação e Comunicação – PSIC, do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte.

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE, faz saber que este Conselho, reunido ordinariamente nesta data, no uso das atribuições legais que lhe confere o Art. 9º do Estatuto do IFRN,

CONSIDERANDO

o que consta no Processo nº 23421.030969.2012-00, de 20 de dezembro de 2012,

R E S O L V E:

APROVAR, na forma do anexo, a Política de Segurança da Informação e Comunicação – PSIC, do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte.

BELCHIOR DE OLIVEIRA ROCHA
Presidente

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Dispõe sobre a criação da Política de Se-gurança da Informação e Comunicação do Instituto Federal do Rio Grande no Norte.

CAPITULO I

DA FINALIDADE

Art. 1º. A Política de Segurança da Informação e Comunicação do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN) é uma declaração formal da Instituição acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os servidores, colaboradores, consultores externos, estagiários, alunos e prestadores de serviço que exerçam atividades no âmbito do IFRN, ou quem quer que tenha acesso a dados ou informações no ambiente do IFRN. Tem como propósito estabelecer diretrizes, normas, procedimentos e responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes ao IFRN.

CAPITULO II

DAS FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

Art. 2º. As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFRN são as seguintes:

I – Constituição Federal de 1988;

II – Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto Lei no 2848/40 (Código Penal Brasileiro), de modo a prever a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

III – Decreto nº 1.171, de 24 de junho de 1994, que dispõe sobre o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

IV – Lei nº 3.689, de 3 de outubro de 1941, atualizado até as alterações introduzidas pela Lei no 11.900, de 8 de janeiro de 2009;

V – Lei nº 5.869, de 11 de janeiro de 1973;

VI – Lei nº 7.232, de 29 de outubro de 1984, que dispõe sobre a Política Nacional de Informática;

VII – Lei nº 8.027, de 12 de abril de 1990, que dispõe sobre as normas de conduta a serem observadas pelos servidores públicos civis da União, das Autarquias e das Fundações Públicas;

VIII – Lei nº 8.112, de 11 de dezembro de 1990, que trata do regime jurídico dos servidores

públicos civis da União, das autarquias e das fundações públicas federais;

IX – Lei nº 8.429, de 2 de junho de 1992, que dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional;

X – Decreto nº 6.029, de 1o de fevereiro de 2007, que trata do Sistema de Gestão da Ética do Poder Executivo Federal;

XI – Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

XII – Lei nº 12.737, de 30 de novembro de 2012, que dispões sobre a tipificação criminal de delitos informáticos;

XIII – Decreto nº 1.048, de 21 de janeiro de 1994, que trata do Sistema de Administração dos Recursos de Informação e Informática da Administração Pública Federal;

XIV – 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;

XV – Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da Administração Pública Federal; e

XVI – Outros dispositivos infralegais aplicáveis, a saber:

a) Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;

b) Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;

c) Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;

d) Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;

e) Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;

f) Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;

g) Acórdão nº 1603/2008 – Plenário do Tribunal de Contas da União (TCU);

h) Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;

i) Norma ABNT NBR ISO Guia nº 73:2002: Gestão de Riscos / Vocabulário;

j) Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;

k) Norma ABNT NBR ISO/IEC nº 27002:2005: Código de Prática para a Gestão de Segurança da Informação;

l) Norma ISO/IEC TR nº 13335-3:1998, que fornece técnicas para a gestão de segurança na área de tecnologia da informação, baseada nas normas ISO/IEC no 13335-1 e TR ISO/IEC no 13335-2; e

m) Norma ISO/IEC GUIDE nº 51:1999, que fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

CAPITULO III

DA DECLARAÇÃO DE COMPROMETIMENTO DA REITORIA

Art. 3º. A alta direção do IFRN na figura do Reitor, declara-se comprometida em proteger todos os seus ativos de informação.

CAPITULO IV

DOS TERMOS E DEFINIÇÕES

Art. 4º. Para os efeitos desta Política, são adotadas as seguintes definições:

I – *Ativo de informação*: qualquer informação que tenha valor para a Instituição, nos termos da Norma ISO/IEC no 13335-1:2004;

II – *Recursos de processamento da informação*: qualquer sistema, serviço ou infraestrutura de processamento da informação, ou as instalações físicas que os abriguem;

III – *Segurança da informação*: preservação da confidencialidade, da integridade e da disponibilidade da informação. Adicionalmente, outras propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas;

IV – *Controle*: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle também é usado como sinônimo para proteção ou contra-medida;

V – *Evento de segurança da informação*: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança da informação, nos termos da Norma ISO/IEC TR no 18044:2004;

VI – *Incidente de segurança da informação*: ocorrência indicada por um único ou por uma série de eventos de segurança da informação indesejados ou inesperados, que apresentem grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação, nos termos da Norma ISO/IEC TR no 18044:2004;

VII – *Risco*: combinação da probabilidade de ocorrência de um evento e de suas consequências;

VIII – *Ameaça*: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição, nos termos da Norma ISO/IEC no 13335-1:2004;

IX – *Vulnerabilidade*: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

X – *Contingência*: indisponibilidade ou perda de integridade da informação que os controles de segurança não tenham conseguido evitar;

XI – *Plano de continuidade de negócios*: conjunto de procedimentos a serem adotados quando a Instituição se deparar com problemas que comprometam o andamento normal dos processos e a

consequente prestação dos serviços;

XII – *Princípios da Segurança da Informação e Comunicações*: princípios que regem a Segurança da Informação e Comunicações, nos termos do art. 3° do Decreto n° 3.505, de 13 de junho de 2000, ou seja, a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não-repúdio;

XIII – *Termo de responsabilidade*: acordo de confidencialidade e não divulgação de informações, que atribui responsabilidades ao servidor e ao administrador de serviço quanto ao sigilo e à correta utilização dos ativos de propriedade da Instituição ou por ela custodiados;

XIV – *Quebra de segurança*: ação ou omissão, intencional ou acidental, que resulte no comprometimento da Segurança da Informação e Comunicações;

XV – *Tratamento da informação*: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive das sigilosas;

XVI – *Continuidade de negócios*: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável e previamente definido;

XVII – *Plano de gerenciamento de incidentes*: plano de ação claramente definido e documentado, para ser utilizado quando ocorrer um incidente e que especifique as pessoas, recursos, serviços e outras ações que forem necessárias para implementar o processo de gerenciamento de incidentes;

XVIII – *Plano de Continuidade*: plano constituído de um conjunto de medidas, regras e procedimentos definidos, a serem adotados para assegurar que, após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações, as funções ou atividades críticas da Instituição possam ser mantidas ou recuperadas;

XIX – *Gestão da continuidade de negócios*: processo contínuo de gestão e governança, suportado pela alta direção, com recursos apropriados para garantir que as ações necessárias sejam executadas de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento dos serviços;

XX – *Análise de riscos*: uso sistemático de informações para identificar fontes e estimar seu risco;

XXI – *Avaliação de riscos*: processo por intermédio do qual se compara o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;

XXII – *Gestão de Riscos de Segurança da Informação e Comunicação*: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias, especificamente, para mitigar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXIII – *Identificação de riscos*: processo de localização, enumeração e caracterização dos elementos do risco;

XXIV – *Tratamento dos riscos*: processo de implementação de ações de Segurança da Informação e Comunicações destinadas a evitar, reduzir, reter ou transferir um risco;

XXV – *Gestor*: agente da Instituição responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas de uso da informação;

XXVI – *Usuário interno*: qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente ao IFRN;

XXVII – *Usuário externo*: qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente ao IFRN;

XXVIII – *Comunicação oficial*: tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas do IFRN de atividades especiais ou ainda de projetos específicos; e

XXIX – *Comunicação informal*: tráfego de documentos, informações ou formulários que não estejam incluídos no conceito de que trata o inciso anterior, emitidos via caixas postais eletrônicas individuais de autoridade, servidor, estagiário ou fornecedor de bens e/ou serviços.

CAPITULO V

DOS PRINCÍPIOS

Art. 5º. Esta Política abrange onze aspectos básicos da Segurança da Informação e Comunicações, destacados a seguir:

I – *Confidencialidade*: somente pessoas devidamente autorizadas pelo gestor da informação devem ter acesso a informação não pública;

II – *Integridade*: somente operações de alteração, supressão e adição autorizadas pelo IFRN devem ser realizadas nas informações;

III – *Disponibilidade*: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;

IV – *Autenticidade*: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;

V – *Criticidade*: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

VI – *Não-Repúdio*: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo sua identificação;

VII – *Responsabilidade*: as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todos os servidores do IFRN são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação advindas desta Política;

VIII – *Ciência*: todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;

IX – *Ética*: todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação do IFRN devem ser respeitados;

X – *Legalidade*: além de observar os interesses do IFRN, as ações de Segurança da Informação e Comunicações levarão em consideração leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e aos direitos de uso; e

XI – *Proporcionalidade*: o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações no âmbito do IFRN serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

CAPITULO VI

DO ESCOPO

Art. 6º. O escopo do Plano de Segurança da Informação do IFRN refere-se:

I – aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos demais documentos normativos que os incorporarão;

II – aos requisitos de segurança humana;

III – aos requisitos de segurança física;

IV – aos requisitos de segurança lógica; e

V – à sustentação dos procedimentos, dos processos de trabalho e dos ativos que influirão diretamente nos produtos e serviços oriundos da informação e comunicação do IFRN.

CAPITULO VII

DA ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 7º. A estrutura normativa da Segurança da Informação e Comunicação do IFRN é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

I – *Política de Segurança da Informação (PSI)*: constituída por este documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação, e será detalhada em um conjunto de Normas específicas;

II – *Normas de Segurança da Informação (Normas)*: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem observados em diversas instâncias em que a informação seja tratada. A cada Norma será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações contidas no documento "Atividade de Normatização" do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República; e

III – *Procedimentos de Segurança da Informação e Comunicações (Procedimentos)*: instrumentalizam o disposto nas Normas, permitindo sua direta aplicação nas atividades do IFRN, cabendo a cada gestor a responsabilidade de gerá-los. Cada procedimento poderá ainda ser detalhado em instruções. Estes procedimentos e instruções serão de uso interno, não sendo obrigatória sua publicação.

CAPITULO VIII

DAS DIRETRIZES GERAIS

Art. 8º. É dever de todos zelar pela Segurança da Informação e Comunicações.

Art. 9º. O IFRN, na condição de usuário dos serviços providos pela Rede Nacional de Ensino e

Pesquisa (RNP) é, por princípio, signatário de suas Políticas e Normas de Segurança.

Art. 10º. Usuários internos e externos devem observar as seguintes diretrizes:

I – *Acesso à informação*: será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFRN é considerada seu patrimônio e deve ser protegida;

II – *Recursos disponibilizados pelo IFRN*: na condição de recursos da propriedade do IFRN, serão fornecidos com o propósito único de garantir o desempenho das suas atividades;

III – *Tratamento de informações*: as normas para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação serão definidas de acordo com a classificação desta, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor;

IV – *Gestão de incidentes*: será estabelecido um serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências;

V – *Gestão de Riscos*: será estabelecido um processo de Gestão de Riscos, contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicação, de modo a produzir subsídios para a Gestão de Continuidade dos Negócios. Os riscos devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e em fatores de risco como ameaça, vulnerabilidade, probabilidade e impacto;

VI – *Auditoria e Conformidade*: deverão ser levantados regulamente os aspectos legais de segurança aos quais as atividades do IFRN estão submetidas, de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão;

VII – *Segurança Física*: controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos do IFRN e que garantam a proteção dos recursos, de forma que apenas as pessoas autorizadas tenham acesso, de modo a restringir a entrada e saída de visitantes, pessoal interno, equipamentos e mídias e estabelecer perímetros de segurança;

VIII – *Uso de e-mail*: o correio eletrônico é um serviço disponibilizado pelo IFRN aos servidores e estudantes na rede de comunicação de dados, para aumentar a agilidade, a segurança e a economia da comunicação oficial e informal;

IX – *Capacitação e Aperfeiçoamento*: os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicação;

X – *Acesso à Internet*: todos os servidores têm o direito de acesso à internet, com utilização exclusiva para fins diretos e complementares às atividades do setor, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham a contribuir para o desenvolvimento de seus trabalhos. O acesso à Internet pelo corpo discente da Instituição deverá observar estritamente os objetivos acadêmicos constantes dos programas de cursos;

XI – *Patrimônio Intelectual*: as informações, os sistemas e os métodos criados pelos servidores do IFRN, no exercício de suas funções, são patrimônios intelectuais da Instituição, não cabendo a seus criadores qualquer forma de direito autoral; e

XII – *Termo de Responsabilidade e Sigilo*: é o documento oficial que compromete colaboradores,

terceirizados e prestadores de serviço com a PSI do IFRN.

CAPITULO IX

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 11º. A implementação, o controle e a gestão da PSI observarão a seguinte estrutura de gerenciamento:

I – O Conselho Superior será responsável pela aprovação da PSI;

II – Ao Comitê Gestor de Segurança da Informação compete:

a) promover a cultura de Segurança da Informação;

b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) propor recursos necessários às ações de Segurança da Informação;

d) instituir e coordenar a Equipe de Tratamento e Respostas a Incidentes de Segurança da Informação;

e) realizar e acompanhar estudos de novas tecnologias, no que diz respeito a possíveis impactos sobre a Segurança da Informação;

f) manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República, para o trato de assuntos relativos à Segurança da Informação e Comunicação;

g) coordenar as revisões das normas de segurança em vigor;

h) promover intercambio científico-tecnológico entre órgãos e as entidades da Administração Pública federal e as instituições públicas e privadas sobre as atividades de Segurança da Informação (art.3º do Decreto 3.505 de 2000); e

h) propor Normas adicionais e procedimentos relativos à Segurança da Informação no âmbito do IFRN.

CAPITULO X

DA DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

Art. 12º. A Política e as Normas de Segurança da Informação e Comunicação devem ser divulgadas a todos os servidores do IFRN e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Art. 13º. As áreas atingidas por esta PSI são imediatamente responsáveis pela elaboração e proposição de normas, procedimentos e atividades necessárias ao cumprimento.

Art. 14º. As áreas deverão submeter suas propostas de normas ao Comitê de Segurança da Informação para análise, discussão e aprovação.

Art. 15º. Após aprovação, as normas e procedimentos serão divulgados aos interessados pela área responsável por sua proposição e manutenção.

CAPITULO XI

DAS DISPOSIÇÕES FINAIS

Art. 16º. Esta PSI será revista e alterada sempre que as atribuições e normas do IFRN justificarem tais alterações, sendo ainda obrigatória sua revisão anual.

Art. 17º. O descumprimento ou a violação de um ou mais itens da Política ou das suas Normas, procedimentos ou atividades pertinentes à Segurança da Informação, serão tratados conforme a legislação e os regulamentos internos aplicáveis.

Art. 18º. A presente política entra em vigor a partir da data de sua publicação.