INSTITUTO FEDERAL
NORTE DE MINAS GERAIS

Comitê de Segurança da Informação e Comunicações

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - POSIC

1 FINALIDADE

A Política de Segurança da Informação e Comunicações do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO NORTE DE MINAS GERAIS-IFNMG é uma declaração formal da Instituição acerca do 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 e prestadores de serviço que exerçam atividades no âmbito do IFNMG ou quem quer que tenha acesso a dados ou informações no ambiente do IFNMG. O seu propósito é estabelecer diretrizes, normas, procedimentos, e responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes ao IFNMG.

2 FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicações do IFNMG são:

2.1 Constituição Federal de 1988 reformada em 2008;

2.2 Lei nº 9.983, de 14 de julho de 2000 - Altera o Decreto Lei nº 2848/40 – Código Penal - tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

2.3 Decreto 1.171, de 24 de junho de 1994 - Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;

2.4 Lei 3.689, de 03 de outubro de 1941, atualizado até as alterações introduzidas pela Lei nº 11.900, de 08 de janeiro de 2009;

2.5 Lei 5.869, de 11 de janeiro de 1973;

2.6 Lei nº 7.232 de 29 de Outubro de 1984 - Política Nacional de Informática, e dá outras providências;

2.7 Lei nº 8.027 de 12 de abril de 1990 - Normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências;

2.8 Lei nº 8.112 de 11 de dezembro de 1990 - Regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

2.9 Lei nº 8.429 de 2 de junho de 1992 - 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 e dá outras providências;

2.10 Decreto nº 6.029 de 1 de fevereiro de 2007 - Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;

2.11 Lei nº 8.159 de 8 de janeiro de 1991 - política nacional de arquivos públicos e privados e dá outras providências;

2.12 Decreto nº 1.048 de 21 de janeiro de 1994 - Sistema de Administração dos Recursos de Informação e Informática, da Administração Pública Federal, e dá outras providências;

2.13 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;

2.14 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 dá outras providências;

2.15 Normas e Resoluções do Gabinete de Segurança Institucional da Presidência da Republica;

2.15.1 Instrução Normativa GSI Nº 01 de 13 de Junho de 2008;

2.15.2 Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 Out 2008;

2.15.3 Norma Complementar nº 03/IN01/DSIC/GSIPR, de 03 Jul 2009;

2.15.4 Norma Complementar nº 04/IN01/DSIC/GSIPR, de 17 Ago 2009;

2.15.5 Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 Ago 2009;

2.15.6 Norma Complementar nº 06/IN01/DSIC/GSIPR , de 23 Nov 2009;

2.16 Acórdão 1603/2008 do Plenário do Tribunal de Contas da União – TCU;

2.17 ABNT NBR ISO 17799: 2005 - Código de Práticas para a Gestão da Segurança da Informação;

2.18 ABNT NBR ISO Guia 73: 2002 - Gestão de Riscos / Vocabulário;

2.19 ABNT NBR ISO/IEC 27001:2005 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gerência da Segurança da Informação – Requisitos;

2.20 ABNT NBR ISO/IEC 27002:2005 – Código de Prática para a Gestão de Segurança da Informação;

2.21 ISO/IEC TR 13335-3: 1998 - fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1 e TR ISO/IEC 13335-2;

2.22 ISO/IEC GUIDE 51: 1999 - fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

3 DECLARAÇÃO DE COMPROMETIMENTO DA REITORIA

A alta direção do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO NORTE DE MINAS GERAIS, na pessoa do Reitor, declara-se comprometida em proteger todos os seus ativos de informação.

4 INSTÂNCIAS ADMINISTRATIVAS

Para os efeitos desta Política e das normas nela originadas, entende-se por:

4.1 Comitê Gestor de Tecnologia da Informação (CGTI): instância autônoma que atende ao disposto na Instrução Normativa nº 04/SLTI/MPOG de 19/05/2008 em seu Art. 4º Inciso IV, possui natureza consultiva e deliberativa e é responsável pelo alinhamento e regulação das ações de TIC ao disposto no Plano de Desenvolvimento Institucional (PDI) e Plano Estratégico Institucional (PEI);

4.2 Diretoria de Gestão de Tecnologia da Informação (DGTI): instância administrativa/executiva responsável por propor as políticas e programas do IFNMG na área de informática e telecomunicações, bem como por sua implementação e gestão;

4.3 Gerência de Desenvolvimento, administração e Manutenção de Tecnologia da Informação do IFNMG: instância responsável pelo desenvolvimento, implantação e manutenção dos recursos e serviços de tecnologia da informação e comunicações no âmbito do IFNMG;

4.4 Coordenação de Tecnologia da Informação de um campus: instância que tem como atribuição principal o gerenciamento da rede local, bem como dos recursos de TIC do campus a ela conectados, direta ou indiretamente.

4.5 Unidade: qualquer instância administrativa do IFNMG a exemplo dos *campi*, unidades ligadas aos *campi*, núcleos de pesquisa e centros com funcionalidades específicas.

5 TERMOS E DEFINIÇÕES

5.1 Ativo de informação: qualquer informação que tenha valor para a Instituição [ISO/IEC 13335-1:2004];

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

5.3 Segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidos;

5.4 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 contramedida.

5.5 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 pra a segurança da informação [ISO/IEC TR 18044:2004];

5.6 Incidente de segurança da informação: um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação [ISO/IEC TR 18044:2004];

5.7 Risco: combinação da probabilidade de ocorrência de um evento e de suas consequências;

5.8 Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição [ISO/IEC 13335-1:2004]

5.9 Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

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

5.11 Plano de continuidade de negócios: conjunto de procedimentos que devem ser adotados quando a Instituição se deparar com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços;

5.12 Princípios da Segurança da Informação e Comunicações - são princípios que regem a Segurança da Informação e Comunicações, em acordo com o Artigo 3° do Decreto n° 3.505,

de 13 de junho de 2000, quais sejam: confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio;

5.13 Termo de responsabilidade - acordo de confidencialidade e não divulgação de informações que atribui responsabilidades ao servidor e administrador de serviço quanto ao sigilo e a correta utilização dos ativos de propriedade ou custodiados da Instituição. Prestadores de serviços que, por força de contratos de suporte e manutenção de sistemas, ficam sujeitos às mesmas condições;

5.14 Quebra de segurança - ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação e das Comunicações;

5.15 Tratamento da informação - recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

5.16 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;

5.17 Plano de gerenciamento de incidentes - plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente e que explicite as pessoas, recursos, serviços e outras ações que forem necessárias para implementar o processo de gerenciamento de incidentes;

5.18 Plano de Continuidade - É constituído de um conjunto de medidas, regras e procedimentos definidos, que serão adotados para assegurar que as funções ou atividades críticas da Instituição possam ser mantidas ou recuperadas após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações.

5.19 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.

5.20 Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;

5.21 Avaliação de riscos: processo onde se compara o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;

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

5.23 Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco;

5.24 Tratamento dos riscos: processo e implementação de ações de Segurança da Informação e Comunicações para evitar, reduzir, reter ou transferir um risco;

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

5.26 Usuário interno: qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente ao IFNMG;

5.27 Usuário externo: qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente ao IFNMG;

5.28 Comunicação oficial: tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas do IFNMG, de atividades especiais ou ainda de projetos específicos;

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

6 PRINCÍPIOS

Esta política abrange onze aspectos básicos da Segurança da Informação e Comunicações, destacados a seguir:

6.1 Confidencialidade: somente pessoas devidamente autorizadas pelo gestor da informação devem ter acesso à informação não pública.

6.2 Integridade: somente operações de alteração, supressão e adição autorizadas pelo IFNMG devem ser realizadas nas informações.

6.3 Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado.

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

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

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

6.7 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 IFNMG são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação e Comunicações advindas desta política.

6.8 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.

6.9 Ética - Todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação do IFNMG devem ser respeitados.

6.10 Legalidade - Além de observar os interesses do IFNMG, 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 direitos de uso.

6.11 Proporcionalidade - O nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações no IFNMG serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

7 ESCOPO

O escopo do Plano de Segurança da Informação e Comunicações do IFNMG refere-se:

7.1 aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos demais documentos normativos que as incorporarão;

7.2 aos requisitos de segurança humana;

7.3 aos requisitos de segurança física;

7.4 aos requisitos de segurança lógica;

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

8 ESTRUTURA DA POSIC.

A POSIC do IFNMG é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

8.1 Política de Segurança da Informação e Comunicações (POSIC): constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação e Comunicações e será detalhada em documentos denominados Normas.

8.2 Normas de Segurança da Informação e Comunicações (Normas): estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas instâncias em que a informação é tratada. A cada Norma será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações contidas em um documento do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República intitulado Atividade de Normatização (http://dsic.planalto.gov.br/documentos/nc_1_normatizacao.pdf acessado em 09/07/2013).

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

9 DIRETRIZES GERAIS

9.1 É política do IFNMG prover para a sua comunidade o acesso a fontes de informação locais, nacionais e internacionais, promovendo um ambiente de produção, uso e compartilhamento do conhecimento e de comprometimento com a liberdade acadêmica.

9.2 Zelar pela Segurança da Informação e Comunicações é dever de todos.

9.3 O IFNMG, como usuário dos serviços providos pela Rede Nacional de Pesquisa (RNP) é, por princípio, signatário de suas Políticas e Normas de Segurança.

9.4 Usuários internos e externos devem observar:

9.4.1 que o acesso à informação será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFNMG é considerada seu patrimônio e deve ser protegida.

9.4.2 que os recursos disponibilizados pelo IFNMG, de sua propriedade, são fornecidos com o propósito único de garantir o desempenho das suas atividades.

9.4.3 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.

9.5 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.

9.6 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, produzindo 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.

9.7 Auditoria e Conformidade - Deverá ser levantado regularmente os aspectos legais de segurança aos quais as atividades do IFNMG estão submetidas, de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão.

9.8 Segurança Física - Controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos do IFNMG e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança.

9.9 Uso de e-mail - O serviço de correio eletrônico disponibilizado pelo IFNMG constitui recurso do Instituto disponibilizado na rede de Comunicação de dados para aumentar a agilidade, segurança e economia da Comunicação oficial e informal. O correio eletrônico constitui bem do IFNMG e, portanto, passível de auditoria.

9.10 Capacitação e Aperfeiçoamento – os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicação.

9.11 Acesso a 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 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.

9.12 Patrimônio Intelectual - As informações, os sistemas e os métodos criados pelos servidores do IFNMG, no exercício de suas funções, são patrimônios intelectuais da Instituição, não cabendo a seus criadores qualquer forma de direito autoral.

9.13 Termo de Responsabilidade e Sigilo - É o documento oficial que compromete colaboradores, terceirizados e prestadores de serviço com a POSIC do IFNMG, os quais deverão ser signatários.

10 COMPETÊNCIAS E RESPONSABILIDADES

A implementação, o controle e a gestão da POSIC são de responsabilidade da seguinte infraestrutura de gerenciamento:

10.1 A autoridade máxima é o Reitor, responsável pela aprovação da Política de Segurança da Informação e Comunicação do IFNMG;

10.2 Ao Comitê Gestor da Segurança da Informação e Comunicação compete:

10.2.1 propor, aprovar e implantar políticas, normas e procedimentos gerais relacionados à segurança da informação;

10.2.2 estabelecer diretrizes e oferecer suporte às iniciativas de segurança da informação no IFNMG;

10.2.3 propor iniciativas para a melhoria contínua das medidas de proteção;

10.2.4 apoiar a implantação de soluções para eliminação ou minimização de riscos;

10.2.5 estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança;

10.2.6 desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações;

10.2.7 acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação;

10.2.8 estabelecer normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados e das informações, em vista da possibilidade de detecção de emanações eletromagnéticas, inclusive as provenientes de recursos computacionais;

10.2.9 executar outras funções que, por sua natureza, lhe estejam afetas ou lhe tenham sido atribuídas.

10.2.10 Para fins de regulamentação de suas atividades, o Comitê de Segurança da Informação e Comunicações poderá ter regulamento próprio, o qual deverá ser aprovado pelo Conselho Superior do IFNMG.

10.3 O Comitê Gestor de Tecnologia da Informação e o Comitê de Segurança da Informação e Comunicações será composto por:

I - Diretor de Gestão de Tecnologia da Informação da Reitoria;

II - Coordenador de Gestão de Tecnologia de Informação da Reitoria;

III - Coordenadores de Gestão de Tecnologia da Informação dos *campi* ;

IV - Representantes das Pró-Reitorias, das Diretorias Sistêmicas e do Gabinete.

11 DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

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

11.1 As áreas atingidas por esta POSIC são imediatamente responsáveis pela elaboração e proposição de normas, procedimentos e atividades necessárias ao cumprimento.

11.2 As áreas deverão submeter suas propostas de normas ao "Comitê de Segurança da Informação e Comunicação" para análise, discussão e aprovação no âmbito do Comitê;

11.3 Após aprovação, estas normas e procedimentos serão divulgadas aos interessados pela área responsável por sua proposição e manutenção.

12 REVISÕES E ATUALIZAÇÃO

Esta POSIC será revista e alterada sempre que as atribuições e normas do IFNMG justificar tais alterações, sendo ainda obrigatória a sua revisão anual.

13 VIOLAÇÕES, PENALIDADES E SANÇÕES

Nos casos em que houver o descumprimento ou violação de um ou mais itens da Política ou das suas Normas, procedimentos ou atividades pertinentes à Segurança da Informação e Comunicação, estes serão tratadas conforme legislação e regulamentos internos aplicáveis.

14 VIGÊNCIA

A presente política passa a vigorar a partir da data de sua publicação.