POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IFSUL

1 OBJETIVO

A Política de Segurança da Informação do Instituto Federal Sul-rio-grandense estabelece as diretrizes para a segurança da informação, visando preservar a integridade, a confidencialidade e a disponibilidade dos ativos de informação do IFSul, sendo de responsabilidade de todos os servidores, tanto efetivos como substitutos, temporários, colaboradores, consultores externos, estagiários, bolsistas e prestadores de serviços, o compromisso com o seu cumprimento.

2 FUNDAMENTOS LEGAIS E NORMATIVAS

Referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação do IFSul.

a) Constituição Federal de 1988 reformada em 2008;

b) Lei nº 9.983, de 14 de julho de 2000 - Altera o Decreto Lei nº 2.848/40 – Código Penal - tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

c) Decreto nº 1.171, de 24 de junho de 1994 - Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;

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

e) Lei nº 5.869, de 11 de janeiro de 1973;

f) Lei nº 7.232 de 29 de outubro de 1984 - Política Nacional de Informática, e dá outras providências;

g) 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;

h) 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;

i) 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;

j) Decreto nº 6.029 de 01 de fevereiro de 2007 - Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;

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

l) Decreto nº 7.579 de 11 de outubro de 2011 - Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo Federal, e dá outras providências;

m) 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;

n) 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;

o) Normas e Resoluções do Gabinete de Segurança Institucional da Presidência da República;

I. Instrução Normativa GSI nº 01 de 13 de junho de 2008;

II. Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 outubro de 2008;

III. Norma Complementar nº 03/IN01/DSIC/GSIPR, de 03 julho de 2009;

IV. Norma Complementar nº 04/IN01/DSIC/GSIPR, de 17 agosto de 2009;

V. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 agosto de 2009;

VI. Norma Complementar nº 06/IN01/DSIC/GSIPR , de 23 novembro de 2009.

p) Acórdão nº 1.603/2008 do Plenário do Tribunal de Contas da União – TCU;

q) ABNT NBR ISO 17.799:2005 - Código de Práticas para a Gestão da Segurança da Informação;

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

s) ABNT NBR ISO/IEC 27.001:2005 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gerência da Segurança da Informação – Requisitos;

t) ABNT NBR ISO/IEC 27.002:2005 – Código de Prática para a Gestão de Segurança da Informação;

u) ISO/IEC TR 13.335-3:1998 - fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13.335-1 e TR ISO/IEC 13.335-2;

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

w) Lei nº 12.527 de 18 de novembro de 2011 – Regula o acesso a informações;

x) Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do *caput* do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

3. INSTÂNCIAS ADMINISTRATIVAS

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

a) 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, possuidora de natureza consultiva e deliberativa e responsável pelo alinhamento e regulação das ações de Tecnologia da Informação e Comunicação (TIC) ao disposto no Plano de Desenvolvimento Institucional (PDI);

b) Diretoria de Tecnologia da Informação e Comunicação (DTIC): órgão que planeja, supervisiona, orienta e controla as atividades relacionadas às políticas de Tecnologia da Informação e Comunicação (Art. 74 – Regimento Geral);

c) Coordenadoria de Estratégia de Tecnologia (CESTEC): coordenadoria a qual compete incentivar a pesquisa de soluções tecnológicas em todas as áreas de atuação da Diretoria de Tecnologia da Informação e Comunicação, além de acompanhar a implantação de soluções tecnológicas, em todas as áreas de atuação desta Diretoria, atuando junto aos *campi* para que novas soluções sejam desenvolvidas e propor a padronização para aquisição de equipamentos e contratação de serviços (Art. 76 – Regimento Geral).

4. TERMOS E DEFINIÇÕES

a) Ativo de informação: qualquer informação que tenha valor para a instituição [ISO/IEC 13.335-1:2004];

b) Recursos de Tecnologia da Informação: equipamento de Tecnologia da Informação e seus acessos, bem como também sistemas, serviços e infraestrutura;

c) 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;

d) 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;

e) 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 [ISO/IEC TR 18.044:2004];

f) Incidente de segurança da informação: indicado por um simples evento 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 18.044:2004];

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

h) Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a instituição [ISO/IEC 13.335-1:2004];

i) Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

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

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

l) Termo de responsabilidade: acordo de confidencialidade de não divulgação de informações que atribui responsabilidades ao servidor e administrador de serviço quanto ao sigilo e à correta utilização dos ativos de propriedade ou custodiados da Instituição;

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

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

o) 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;

p) 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;

q) Plano de continuidade: constituído por um conjunto de medidas, regras e procedimentos definidos, 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;

r) 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;

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

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

u) Gestão de riscos de segurança da informação e comunicação: 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;

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

w) Usuário interno: qualquer pessoa física ou unidade interna que faça uso de informações e/ou

serviços, e que esteja vinculada administrativamente ao IFSul;

x) Usuário externo: qualquer pessoa física ou jurídica que faça uso de informações e/ou serviços, e que não esteja vinculada administrativamente ao IFSul;

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

z) 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, bolsista, terceirizados, contratados ou fornecedor de bens e/ou serviços.

5. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

a) Confidencialidade: devem ter acesso à informação não pública somente pessoas devidamente autorizadas pelo gestor da informação;

b) Integridade: devem ser realizadas nas informações somente operações de alteração, supressão e adição autorizadas pelo IFSul;

c) Disponibilidade: deve estar disponível a informação para as pessoas autorizadas sempre que necessário ou solicitado;

d) Autenticidade: assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;

e) Criticidade: define a importância da informação para a continuidade da atividade-fim da Instituição;

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

g) Responsabilidade: devem ser claramente definidas as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança. Todos os servidores do IFSul são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação e Comunicação advindas dessa política;

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

i) Ética: devem ser respeitados todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, bolsistas, prestadores de serviço e usuários do Sistema de Informação do IFSul;

j) Legalidade: levarão em consideração, as ações de Segurança da Informação e Comunicação, além de observar os interesses do IFSul, leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e a direitos de uso;

k) Proporcionalidade: serão adequados ao entendimento administrativo e ao valor do ativo a proteger, o nível, a complexidade e os custos das ações de Segurança da Informação no IFSul.

6. ESCOPO

O escopo do Plano de Segurança da Informação do IFSul refere-se

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

b) aos requisitos de segurança humana;

c) aos requisitos de segurança física;

d) aos requisitos de segurança lógica;

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

7. DIRETRIZES GERAIS

a) O zelo pela Segurança da Informação é dever de todos;

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

c) Os usuários internos e externos devem observar que

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

II. os recursos disponibilizados pelo IFSul, de sua propriedade, são fornecidos com o propósito único de garantir o desempenho das suas atividades;

III. as normas para as operações de armazenamento, divulgação, reprodução, recuperação e destruição da informação serão definidos de acordo com a classificação desta, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor;

d) Um serviço de Gestão de Incidentes será estabelecido, o qual 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;

e) Um processo de Gestão de Riscos será estabelecido, 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;

f) Os aspectos legais de segurança, aos quais as atividades do IFSul estão submetidas, de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão, deverão ser levantados regularmente;

g) A criação de controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos do IFSul 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 serão efetivados;

h) O serviço de correio eletrônico disponibilizado pelo IFSul 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 IFSul e, portanto, passível de auditoria;

i) Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação;

j) O acesso à Internet será concedido para todos os servidores, 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;

k) As informações, os sistemas e os métodos criados pelos servidores do IFSul, no exercício de suas funções, são patrimônios intelectuais da instituição, não cabendo a seus criadores qualquer forma de direito autoral, exceto em casos regulamentados pela área competente;

l) O Termo de Responsabilidade e Sigilo é documento oficial que compromete os servidores, colaboradores, terceirizados e prestadores de serviço com a Política de Segurança da Informação do IFSul.

8. COMPETÊNCIAS E RESPONSABILIDADES

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

a) A autoridade máxima é o reitor, responsável pela aprovação da Política de Segurança da Informação do IFSul;

b) Ao Comitê Gestor da Segurança da Informação compete:

I. promover a cultura de Segurança da Informação;

II. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. propor recursos necessários às ações de Segurança da Informação;

IV. instituir e coordenar a Equipe de Tratamento e Respostas a Incidentes de Segurança da Informação;

V. realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação;

VI. seguir as recomendações do 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;

VII. coordenar as revisões das normas de segurança em vigor;

VIII. propor normas adicionais e procedimentos relativos à Segurança da Informação no âmbito do IFSul.

c) À diretoria de Tecnologia da Informação e Comunicação compete zelar pela segurança da informação no âmbito do IFSul quando estas informações estiverem sob custódia dos recursos de tecnologia da informação;

d) À coordenação ou área de Tecnologia da Informação dos *campi* compete zelar pela segurança da informação, no âmbito do *campus,* quando tais informações estiverem sob custódia dos recursos de tecnologia da informação;

e) É de responsabilidade individual de cada servidor:

I. cumprir e fazer cumprir as regras normas e procedimentos estabelecidos neste documento;

II. zelar pelos equipamentos que utiliza, não sendo permitida qualquer remoção, desconexão de partes, substituição ou qualquer alteração nas características físicas ou técnicas dos equipamentos integrantes da rede;

III. respeitar áreas de acesso restrito, não executando tentativas de acesso a áreas e/ou máquinas alheias as suas permissões de acesso;

IV. evitar atitudes ou ações que possam, direta ou indiretamente, prejudicar o bom funcionamento dos recursos da rede;

V. abster-se de executar programas que tenham como finalidade a decodificação de senhas, monitoração da rede, a leitura de dados de terceiros, a propagação de vírus de computador, o desbloqueio de serviços, a destruição parcial ou total de arquivos ou que venha a prejudicar o bom funcionamento de serviços;

VI. manter seus dados locais atualizados e com cópias de segurança, evitando a perda de informações valiosas;

VII. abster-se de executar programas, instalar equipamentos ou executar ações que possam facilitar o acesso à rede de usuários não autorizados;

VIII. não executar programas de conversação como chats on-line, MSN e outros, sem prévia autorização, exceto quando autorizado pelo chefe imediato para o desenvolvimento das atividades funcionais;

IX. não fazer uso de direitos especiais de acesso ou de qualquer outro privilégio já extintos com o término do período de ocupação de cargo ou função.

9. DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

a) A Política e os Regulamentos de Segurança da Informação devem ser divulgadas a todos os servidores do IFSul, e dispostos de maneira que o seu conteúdo possa ser consultado a qualquer momento;

b) As áreas atingidas por esta Política são imediatamente responsáveis pela classificação da informação, elaboração e proposição de normas, procedimentos e atividades necessárias ao cumprimento;

c) As áreas deverão elaborar os seus regulamentos com base nas diretrizes propostas pelo "Comitê Gestor de Segurança da Informação", submetendo-os para análise, discussão e aprovação no âmbito do Comitê;

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

10. REVISÕES E ATUALIZAÇÃO

Esta Política será revista anualmente e alterada sempre que as atribuições e normas do IFSul justificarem tais alterações.

11. VIOLAÇÕES, PENALIDADES E SANÇÕES

Nos casos em que houver o descumprimento ou violação de um ou mais itens da Política ou de seus regulamentos, procedimentos ou atividades pertinentes à Segurança da Informação, estes serão tratados conforme legislação, podendo também ser revogado o acesso aos ativos de informação.

12. VIGÊNCIA

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