POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Anexo I – Resolução do Conselho Superior nº 10/2014, de 11.04.2014

ORIGEM

Comitê Gestor de Segurança da Informação – CGSI.

REFERÊNCIA LEGAL E NORMATIVA

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

II. 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;

III. 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;

IV. 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, bem como as subsequentes Normas Complementares IN01/DSIC/GSIPR 01, 02, 03, 04, 05, 06, 07 e 08;

V. Aplicação de boas práticas em Tecnologia da Informação recomendadas pela Corte de Contas da União (TCU) e assinaladas na edição dos Acórdãos 1603/2008 - Plenário, 71/2007 – Plenário, 1092/2007-Plenário e 2023/2005 – Plenário;

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

VII. ABNT NBR ISO/IEC 27001:2006 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gerência da Segurança da Informação – Requisitos;

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

CAMPO DE APLICAÇÃO

O disposto neste documento se aplica no âmbito do Ifes.

SUMÁRIO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Anexo I – Resolução do Conselho Superior nº 10/2014, de 11.04.2014

1. Finalidade;
2. Fundamentações Legais e Normativas;
3. Declaração de Comprometimento da Reitoria;
4. Instâncias Administrativas;
5. Termos e Definições;
6. Princípios;
7. Escopo;
8. Estrutura da Política de Segurança da Informação - PSI;
9. Diretrizes Gerais;
10. Divulgação e Acesso à Estrutura Normativa;
11. Revisão e Atualização;
12. Violações, Penalidades e Sanções;
13. Vigência.

INFORMAÇÕES ADICIONAIS

Anexo: Não há.

APROVAÇÃO

Resolução do Conselho Superior nº 10/2014, de 11 de abril de 2014, homologada na 31ª reunião ordinária, ocorrida em 28 de março de 2014.

Anexo I – Resolução do Conselho Superior nº 10/2014, de 11.04.2014

1 FINALIDADE

A Política de Segurança da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo - Ifes é uma declaração formal 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, alunos, estagiários, bolsistas e prestadores de serviço que exerçam atividades no âmbito do Ifes ou quem quer que tenha acesso a dados ou informações no ambiente do Ifes. O seu propósito é estabelecer diretrizes, normas, procedimentos e responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes ao Ifes.

2 FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

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

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

2.2 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;

2.3 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;

2.4 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, bem como as subsequentes Normas complementares IN01/DSIC/GSIPR 01, 02, 03, 04, 05, 06, 07 e 08;

2.5 Aplicação de boas práticas em Tecnologia da Informação recomendadas pela Corte de Contas da União (TCU) e assinaladas na edição dos Acórdãos 1603/2008 - Plenário, 71/2007 – Plenário, 1092/2007- Plenário e 2023/2005 – Plenário;

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

2.7 ABNT NBR ISO/IEC 27001:2006 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gerência da Segurança da Informação – Requisitos;

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

3 DECLARAÇÃO DE COMPROMETIMENTO

A alta direção do Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo, na pessoa do Reitor, declara estar de acordo e comprometida com o cumprimento da Política de Segurança da Informação.

4 INSTÂNCIAS ADMINISTRATIVAS

4.1 Diretoria de Tecnologia da Informação (DTI): instância administrativa/executiva responsável por propor as políticas e programas do Ifes na área de Tecnologia da Informação (T.I) e telecomunicações, bem como por sua implementação e gestão.

4.2 Coordenação de Tecnologia da Informação (CTI): instância que tem como atribuição principal o gerenciamento da rede local, bem como dos recursos de T.I e telecomunicações do campus.

4.3 Unidade: qualquer instância administrativa do Ifes, a exemplo dos *campi*, unidades ligadas aos *campi*, núcleos de pesquisa, setores administrativos e acadêmicos e centros com funcionalidades específicas.

4.4 Comitê Gestor de Tecnologia da Informação (CGTI): instância criada pela resolução nº 67/2011 do Conselho Superior do Ifes, responsável por alinhar os investimentos de Tecnologia da Informação com os objetivos estratégicos institucionais e definir a prioridade dos projetos de Tecnologia da Informação.

4.5 Comitê Gestor de Segurança da Informação (CGSI): instância que têm como principal função verificar junto às unidades a consecução das diretrizes da Política de Segurança da Informação no Ifes, bem como a avaliação e análise de assuntos relativos aos objetivos estabelecidos nesta PSI.

4.6 Centro de Tratamento e Resposta a Incidentes de Segurança da Informação (CTRI): tem como finalidade o atendimento aos incidentes de segurança da informação no âmbito do Ifes.

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 envolvidas;

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 contra medida;

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 para 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 suas consequências [ABNT ISO/IEC GUIA 73:2005];

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 [ABNT NBR ISO/IEC 17799:2005];

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 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, por força de contratos de suporte e manutenção de sistemas, ficam sujeitos às mesmas condições;

5.13 Quebra de segurança: ação ou omissão, intencional ou acidental, que resulte no comprometimento da Segurança da Informação;

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

5.15 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;

5.16 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;

5.17 Gestão de Riscos de Segurança da Informação: 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;

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

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

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

5.21 Comunicação oficial: tráfego de documentos e/ou informações institucionais por meio físico e/ou digital, autorizado pela instituição;

5.22 Comunicação informal: tráfego de documentos e/ou informações que não estejam incluídos no conceito de comunicação oficial.

6 PRINCÍPIOS

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 Ifes 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: consiste na garantia da veracidade da fonte das informações.

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

6.6 Legalidade: Além de observar os interesses do Ifes, as ações de Segurança da Informação deverão considerar 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.

6.7 Auditabilidade: o acesso e o uso da informação, por meio de recursos e/ou ativos, devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.

7 ESCOPO

O escopo da Política de Segurança da Informação do Ifes refere-se:

7.1 aos aspectos estratégicos, estruturais e organizacionais;

7.2 aos requisitos de segurança humana;

7.3 aos requisitos de segurança física;

7.4 aos requisitos de segurança lógica.

8 ESTRUTURA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

A Segurança da Informação do Ifes é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

8.1 Política de Segurança da Informação: constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação, sendo detalhada em documentos denominados Norma.

8.2 Norma de Segurança da Informação: estabelece responsabilidades e define os procedimentos de acordo com as diretrizes da Política, a serem seguidos nas diversas instâncias em que a informação é tratada. A cada Norma será associado um conjunto de procedimentos destinados a orientar sua implementação.

8.3 Procedimentos de Segurança da Informação: instrumentalizam o disposto nas Normas, permitindo sua direta aplicação nas atividades do Ifes, cabendo a cada gestor a responsabilidade de implementá-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 Ifes 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 Esta política se aplica, no que couber, às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exerçam atividades no âmbito desta Instituição de Ensino ou quem quer que venha a ter acesso a dados ou informações protegidos por este regulamento.

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

9.4 O usuário é responsável por cumprir e fazer cumprir a aplicação eficaz das normas, procedimentos e princípios da Segurança da Informação, no compromisso com os critérios legais e éticos que envolvem o Ifes.

9.5 Deverão ser previstas, nos contratos de prestação de serviços de terceiros, cláusulas que contemplem as responsabilidades no cumprimento da Política de Segurança da Informação do Ifes, bem como suas normas e procedimentos.

9.6 Todo incidente que afetar a segurança da informação deverá ser reportado ao Comitê de Segurança da Informação, que é responsável para tratar do assunto.

9.7 Será estabelecido um processo de Gestão de Riscos contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação, produzindo subsídios para a Gestão de Continuidade dos Negócios.

9.8 Deverão ser levantados regularmente os aspectos legais de segurança aos quais as atividades do Ifes estão submetidas, de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão.

9.9 Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação.

9.10 O Termo de Responsabilidade e Sigilo é o documento oficial que compromete colaboradores, terceirizados e prestadores de serviço com a PSI do Ifes, os quais deverão ser signatários.

10 DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

10.1 A Política e as Normas de Segurança da Informação devem ser divulgadas e publicadas a todos os usuários do Ifes de modo que todos tenham ciência seu conteúdo e que possam ser consultadas a qualquer momento.

Anexo I – Resolução do Conselho Superior nº 10/2014, de 11.04.2014

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

10.3 As áreas deverão submeter suas propostas de normas ao Comitê de Gestão de Segurança da Informação para análise, discussão e aprovação no âmbito do Comitê.

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

11 **REVISÕES E ATUALIZAÇÃO**

Esta PSI será revista e alterada sempre que as atribuições e normas do Ifes justificarem tais alterações, sendo ainda obrigatória a sua revisão anual.

12 **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, estes serão tratados conforme legislação e regulamentos internos aplicáveis.

13 **VIGÊNCIA**

A presente política passa a vigorar a partir de sua homologação pelo Conselho Superior do Ifes.