SERVIÇO PÚBLICO FEDERAL
MEC-SETEC
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO
CONSELHO SUPERIOR

RESOLUÇÃO Nº 028, DE 30 DE ABRIL DE 2012

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO, no uso de suas atribuições legais conferidas pela Portaria Ministerial nº 37 de 07/01/2009, publicada no DOU de 08/01/2009 e Lei nº 11.892, de 29/12/2008,

RESOLVE:

Art. 1º – Aprovar, *ad referendum*, a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – POSIC** do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso, conforme anexo.

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

Cuiabá-MT, 30 de abril de 2012.

PROF. JOSÉ BISPO BARBOSA
PRESIDENTE DO CONSUP/IFMT

SERVIÇO PÚBLICO FEDERAL
MEC – SETEC
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - POSIC

1. INTRODUÇÃO

De acordo com as Normas NBR ISO/IEC 27001 e 27002, organização deve implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) documentado dentro do contexto das atividades de negócio globais da instituição e os riscos que ela enfrenta.

A Política de Segurança da Informação e Comunicações (POSIC) é um documento que compõe um SGSI. Este documento estabelece uma diretriz global e princípios para ações relacionadas com a Segurança da Informação.

O Instituto Federal de Educação Ciência e Tecnologia de Mato Grosso – IFMT é uma Instituição de educação superior, básica e profissional, pluricurricular e multicampi, especializada na oferta de educação profissional e tecnológica nas diferentes modalidades de ensino, com base na conjugação de conhecimentos técnicos e tecnológicos com sua pratica pedagógica.

2. FINALIDADE

A Política de Segurança da Informação e Comunicações do Instituto Federal de Mato Grosso 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 clientes internos e externos definidos como:

a) Servidores;
b) Alunos;
c) Colaboradores;
d) Estagiários;

e) Prestadores de serviço que exerçam atividades no âmbito da Instituição ou;
f) Qualquer cidadão que tenha acesso a dados ou informações no âmbito do Instituto.

O seu propósito é estabelecer diretrizes gerais que servirão como base para às normas, procedimentos e instruções referentes à segurança da informação, atribuindo responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes a Instituição.

3. CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

Comitê de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da Instituição.

Equipe de Tratamento e Resposta de Incidentes: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança.

Gestor de Segurança da Informação e Comunicações: é responsável pelas ações de segurança da informação e comunicações no âmbito da Instituição.

Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pela autoridade responsável da Instituição, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.

Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

4. DECLARAÇÃO DE COMPROMETIMENTO DA REITORIA E CAMPI

A Reitoria e os Campi do IFMT declaram-se comprometidos em proteger todos os ativos de informação da Instituição, na sua implementação, operação, monitoramento, análise critica, manutenção e melhoria da POSIC mediante:

a) Estabelecimento da POSIC;
b) Garantir os planos e objetivos da POSIC;
c) Estabelecimento de papeis e responsabilidades pela POSIC;
d) Divulgação, conscientização e treinamento para atender os objetivos da POSIC no âmbito geral do Instituto;
e) Definir critérios para a aceitação de riscos e níveis de riscos aceitáveis;
f) Garantir que auditorias internas sejam realizadas a fim de verificar a aplicação da POSIC em todo o Instituto;

5. PRINCIPIOS

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

a) Confidencialidade: somente pessoas devidamente autorizadas pela Instituição devem ter acesso à informação.
b) Integridade: a informação não deve ser alterada sem autorização da Instituição.
c) Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado.
d) Autenticidade: princípio de segurança que atesta com exatidão a origem da informação e a responsabilidade pela criação ou divulgação da mesma.
e) Criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição.
f) Não-Repúdio: garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação.
g) Responsabilidade - As responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todos os clientes internos e externos da Instituição são responsáveis pelo tratamento da informação e pelo cumprimento das normas de Segurança da Informação e Comunicações.

h) Conhecimento - Todos os clientes internos e externos da Instituição devem ter ciência de normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança da informação.
i) Ética - Todos os direitos e interesses legítimos dos clientes internos e externos da Instituição devem ser respeitados.
j) Legalidade - Além de observar os interesses da Instituição, as ações desta POSIC 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.
k) Proporcionalidade - O nível, a complexidade e os custos das ações da POSIC na Instituição serão adequados ao valor da informação a ser protegida e/ou a aceitação do nível de risco.

6. ESCOPO

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

a) Aos aspectos estratégicos, estruturais e institucionais, 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 influenciarão diretamente nos serviços oriundos da Informação e Comunicações da Instituição.

7. ESTRUTURA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

A estrutura da Segurança da Informação e Comunicações da Instituição é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

a) **Política de Segurança da Informação e Comunicações:** constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação e Comunicações;

b) **Normas de Segurança da Informação e Comunicações:** estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada em forma de Instruções Normativas;

c) **Procedimentos de Segurança da Informação e Comunicações:** instrumentalizam o disposto nas Instruções Normativas e na Política, permitindo a direta aplicação nas atividades da Instituição.

8. DIRETRIZES GERAIS

Clientes internos e externos da Instituição devem observar que:

a) Acesso, Proteção e Guarda da Informação - O acesso à informação deve ser regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Instituição é considerada seu patrimônio e deve ser protegida seja ela em meio físico ou meio digital.

b) Utilização dos Recursos de Informação - Os recursos disponibilizados são fornecidos com o propósito único de garantir o desempenho das atividades da Instituição.

c) Classificação das informações – Para que o nível adequado de proteção para a informação seja estabelecido, é necessário que todas as informações, existentes e futuras, sejam devidamente classificadas.

d) Deverão ser estabelecidas normas para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação que serão definidos de acordo com a classificação desta, sem prejuízo de outros cuidados que serão especificados pelo IFMT.

e) Gestão de Incidências - É estabelecida uma área 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.

f) Gestão de Risco – É estabelecido um processo de Gestão de Risco, contínuo e aplicado na implementação e operação da SGSI, 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.

g) Plano de Continuidade - É estabelecido um processo 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.

h) Auditoria e Conformidade - Deverão ser levantados regularmente os aspectos legais de segurança aos quais as atividades da Instituição estão submetidas, de forma a evitar responsabilizações decorrentes da não observância de tais aspectos por desconhecimento ou omissão.

i) Segurança Física - Controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos da Instituição. 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.

j) Uso de e-mail - O serviço de correio eletrônico disponibilizado pela Instituição constitui-se de recurso de envio de mensagens disponibilizado na rede de comunicação de dados para aumentar a agilidade, segurança e economia da comunicação interna e externa da Instituição. O correio eletrônico deve ser utilizado exclusivamente no interesse do serviço, passível de auditoria.

k) Uso de software – É proibido à utilização de software sem a autorização dos autores ou sem licença de uso quando necessário. É proibido uso de software para práticas ilícitas conforme legislação vigente.

l) Acesso a Internet - Todos os servidores têm o direito de acesso à internet, com utilização exclusiva para fins complementares às atividades da Instituição, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos. É proibido o uso de internet para práticas ilícitas.

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

n) Patrimônio Intelectual - As informações, os sistemas e os métodos criados pelos servidores da Instituição, no exercício de suas funções, são patrimônios intelectuais da Instituição, não cabendo a seus criadores qualquer forma de direito autoral, ressalvado o disposto na lei 10.973/ 2004.

o) Termo de Responsabilidade e Sigilo - É o documento oficial que compromete colaboradores, terceirizados e prestadores de serviço com a política de segurança da Instituição.

9. COMPETÊNCIAS E RESPONSABILIDADES

A implementação, o controle e a gestão da política de Segurança da Informação e Comunicações são de responsabilidade da seguinte infraestrutura de gerenciamento:

a) CONSUP, responsável pela aprovação da Política de Segurança da Informação e Comunicações.

b) Ao Reitor, gestor responsável pelo Instituto Federal compete:

   I. Coordenar as ações de segurança da informação e comunicações;

   II. Aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;

III. Propor programa orçamentário específico para as ações de segurança da informação e comunicações;
IV. Nomear Gestor de Segurança da Informação e Comunicações;
V. Instituir e implementar equipe de tratamento e resposta a incidentes em Segurança da Informação na Instituição.;
VI. Instituir Comitê de Segurança da Informação e Comunicações;
VII. Aprovar normas de segurança da informação e comunicações;

c) Gestor de Segurança da Informação, conforme Instrução Normativa GSI/PR n° 1, responsável por:

I. Promover cultura de Segurança da Informação e Comunicações;
II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III. Propor recursos necessários às ações de Segurança da Informação e Comunicações;
IV. Coordenar o Comitê de Segurança e a Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação;
V. Instituir a Equipe de Gestão de Riscos em Segurança da Informação na Instituição.
VI. Coordenar a Equipe de Gestão de Riscos em Segurança da Informação;
VII. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação e Comunicações;
VIII. Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à Segurança da Informação e Comunicações;
IX. Propor e avaliar Normas adicionais e procedimentos relativos à segurança da informação e comunicações no âmbito da Instituição.
X. Coordenar a Equipe de Tratamento e Respostas a Incidentes em Segurança da Informação.
XI. Propor e implantar Plano de Continuidade de Negócio.

d) Comitê de Segurança da Informação e Comunicações - CSI, conforme Portaria n° 1.100 de 18 de agosto de 2011, responsável por:
    I. Assessorar o Gestor de Segurança da Informação e o IFMT na consecução das Diretrizes da POSIC, bem como na avaliação e análise de assuntos relativos à Segurança da Informação.
    II. Elaborar, propor e manter a POSIC para o IFMT, a ser submetida ao Gestor de Segurança da Informação para análise.
e) Cada Pró-Reitoria, Diretoria Sistêmica e Diretoria Geral dos Campi são responsáveis por:
    I. Criar Instruções Normativas e Procedimentos de suas áreas de acordo com esta POSIC, submetendo-os a um parecer do Gestor de Segurança da Informação.
    II. Promover cultura de Segurança da Informação e Comunicações.
    III. Apresentar sugestões de melhorias ou denúncias de quebra de segurança que deverão ser averiguadas pela Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação.

10. DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política, as Normas e Procedimentos de Segurança da Informação e Comunicações devem ser divulgados a todos os colaboradores da Instituição e dispostas de maneira que o seu conteúdo possa ser consultado a qualquer momento.

a) As áreas atingidas por esta política são imediatamente responsáveis pela elaboração e proposição de normas, procedimentos e atividades necessárias ao cumprimento desta política bem como sua manutenção.
b) As áreas deverão submeter suas propostas de normas ao Gestor de Segurança para análise, discussão e aprovação no âmbito do Instituto;
c) Após aprovação, estas normas e procedimentos serão divulgados aos interessados para sua aplicação.

11. REVISÕES E ATUALIZAÇÃO

Esta POSIC será revisada e alterada sempre que as atribuições e normas da Instituição justificar as alterações, sendo ainda obrigatória a revisão anual.

12. VIOLAÇÕES, PENALIDADES E SANÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES.

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

13. REFERÊNCIAS LEGAIS E NORMATIVAS

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

- ABNT NBR ISO/IEC 27001: 2006 – Sistema de Gestão da Segurança da Informação - Requisitos. Esta Norma especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização.
- ABNT NBR ISO/IEC 27002: 2005 – Código de Prática para Gestão de Segurança da Informação. Esta Norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.
- ABNT NBR ISO/IEC 27005:2011 - Gestão de riscos de segurança da informação. Esta Norma fornece diretrizes para o processo de gestão de riscos de segurança da informação.
- Constituição Federal de 1988.
- 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.

- 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.
- Decreto 1.171, de 24 de junho de 1994 - Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências.
- 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.
- 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.
- Normas e Resoluções do Gabinete de Segurança Institucional da Presidência da Republica.
  - Instrução Normativa GSI/PR Nº 01 de 13 de Junho de 2008.
  - Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 Out 2008.
  - Norma Complementar nº 03/IN01/DSIC/GSIPR, de 03 Jul 2009.
  - Norma Complementar nº 04/IN01/DSIC/GSIPR, de 17 Ago 2009.
  - Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 Ago 2009.
  - Norma Complementar nº 06/IN01/DSIC/GSIPR, de 23 Nov 2009.
  - Norma Complementar nº 07/IN01/DSIC/GSIPR, de 07 Mai 2010.
  - Norma Complementar nº 08/IN01/DSIC/GSIPR, de 24 Ago 2010.
  - Norma Complementar nº 09/IN01/DSIC/GSIPR, de 22 Nov 2010.
  - Norma Complementar nº 10/IN01/DSIC/GSIPR, de 10 Fev 2012.
  - Norma Complementar nº 11/IN01/DSIC/GSIPR, de 10 Fev 2012.
  - Norma Complementar nº 12/IN01/DSIC/GSIPR, de 10 Fev 2012.
  - Norma Complementar nº 13/IN01/DSIC/GSIPR, de 10 Fev 2012.
  - Norma Complementar nº 14/IN01/DSIC/GSIPR, de 10 Fev 2012.
- Instrução Normativa SLTI/MPOG Nº 4 de 12 de novembro de 2010.
- Acórdão 1603/2008 do Plenário do Tribunal de Contas da União – Tribunal de Contas da União.

- Lei nº 11.892 de 29 de dezembro de 2008 – Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências.
- Resolução nº 1 do Conselho Superior/IFMT de 01 de setembro de 2009 - Aprova, ad referendum, o Estatuto do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso - IFMT.
- Plano de Desenvolvimento Institucional do Instituto Federal de Mato Grosso de 26 de junho de 2009.

14. VIGÊNCIA E VALIDADE

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

_____

José Bispo Barbosa

Presidente do CONSUP