MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

RESOLUÇÃO Nº 046, DE 01 DE SETEMBRO DE 2015.

Dispõe sobre a Política de Segurança da Informação e Comunicação – PoSIC do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão.

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO, no uso de suas atribuições consagradas na Lei nº 11.892/2008, com base no Decreto Presidencial de 15 de agosto de 2012, publicado no D.O.U. de 16 de agosto de 2012; e,

considerando a decisão do plenário deste Conselho Superior na 26ª Reunião Ordinária de 31 de agosto de 2015;

considerando ainda, o que consta no processo nº 23249.026596.2013-93;

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicação – PoSIC do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão, conforme anexo.

Art. 2º Esta resolução entra em vigor na data de sua assinatura.

Francisco Roberto Brandão Ferreira
Presidente

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

ANEXO À RESOLUÇÃO Nº 046, DE 01 DE SETEMBRO DE 2015.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO – PoSIC DO IFMA

1 FINALIDADE

A Política de Segurança da Informação e Comunicações do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO - IFMA - 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 IFMA ou quem quer que tenha acesso a dados ou informações no ambiente do IFMA. O seu propósito é estabelecer diretrizes, normas, procedimentos, e responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes ao IFMA.

2 FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFMA 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 infra legais aplicáveis, a saber:

- Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;
- Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;
- Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;
- Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010;
- Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 12/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 14/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 15/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 16/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 17/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 18/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 19/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 20 /IN01/DSIC/GSI/PR, de 15 de dezembro de 2014;
- Norma Complementar nº 21 /IN01/DSIC/GSI/PR, de 10 de outubro de 2014;
- Acórdão nº 1603/2008 – Plenário do Tribunal de Contas da União (TCU);
- Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;
- Norma ABNT NBR ISO Guia nº 73:2002: Gestão de Riscos / Vocabulário;
- Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;
- Norma ABNT NBR ISO/IEC nº 27002:2005: Código de Prática para a Gestão de Segurança da Informação;

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

Conforme disposto no seu Regimento Interno, compete ao CSIC do IFMA determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFMA.

3 DECLARAÇÃO DE COMPROMETIMENTO DA REITORIA

A alta direção do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO, 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 e Comunicação (CGTIC):** 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 IFMA na área de informática e telecomunicações, bem como por sua implementação e gestão;

4.3 **Núcleo de Sistemas:** instância responsável pelo desenvolvimento, implantação e manutenção dos sistemas no âmbito do IFMA;

4.4 **Núcleo de Redes:** instância responsável pela infraestrutura de redes, desenvolvimento e manutenção de dados e informações no âmbito do IFMA;

4.5 **Núcleo de Governança de TI:** instância responsável pela gestão do cumprimento de normativos legais e requisições de serviços;

4.6 **Núcleo 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.

4.7 **Unidade:** qualquer instância administrativa do IFMA 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 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 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 IFMA;

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

5.28 **Comunicação oficial:** tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas do IFMA, 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 IFMA 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 IFMA 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 IFMA devem ser respeitados.

6.10 **Legalidade:** além de observar os interesses do IFMA, 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 IFMA 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 IFMA 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 IFMA.

8 ESTRUTURA DA POSIC

A POSIC do IFMA 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 02/05/2012).

8.3 **Procedimentos de Segurança da Informação e Comunicações (Procedimentos):** instrumentalizam o disposto nas Normas, permitindo a direta aplicação nas atividades do IFMA, 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.

8.4 **Gestão de Software Proprietário –** Norma que estabelece critérios gerais para o uso de software proprietário dentro do IFMA.

8.5 **Uso do Correio eletrônico Constitucional –** Estabelece critérios para uso do correio eletrônico institucional.

8.6 **Gestão de dados corporativos** - Estabelece critérios para gestão dos dados corporativos.

8.7 **Gestão de Senhas** - Estabelece critérios para geração e manutenção de senhas de usuários.

8.8 **Hospedagens e Publicações na Internet** – Estabelece critérios para hospedagem de páginas e publicações na internet.

9 DIRETRIZES GERAIS

9.1 É política do IFMA 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 IFMA, 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 IFMA é considerada seu patrimônio e deve ser protegida.

9.4.2 que os recursos disponibilizados pelo IFMA, 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 IFMA 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 IFMA 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 IFMA 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 IFMA 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 IFMA, 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 IFMA, 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 O Conselho Superior – CONSUP do IFMA é o responsável pela aprovação da Política de Segurança da Informação e Comunicação do IFMA;

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

10.2.1 promover a cultura de Segurança da Informação e Comunicação;

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

10.2.3 propor recursos necessários às ações de Segurança da Informação e Comunicação;

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

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

10.2.6 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;

10.2.7 coordenar as revisões das normas de segurança em vigor;

10.2.8 propor normas adicionais e procedimentos relativos à Segurança da informação e Comunicação no âmbito do IFMA.

10.3 Compete à Diretoria de Gestão de Tecnologia da Informação zelar pela segurança da informação e Comunicação no âmbito do IFMA quando estas informações estiverem sob custódia dos recursos de tecnologia da informação;

10.4 Compete aos Núcleos de Tecnologia da Informação dos *campi* zelar pela segurança da informação e Comunicação no âmbito do campus quando estas informações estiverem sob custódia dos recursos de tecnologia da informação;

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 IFMA, 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 IFMA 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 assinatura.

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

Número da Norma	Revisão	Emissão	Folha
01/IN01/CSIC/IFMA		01/09/2015	1/8

ESTRUTURA DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ORIGEM

Esta é uma norma complementar à Política de Segurança de Informação e Comunicações (POSIC) e foi elaborada pelo Comitê Gestor de Segurança da Informação e Comunicações (CSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão (IFMA) instituído pela Portaria número 5851 de 05 de dezembro de 2012.

REFERÊNCIA NORMATIVA

Conforme disposto no Regimento do Comitê Gestor de Segurança da Informação e Comunicações do IFMA, compete ao CSIC orientar acerca da estrutura a ser seguida na elaboração de normas de segurança da informação de comunicações.

CAMPO DE APLICAÇÃO

Esta norma aplica-se a todo o IFMA.

OBJETIVOS GERAIS

Com o objetivo de criar um padrão para apresentação de normas de segurança da informação e comunicações o CSIC apresenta a estrutura básica de uma norma e que deverá ser seguida por todos os responsáveis pela preservação das informações e recursos de comunicação no âmbito do IFMA.

SUMÁRIO

ESTRUTURA DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

INFORMAÇÕES ADICIONAIS

Esta norma observa a estrutura proposta pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança da Informação da Presidência da República disponibilizada em seu sítio - http://dsic.planalto.gov.br/documentos/nc_1_normatizacao.pdf (acessado em 25/04/2013).

1 OBJETIVO

Estabelecer critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas sobre Gestão de Segurança da Informação e Comunicações no âmbito do IFMA.

2 FUNDAMENTAÇÃO LEGAL E NORMATIVA

Conforme disposto no Regimento do CSIC do IFMA compete a ele estabelecer estes critérios para normas de segurança da informação.

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFMA 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 infra legais aplicáveis, a saber:

- Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;
- Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;
- Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;
- Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010;
- Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 12/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 14/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 15/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 16/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 17/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 18/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 19/IN01/DSIC/GSI/PR, de 16 de julho de 2014;

- Norma Complementar nº 20 /IN01/DSIC/GSI/PR, de 15 de dezembro de 2014;
- Norma Complementar nº 21 /IN01/DSIC/GSI/PR, de 10 de outubro de 2014;
- Acórdão nº 1603/2008 – Plenário do Tribunal de Contas da União (TCU);
- Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;
- Norma ABNT NBR ISO Guia nº 73:2002: Gestão de Riscos / Vocabulário;
- Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;
- Norma ABNT NBR ISO/IEC nº 27002:2005: Código de Prática para a Gestão de Segurança da Informação;
- 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
- Norma ISO/IEC GUIDE nº 51:1999, que fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

Conforme disposto no seu Regimento Interno, compete ao CSIC do IFMA determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFMA.

3 ELABORAÇÃO DAS NORMAS

Cabe a toda a comunidade envolvida com a geração, uso e tratamento da informação propor normas de segurança da informação e comunicações. Estas normas deverão ser apresentadas ao CSIC que é a instância competente para aprová-las e publicá-las.

4 APRESENTAÇÃO DAS NORMAS

4.1 Folha(s) de rosto

Toda norma será apresentada por uma folha de rosto, aos moldes desta própria norma, que deverá conter informações que a contextualizem e que será composta pelos seguintes itens:

4.1.1 Logotipo do IFMA;

4.1.2 Caixa de identificação da norma contendo: número da norma formado pelo número geral da norma atribuído pelo CSIC, pelo número da norma dentro do

conjunto de normas propostas pela entidade administrativa (departamento, diretoria, coordenação etc.) seguido de sua hierarquia organizacional, a exemplo desta norma onde 01/IN01/CSIC/IFMA significa a instrução normativa número 01 proposta pelo Comitê Gestor da Segurança da Informação e Comunicações do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão – IFMA. O número da revisão da norma e a data de sua aprovação. A data da primeira versão da norma e a numeração das folhas no formato "página/total de páginas";

4.1.3 Normas numeradas com "00" no primeiro campo referem-se a normas de interesse exclusivo da entidade administrativa. Estas normas deverão ser submetidas ao CSIC e sua divulgação no âmbito do IFMA não é obrigatória;

4.1.4 Título da Norma: expressão identificadora do conteúdo da norma, de forma concisa, precisa e inequívoca; digitado com a fonte "Times New Roman" tamanho 12 em negrito;

4.1.5 Origem: responsável pela atividade normativa;

4.1.6 Referência Normativa: documentos normativos e respectivas datas de aprovação, se houver;

4.1.7 Campo de Aplicação: unidades onde se aplica a norma e/ou áreas envolvidas com a execução e com o acompanhamento do assunto nela tratado;

4.1.8 Objetivos gerais: texto sucinto descrevendo o objetivo da norma;

4.1.9 Sumário: lista dos itens constantes da norma, que permite uma visão global e facilita a sua consulta;

4.1.10 Informações adicionais: contém esclarecimentos sobre a edição ou revisão da norma, especialmente quanto a substituições e cancelamentos de normas anteriores;

4.1.11 Aprovação: assinatura da norma pelo Presidente do CSIC;

4.1.12 As folhas subsequentes obedecerão ao layout de cabeçalho da folha de rosto.

4.2 Conteúdo da norma:

4.2.1 As normas devem conter uma estrutura básica compostas dos seguintes itens:

4.2.1.1 Objetivo: definir detalhadamente o escopo da norma e os aspectos por ela abrangidos;

4.2.1.2 Procedimentos: passos estabelecidos, em sequência lógica, correspondentes ao assunto tratado, abrangendo todas as tarefas envolvidas no processo;

4.2.1.3 Disposições Gerais: informações adicionais julgadas necessárias, especialmente com relação a esclarecimento de eventuais dúvidas e casos omissos;

4.2.1.4 Vigência: data em que a norma entra em vigor; e

4.2.1.5 Anexos: formulários, fluxogramas e dados adicionais, necessários à execução das atividades constantes da norma ou que facilitem a sua compreensão ou uso;

4.2.2 Os procedimentos podem estar divididos em vários itens, observadas as orientações constantes do item 4.3.3 desta Norma;

4.2.3 Sempre que uma sigla é citada pela primeira vez em uma norma, ela deve ser colocada entre parênteses, logo após o nome por extenso. O uso da sigla só se justifica quando é usado repetidamente na norma;

4.2.4 Serão grafadas por extenso quaisquer referências, feitas no texto, a números e percentuais (trinta, dez, treze, dois vírgula quinze por cento, etc.), exceto nos casos em que houver prejuízo para compreensão do texto;

4.2.5 Valores monetários devem ser expressos em algarismos arábicos, seguidos da indicação, por extenso, entre parênteses;

4.2.6 A redação deve ter estilo próprio, linguisticamente correta, sem preocupações literárias e, tanto quanto possível, uniforme. A qualidade essencial é a clareza do texto, que deve ser facilmente compreensível por pessoas que não tenham participado na elaboração da norma;

4.2.7 Para maior clareza e objetividade deve-se:

4.2.7.1 construir as frases em ordem direta (sujeito, verbo, complementos);

4.2.7.2 utilizar frases curtas, para facilitar o entendimento e evitar duplo sentido;

4.2.7.3 usar, preferencialmente, o substantivo em lugar do pronome, mesmo com o prejuízo da elegância da frase;

4.2.7.4 utilizar termos técnicos já definidos em terminologia existente;

4.2.7.5 usar, preferencialmente, o presente do indicativo, salvo quando a

regência gramatical exigir o uso de outros tempos ou modos;

4.2.7.6 utilizar o verbo no infinitivo nas descrições de etapas (exemplos: elaborar, emitir, aprovar); e

4.2.7.7 evitar detalhes excessivos e desnecessários que inibam a criatividade.

4.2.8 As aspas devem ser utilizadas para:

4.2.8.1 dar ênfase a um determinado termo;

4.2.8.2 indicar termo de língua estrangeira; e

4.2.8.3 indicar expressões de linguagem, comumente usadas no meio da especialidade, as quais, todavia, ainda não foram incorporadas ao vernáculo.

4.3 Estrutura do texto.

4.3.1 As linhas deverão obedecer ao espaçamento simples com 2 mm (dois milímetros) de espaçamento acima e após o parágrafo;

4.3.2 O texto pode ser subdividido em itens e subitens;

4.3.3 Os títulos dos itens devem ser escritos em letras maiúsculas e em negrito, a fim de facilitar a sua identificação e localização. A escolha dos títulos dos itens deve ser feita de maneira criteriosa, de forma a permitir reconhecer a sequência lógica de estruturação da norma. Para facilitar essa estruturação, deve-se definir a lista de todos os aspectos a serem incluídos, antes do início de sua redação;

4.3.4 A matéria do item deve ser apresentada em um único parágrafo, podendo, entretanto, existir uma ou mais frases. Caso o assunto seja extenso, o item deve ser dividido em dois ou mais subitens;

4.3.5 A numeração dos itens deve ser separada por pontos e obedecer ao posicionamento hierárquico de modo que a numeração do subitem fique alinhada com o texto do item logo acima. Entre o último número e a primeira letra do texto deve-se obedecer um distanciamento suficiente para não comprometer a legibilidade da numeração;

4.3.6 Sempre que o título de um item ocupar mais de uma linha, a segunda e as demais linhas devem ser alinhadas com a primeira letra do título;

4.3.7 Em algumas situações os subitens podem ter títulos. Nestes casos, todas as

palavras são escritas com apenas a primeira letra em maiúsculo;

4.3.8 O texto deve ser digitado em editor de texto, utilizando a fonte "Times New Roman", tamanho 12;

4.3.9 Esta Norma obedece ao padrão proposto por ela.

5 ATUALIZAÇÃO DAS NORMAS

5.1 Uma norma pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:

5.1.1 alteração dos procedimentos vigentes ou adoção de novos;

5.1.2 estabelecimento de novos dispositivos legais ou regulamentares, bem como reformulação dos existentes;

5.1.3 acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento; ou encerramento de atividades.

5.2 Os procedimentos para aprovação e divulgação das normas alteradas seguem a mesma tramitação de uma norma nova.

6 DISPOSIÇÕES GERAIS

6.1 A formatação desta Norma deve ser utilizada como modelo para a criação das demais;

6.2 Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Presidente do CSIC que, se considerar necessário fará convocação de reunião do Comitê.

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

Número da Norma	Revisão - Data	Emissão	Folha
02/IN02/CSIC/IFMA		01/09/2015	1/7

NORMA GERAL DE SEGURANÇA E USO DE RECURSOS COMPUTACIONAIS E DE REDE – INTERNET

ORIGEM

Esta é uma norma complementar à Política de Segurança de Informação e Comunicações (POSIC) e foi elaborada pelo Comitê Gestor de Segurança da Informação e Comunicações (CSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão (IFMA) instituído pela Portaria número 5851 de 05 de dezembro de 2012.

REFERÊNCIA NORMATIVA

Conforme disposto no Regimento do Comitê Gestor de Segurança da Informação e Comunicação do IFMA compete ao CSIC determinar e orientar acerca do uso legal de recursos computacionais dentro de seu domínio.

CAMPO DE APLICAÇÃO

Esta norma aplica-se a todo o IFMA.

OBJETIVOS GERAIS

Estabelecer regras e diretrizes gerais no uso de recursos computacionais e de rede e acesso à Internet, observados os objetivos Institucionais.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta norma observa a estrutura proposta pela Norma 01/IN01/CSIC/IFMA.

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

Número da Norma	Revisão - Data	Emissão	Folha
02/IN02/CSIC/IFMA		01/09/2015	2/7

NORMA GERAL DE SEGURANÇA E USO DE RECURSOS COMPUTACIONAIS E DE REDE – INTERNET

1 OBJETIVO

Estabelecer critérios gerais para a manutenção da segurança da informação e uso de recursos computacionais e de rede, incluindo aqui o acesso à Internet.

2 FUNDAMENTAÇÃO LEGAL E NORMATIVA.

Conforme disposto na POSIC compete ao CSIC do IFMA determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFMA.

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFMA 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 infra legais aplicáveis, a saber:

- Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;
- Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;
- Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;
- Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010;
- Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 12/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 14/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 15/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 16/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 17/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 18/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 19/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 20 /IN01/DSIC/GSI/PR, de 15 de dezembro de 2014;
- Norma Complementar nº 21 /IN01/DSIC/GSI/PR, de 10 de outubro de 2014;
- Acórdão nº 1603/2008 – Plenário do Tribunal de Contas da União (TCU);
- Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;
- Norma ABNT NBR ISO Guia nº 73:2002: Gestão de Riscos / Vocabulário;
- Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de

Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;

- Norma ABNT NBR ISO/IEC nº 27002:2005: Código de Prática para a Gestão de Segurança da Informação;
- 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
- Norma ISO/IEC GUIDE nº 51:1999, que fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

Conforme disposto no seu Regimento Interno, compete ao CSIC do IFMA determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFMA.

3 DO USO E SEGURANÇA DOS RECURSOS COMPUTACIONAIS E DE COMUNICAÇÃO.

O uso dos recursos de tecnologia da informação providos pelo IFMA deve observar os seguintes critérios:

3.1 As fontes de informações devem ser utilizadas pelos membros da comunidade observando-se o respeito ao princípio da dignidade humana e da ética.

3.2 Os Recursos de Tecnologia da Informação e Comunicações (RTIC) devem ser utilizados de maneira responsável, consistente com objetivos educacionais, de ensino, de pesquisa, extensão e finalidades administrativas do IFMA.

3.3 O uso dos recursos de TIC, quando necessitar de autorização prévia, deve estar de acordo com os objetivos específicos do projeto ou tarefa.

3.4 Os recursos de TIC não podem ser utilizados para constranger, assediar, ameaçar ou perseguir qualquer pessoa, invadir, alterar ou destruir recursos computacionais dela própria ou de outras instituições.

3.5 Constituem responsabilidades do usuário relativo ao uso dos recursos de TIC:

3.5.1 Respeitar as políticas, normas e procedimentos de uso dos recursos de TIC do IFMA.

3.5.2 Exibir a comprovação de vínculo com a IFMA ou autorização especial ao pessoal responsável, sempre que solicitado durante a utilização dos recursos, sob pena

de imediata suspensão da conexão, sem prejuízo das disposições legais pertinentes.

3.5.3 Respeitar a integridade e limites de sua autorização de acesso ou conta.

3.5.4 Responsabilizar-se por qualquer atividade desenvolvida com o auxílio dos recursos de TIC sob sua custódia e pelos eventuais prejuízos dela decorrentes, em qualquer nível.

3.5.5 Manter sigilo sobre sua conta e senha, salvo em casos específicos para os quais exige-se autorização expressa e por escrito do responsável pela gestão de TIC/Reitoria.

3.5.6 Não permitir ou colaborar com o acesso aos recursos de TIC do IFMA por parte de pessoas não autorizadas, sob pena de ser co-responsabilizado pelos eventuais problemas que esses acessos vierem a causar.

3.5.7 Usar o computador, sistema ou a rede de forma a não interferir ou interromper a operação normal do computador, sistema ou rede.

3.5.8 Não tentar, permitir ou causar qualquer alteração ou dano aos ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados no IFMA, de sua propriedade ou sob sua responsabilidade

3.5.9 Não ligar ou desligar fisicamente ou eletricamente a um recurso de TIC, nenhum componente externo, como cabos, access points, impressoras, discos ou sistemas de vídeo, sem uma autorização específica emitida pela Diretoria de TI ou Coordenação de TI dos campi.

3.5.10 Respeitar todas as obrigações contratuais do IFMA, inclusive com as limitações definidas nos contratos de software e outras licenças no uso dos recursos de TIC.

3.5.11 Comunicar ao responsável pela gestão de TIC do Câmpus/Reitoria qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros, de qualquer natureza.

3.6 Constituem responsabilidades dos Administradores de TIC (Diretor e Coordenadores) do IFMA:

3.6.1 Constituir e gerir controles que garantam a observância do disposto nesta Norma;

3.6.2 Proteger os direitos dos usuários.

3.6.3 Propor políticas e normas de segurança e uso dos recursos de TIC.

3.6.4 Controlar e, se for o caso, vetar o acesso ao usuário que violar as normas de uso de recursos de TIC;

3.6.5 Garantir prioridade de acesso via rede aos serviços essenciais do Instituto, mesmo que para isto tenha que limitar banda para acesso a outros serviços;

3.6.6 Divulgar junto à comunidade interna a política e as normas de TIC devidamente aprovadas.

3.7 O IFMA caracteriza como não ético e considera como motivo de ação disciplinar, qualquer atividade através da qual um usuário:

3.7.1 Não observe estritamente os objetivos institucionais;
3.7.2 Viole questões tais como direitos autorais, proteção de patentes e licenças de uso e outros contratos.
3.7.3 Interfira no uso correto dos recursos de informação.
3.7.4 Tente conseguir ou consiga acesso não autorizado a recursos de informação.
3.7.5 Sem autorização administrativa, destrua, altere, desmonte, desconfigure, impeça o acesso de direito ou interfira na integridade dos recursos de TIC.
3.7.6 Sem autorização judicial ou por força de sindicância, invada a privacidade de indivíduos ou entidades que são autores, criadores, usuários ou responsáveis por recursos de TIC.
3.7.7 Remova dos recursos computacionais do IFMA algum documento de sua propriedade ou por ela administrado, sem uma autorização específica.
3.7.8 Se faça passar por outra pessoa ou esconda sua identidade na utilização dos recursos de TIC, salvo nos casos em que o acesso anônimo é explicitamente permitido.
3.7.9 Viole ou tente violar os sistemas de segurança dos recursos de TIC, como quebra ou tentativa de obter identificações ou senhas de terceiros, interferir em fechaduras automáticas ou sistemas de alarme.
3.7.10 Intercepte ou tente interceptar transmissão de dados não destinados ao seu próprio acesso.
3.7.11 Tente interferir ou interfira em serviços de outros usuários ou o seu bloqueio, provocando, por exemplo, congestionamento da rede, inserindo códigos maliciosos ou tentando a apropriação dos recursos de TIC.
3.7.12 Obtenha benefícios financeiros ou de outra espécie, para si ou para terceiros através da utilização dos recursos de TIC do IFMA.

3.8 As penalidades a serem aplicadas às condutas relacionadas no Item 3.8, sem prejuízo de outras penas previstas em lei ou em normas do IFMA, são: redução ou eliminação, temporárias ou permanentes de privilégios de acesso, tanto aos recursos de TIC, quanto às redes, salas de computadores do IFMA e outros serviços ou facilidades.

3.9 A infração ou tentativa de infração às regras constantes desta norma ou às regras previstas em lei serão apuradas por meio de sindicância administrativa ou processo administrativo

disciplinar, nos termos da legislação em vigor.

3.10 Sempre que julgar necessário para a preservação da integridade dos recursos de TIC, dos serviços aos usuários ou dos dados, tanto o administrador local dos recursos de TIC, como o Diretor de TI do IFMA poderão suspender temporariamente qualquer conta, seja o responsável pela conta suspeito de alguma violação, ou não.

3.11 No caso do uso de redes externas, as normas envolvendo este tipo de uso também são aplicáveis e precisam ser adotadas.

4 DISPOSIÇÕES GERAIS

4.1 Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Diretor do CSIC que, se considerar necessário fará convocação de reunião do Comitê.

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

Número da Norma	Revisão	Emissão	Folha
03/IN03/CSIC/IFMA		01/09/2015	1/5

GESTÃO DE SOFTWARE PROPRIETÁRIO

ORIGEM

Esta é uma norma complementar à Política de Segurança de Informação e Comunicações (POSIC) e foi elaborada pelo Comitê Gestor de Segurança da Informação e Comunicações (CSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão (IFMA) instituído pela Portaria número 5851 de 05 de dezembro de 2012.

REFERÊNCIA NORMATIVA

Conforme disposto no Regimento do Comitê Gestor de Segurança da Informação e Comunicação do IFMA compete ao CSIC determinar e orientar acerca do uso legal de recursos computacionais dentro de seu domínio.

CAMPO DE APLICAÇÃO.

Esta norma aplica-se a todo o IFMA.

OBJETIVOS GERAIS.

Dar ciência e estabelecer critérios gerais para o uso de software proprietário dentro do IFMA.

SUMÁRIO.

INFORMAÇÕES ADICIONAIS.

Esta norma observa a estrutura proposta pela Norma 01/IN01/CSIC/IFMA.

Número da Norma	Revisão	Emissão	Folha
03/IN03/CSIC/IFMA		01/09/2015	2/5

GESTÃO DE SOFTWARE PROPRIETÁRIO

1 OBJETIVO

Dar ciência e estabelecer critérios gerais para o uso de software proprietário dentro do IFMA.

2 FUNDAMENTAÇÃO LEGAL E NORMATIVA.

Programa de Computador ou *Software* é propriedade intelectual, protegida pela Lei n.º 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, e pela Lei n.º 9.610, de 19 de fevereiro de 1998, que trata dos direitos autorais.

Conforme disposto no Regimento do CSIC do IFMA compete a ele estabelecer estes critérios para normas de segurança da informação.

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFMA 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;

GESTÃO DE SOFTWARE PROPRIETÁRIO

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 infra legais aplicáveis, a saber:

- Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;
- Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;
- Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;
- Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010;
- Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 12/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 14/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 15/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 16/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 17/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 18/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 19/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 20 /IN01/DSIC/GSI/PR, de 15 de dezembro de 2014;
- Norma Complementar nº 21 /IN01/DSIC/GSI/PR, de 10 de outubro de 2014;
- Acórdão nº 1603/2008 – Plenário do Tribunal de Contas da União (TCU);
- Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;
- Norma ABNT NBR ISO Guia nº 73:2002: Gestão de Riscos / Vocabulário;
- Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;

- Norma ABNT NBR ISO/IEC nº 27002:2005: Código de Prática para a Gestão de Segurança da Informação;
- 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
- Norma ISO/IEC GUIDE nº 51:1999, que fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

3 GESTÃO DE SOFTWARE PROPRIETÁRIO

3.1 Nenhum membro da comunidade do IFMA pode violar leis federais, estaduais ou locais relacionadas a direitos de propriedade intelectual referentes a licenças de software ou qualquer outra norma relacionada a software de computador ou conteúdos em formato digital;

3.2 Copiar *software* para distribuição para outros ou usar uma versão monousuário em diversos computadores em rede, caso tal hipótese não seja contemplada na sua licença, é ilegal e viola as leis de *software* e de direitos autorais;

3.3 Para o uso de qualquer *software* de propriedade ou licenciado pelo IFMA os seus usuários devem:

3.3.1 Concordar com todos os termos do acordo de licença de *software*;

3.3.2 Estar cientes de que todos os *softwares* são protegidos por direitos autorais, a menos que explicitamente rotulados como de Domínio Público;

3.4 Para *softwares* de propriedade ou licenciado pelo IFMA e *hardware* ou sistemas computacionais de propriedade ou operados pelo IFMA, os usuários não podem:

3.4.1 Copiar *software* para qualquer propósito com exceção daqueles permitidos no acordo de licença;

3.4.2 Tornar o *software* disponível para outras pessoas usarem ou copiarem, se tal procedimento estiver em desacordo com os termos da licença de *software* e/ou procedimentos adotados pelo IFMA;

3.4.3 Instalar, nem permitir ou induzir outros a instalarem, cópias ilegais de *software*, ou *software* sem as devidas licenças, em qualquer recurso computacional de propriedade ou operado pelo IFMA;

3.5 Toda aquisição de equipamento computacional deve incluir, necessariamente, a aquisição de licenças do *software* básico mínimo apropriado para o seu uso final;

3.6 Toda licença de *software*, de qualquer natureza, adquirida pelo IFMA deve ser obrigatoriamente registrada junto ao seu proprietário se dada essa opção, assim como também as licenças de *software* incluídas na aquisição do equipamento

3.7 As licenças adquiridas só podem ser utilizadas para fins institucionais;

3.8 A instalação de *software* nos equipamentos computacionais do IFMA somente é autorizada mediante as formalizações de registro e arquivamento da licença de uso, em sistema centralizado a instância responsável pelo equipamento, excluídos os *softwares* abertos ou de uso gratuito;

3.8.1 As disposições deste artigo aplicam-se também aos equipamentos e às licenças de *software* doados ou adquiridos por convênios ou projetos de pesquisa vinculados do IFMA;

3.9 Ao violar esta Norma o usuário estará sujeito a sanções em todas as instâncias cabíveis.

4 DISPOSIÇÕES GERAIS

4.1 Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Diretor do CSIC que, se considerar necessário fará convocação de reunião do Comitê.

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

Número da Norma	Revisão	Emissão	Folha
04/IN04/CSIC/IFMA		01/09/2015	1/10

USO DO CORREIO ELETRÔNICO INSTITUCIONAL

ORIGEM

Esta é uma norma complementar à Política de Segurança de Informação e Comunicação (POSIC) e foi elaborada pelo Comitê Gestor de Segurança da Informação e Comunicação (CSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão (IFMA) instituído pela Portaria número 5851 de 05 de dezembro de 2012.

REFERÊNCIA NORMATIVA

Conforme disposto no Regimento do Comitê Gestor de Segurança da Informação e Comunicação do IFMA compete ao CSIC determinar e orientar acerca do uso legal de recursos computacionais dentro de seu domínio.

CAMPO DE APLICAÇÃO

Esta norma aplica-se a todo o IFMA.

OBJETIVOS GERAIS

Estabelecer critérios para concessão e uso do recurso de correio eletrônico institucional.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta norma observa a estrutura proposta pela Norma 01/IN01/CSIC/IFMA.

USO DO CORREIO ELETRÔNICO INSTITUCIONAL

1 OBJETIVO

Dar ciência e estabelecer critérios gerais para o uso do correio eletrônico dentro do IFMA.

2 FUNDAMENTAÇÃO LEGAL E NORMATIVA.

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFMA 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 infra legais aplicáveis, a saber:

- Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;
- Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;
- Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;
- Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010;
- Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 12/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 14/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 15/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 16/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 17/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 18/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 19/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 20 /IN01/DSIC/GSI/PR, de 15 de dezembro de 2014;
- Norma Complementar nº 21 /IN01/DSIC/GSI/PR, de 10 de outubro de 2014;
- Acórdão nº 1603/2008 – Plenário do Tribunal de Contas da União (TCU);
- Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;
- Norma ABNT NBR ISO Guia nº 73:2002: Gestão de Riscos / Vocabulário;
- Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;
- Norma ABNT NBR ISO/IEC nº 27002:2005: Código de Prática para a Gestão de Segurança da Informação;
- 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;
- Norma ISO/IEC GUIDE nº 51:1999, que fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

Conforme disposto no seu Regimento Interno, compete ao CSIC do IFMA determinar critérios

para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFMA.

3 DEFINIÇÕES

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 contramedida;
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 IFMA;

XXVII – *Usuário externo*: qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente ao IFMA;
XXVIII – *Comunicação oficial*: tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas do IFMA 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.

4 DO DOMÍNIO E SUBDOMÍNIOS IFMA.EDU.BR

4.1 Todos os usuários dos serviços de correio eletrônico do IFMA estarão inscritos no domínio ifma.edu.br e seus subdomínios;

4.2 O domínio ifma.edu.br será utilizado apenas para contas de correio eletrônico de cunho institucional;

4.3 As contas de correio eletrônico (e-mail) serão criadas com base na padronização aprovada pela *Worldwide Electronic Messaging Association-WEMA*, conforme padrões internacionais definidos pela *ITU - International Telecommunications Union / Telecommunication Standardization Sector* e terão a seguinte orientação:

Servidores efetivos:

4.3.1 A identificação do nome que vai aparecer no e-mail deve ser exatamente igual ao que está no Sistema Unificado de Administração Pública - SUAP (sem acentos ou cedilha);

4.3.2 O nome de usuário do e-mail será composto pelo primeiro nome, o caracter ".", seguido do último nome do usuário;

4.3.3 Havendo duplicidade de identificação, utilizar-se-á o segundo nome em substituição ao último nome;

4.3.4 Continuando a duplicidade, e se houver nomes intermediários, estes serão utilizados em substituição ao último nome;

4.3.5 Continuando a duplicidade que trata o artigo anterior, será utilizada uma combinação entre nomes intermediários e sobrenome, sempre mantendo o primeiro nome;

4.3.6 Não utilizar acentos (til, agudo, grave, circunflexo, trema);

4.3.7 Quando constarem do sobrenome qualificadores de geração (Júnior, Filho, Neto e outros), é recomendável usar o sobrenome composto;

JOAQUIM.XAVIERFILHO;

4.3.8 Depois da criação o servidor é inserido automaticamente no grupo à qual pertence.

4.3.9 Na criação de e-mail ou grupo de e-mail para setores, o padrão a ser seguido é "sigla do setor" seguido do caracter "." seguido do nome do campus. A título de ilustração, se tivéssemos o setor de T.I. no Campus Codó, o nome indicado seria "NTI.codo@ifma.edu.br".

4.3.10 O envio de mensagens para servidores@ifma.edu.br e servidores.campus@ifma.edu.br serão moderados pela Assessoria de Comunicação, demais grupos terão restrições específicas e serão moderados e definidos pela equipe de TI do Campus/Reitoria de acordo com a finalidade a que se propõe;

4.4 Cada servidor deverá ter uma conta institucional de e-mail e poderá participar de tantos grupos quanto forem necessários;

4.5 As contas de e-mail serão suspensas, nos seguintes casos:

4.5.1 Por *login* inativo maior que 90 dias;

4.5.2 Contas fora do padrão definido no item 4.3 desta norma. Tais contas só serão reativadas se renomeadas para o padrão;

4.5.3 Por perda do vínculo institucional (30 dias após desligamento).

4.6 Contas suspensas que forem reativadas deverão ser acessadas no mesmo dia, caso contrário serão novamente suspensas.

Terceirizados:

4.7 Prestadores de serviços terceirizados e estagiários poderão, durante o período de prestação dos serviços, a critério do responsável pela área onde está sendo prestado o serviço terceirizado ou estágio e no interesse do serviço, ter acesso ao correio eletrônico institucional, desde que solicitadas por memorando da chefia imediata, indicando a data inicial e final do vínculo com a instituição.

5 DA UTILIZAÇÃO DO CORREIO ELETRÔNICO

5.1 Os serviços de correio eletrônico são oferecidos como um recurso oficial para apoiar discentes, docentes e servidores técnico-administrativos no cumprimento de suas

atribuições nas áreas de administração, ensino, pesquisa, extensão, comunicação e serviços, não sendo permitido seu uso para fins pessoais;

5.2 Deve ser incentivado, junto aos seus servidores, o uso do serviço de correio eletrônico no desempenho de suas atividades funcionais, objetivando a racionalização do trabalho e o aumento da produtividade por meio da facilitação da troca de informações e do intercâmbio de ideias;

5.3 O acesso ao correio eletrônico se dá pelo conjunto Identificação do Usuário, Caixa Postal e Senha que é pessoal e intransferível;

5.3.1 Quando do reconhecimento e habilitação de uso do serviço de correio eletrônico para unidades administrativas, grupos de trabalho e outros usuários despersonalizados, deverá ser identificada junto ao administrador do serviço a pessoa responsável pelo uso do correio destes usuários.

5.4 Cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal;

5.5 O usuário deverá manter a segurança de sua conta de correio eletrônico com o uso de senhas fortes;

5.6 Uma conta de correio eletrônico vulnerável é um risco para a Instituição à medida em que possa ser explorada de forma maliciosa por terceiros para distribuição de SPAM e conteúdos nocivos;

5.7 É vedada tentativa de acesso não autorizado às caixas postais de terceiros;

5.8 As mensagens deverão ser redigidas de forma clara e sucinta, devendo conter o grau de formalidade compatível com o destinatário e o assunto tratado;

5.9 É vedado o envio e o armazenamento de mensagens contendo:

5.9.1 Material de natureza racista, difamatória, obsceno, intimidadora, ofensiva, abusiva, preconceituosa, discriminatória, ilegal ou antiético;

5.9.2 Anúncios publicitários;

5.9.3 Listas de endereços eletrônicos dos usuários do Correio Eletrônico da Instituição;

5.9.4 Vírus ou qualquer outro tipo de programa danoso;

5.9.5 Material protegido por leis de propriedade intelectual;

5.9.6 Entretenimentos e "correntes";

5.9.7 Material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos.

USO DO CORREIO ELETRÔNICO INSTITUCIONAL

5.10 O IFMA, de forma geral, não pode e não tem por objetivo, ser o árbitro do conteúdo de mensagens eletrônicas e impedir que os usuários recebam mensagens ofensivas, mas os membros da comunidade são encorajados a utilizar o serviço de correio eletrônico de acordo com a mesma ética aplicada a outras formas de comunicação;

5.11 A concessão de uma conta de e-mail não atribui ao usuário poder de representação do IFMA;

5.12 O e-mail institucional é de propriedade do IFMA, que poderá inserir mensagens informativas à comunidade a qualquer momento utilizando-o como canal de comunicação. As mensagens eletrônicas conterão uma declaração explícita, informando que o autor do texto não está representando o IFMA e que é responsável por seu conteúdo.

5.13 Os usuários do correio eletrônico não devem falsificar sua identidade, o seu nome de usuário ao utilizar o sistema de mensagens ou alterar a linha de origem da mensagem ou qualquer outra indicação da origem da mensagem;

5.14 Listas de distribuição poderão ser criadas sob demanda da Instituição sem a necessidade de consultar os usuários inseridos nas mesmas;

5.15 É facultada ao usuário a opção de solicitar posteriormente seu descadastramento da lista de distribuição que será analisado pela instância competente;

5.16 A inconveniência e possíveis ameaças contidas em mensagens indesejáveis, provenientes de fontes comerciais ou não, podem levar o Administrador de Sistemas e Rede a bloquear a recepção de mensagens provenientes de alguns locais da rede;

5.17 Caracterizado o descumprimento de qualquer dos itens desta Norma, caberá à administração do correio eletrônico informar a chefia imediata ou superior do usuário, apresentando o ocorrido a fim de encaminhar as providências de apuração de responsabilidades.

6 DA PRIVACIDADE DAS MENSAGENS DE CORREIO ELETRÔNICO

6.1 Os e-mails, na condição de arquivos armazenados ou gerados com os recursos de TIC para fins produtivos, também são de propriedade do IFMA e, portanto, passíveis de auditorias;

6.2 A auditoria a que faz referência o item 6.1 desta norma destina-se exclusivamente à manutenção da segurança da infraestrutura de TIC, bem como a resguardar os objetivos da Instituição;

6.3 Fica assegurado aos usuários o sigilo de conteúdo de seus e-mails e arquivos, exceto por determinação judicial em contrário ou por força de sindicância interna ou processo

administrativo disciplinar;

6.4 À DGTI fica assegurado o direito de, em casos nos quais a segurança dos recursos de TIC da Instituição sejam ameaçados, eliminar e-mails e arquivos, bloquear conteúdos e usuários, temporariamente ou permanentemente;

6.5 Solicitações de informações para pedidos de auditoria nas contas de e-mail institucional devem ser encaminhadas à Diretoria de Gestão de Tecnologia da Informação.

7 DISPOSIÇÕES GERAIS

7.1 As contas de correio eletrônico serão criadas pela DGTI e pelos setores de TI de cada campus, em atenção à solicitação formal da chefia imediata ou superior, com os respectivos dados cadastrais;

7.2 Cabe à chefia imediata ou superior comunicar a Administração do Correio Eletrônico o desligamento de empregados terceirizados, temporários e estagiários sob sua responsabilidade para a exclusão definitiva da caixa postal;

7.3 Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Presidente do CSIC que, se considerar necessário, fará convocação de reunião do Comitê.

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

Número da Norma	Revisão	Emissão	Folha
05/IN05/CSIC/IFMA		01/09/2015	1/8

GESTÃO DE DADOS CORPORATIVOS

ORIGEM

Esta é uma norma complementar à Política de Segurança de Informação e Comunicação (POSIC) e foi elaborada pelo Comitê Gestor de Segurança da Informação e Comunicação (CSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão (IFMA) instituído pela Portaria número 5851 de 05 de dezembro de 2012.

REFERÊNCIA NORMATIVA

Conforme disposto no Regimento do Comitê Gestor de Segurança da Informação e Comunicação do IFMA compete ao CSIC determinar e orientar acerca do uso legal de recursos computacionais dentro de seu domínio.

CAMPO DE APLICAÇÃO.

Esta norma aplica-se a todo o IFMA.

OBJETIVOS GERAIS.

Estabelecer critérios para a gestão de dados corporativos

SUMÁRIO.

INFORMAÇÕES ADICIONAIS.

Esta norma observa a estrutura proposta pela Norma 01/IN01/CSIC/IFMA.

Número da Norma	Revisão	Emissão	Folha
05/IN05/CSIC/IFMA		01/09/2015	2/8

GESTÃO DE DADOS CORPORATIVOS

1 OBJETIVO

Dar ciência e estabelecer critérios gerais para o uso de software proprietário dentro do IFMA.

2 FUNDAMENTAÇÃO LEGAL E NORMATIVA.

Conforme disposto no Regimento do CSIC do IFMA compete a ele estabelecer estes critérios para normas de segurança da informação.

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFMA 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 infra legais aplicáveis, a saber:

- Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;
- Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;
- Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;
- Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010;
- Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 12/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 14/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 15/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 16/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 17/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 18/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 19/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 20 /IN01/DSIC/GSI/PR, de 15 de dezembro de 2014;
- Norma Complementar nº 21 /IN01/DSIC/GSI/PR, de 10 de outubro de 2014;
- Acórdão nº 1603/2008 – Plenário do Tribunal de Contas da União (TCU);
- Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;
- Norma ABNT NBR ISO Guia nº 73:2002: Gestão de Riscos / Vocabulário;
- Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;
- Norma ABNT NBR ISO/IEC nº 27002:2005: Código de Prática para a Gestão de Segurança da Informação;

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

Conforme disposto no seu Regimento Interno, compete ao CSIC do IFMA determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFMA.

3 DEFINIÇÕES

3.1 Para efeito desta norma considera-se:

3.1.1 *Dado*: Qualquer elemento identificado em sua forma bruta e que, por si só, não conduz a uma compreensão de um fato ou situação;

3.1.2 *Acesso*: permissão, privilégio ou capacidade de ler, registrar, atualizar, gerenciar ou administrar a consulta e/ou a manipulação do acervo de dados e informações do IFMA;

3.1.3 *Dado de uso corporativo ou institucional*: todos os dados capturados e utilizados nas operações de serviço e administrativas do IFMA;

3.1.4 *Agente*: qualquer pessoa ou conjunto de pessoas autorizadas pelo IFMA para o acesso e/ou tratamento dos dados corporativos: docentes, funcionários, discentes e terceirizados;

3.1.5 *Informação*: dados contextualizados;

3.1.6 *Responsável pela custódia do dado*: agente do IFMA a quem é delegada responsabilidade por uma parte dos dados com o objetivo de garantir a sua integridade e precisão;

3.1.7 *Responsável pelo gerenciamento dos dados*: é o agente do IFMA que fornece serviços de processamento de dados como suporte aos usuários dos dados;

3.1.8 *Administrador de Sistemas e Rede*: responsável pela segurança, disponibilidade e integridade dos dados e serviços disponíveis no ambiente computacional sob seu controle e responsável por manter o sigilo das senhas de acesso a esse ambiente;

3.1.9 *Usuário de dados*: agente autorizado a ler, registrar, e/ou atualizar dados.

4 GESTÃO DE DADOS CORPORATIVOS

4.1 O IFMA é proprietário de todos os seus dados corporativos e detém os direitos autorais de todas as políticas, manuais e compilações destes dados;

4.2 Aos responsáveis pela custódia dos dados cabe:

4.2.1 Identificar os itens de dados corporativos e a sua fonte primária;

4.2.2 Identificar e documentar a quem é permitido o acesso ao dado e o nível de acesso;

4.2.3 Autorizar acesso aos dados;

4.2.4 Especificar os requisitos de segurança de acesso;

4.2.5 Estabelecer procedimentos para a obtenção de autorização para acesso aos dados;

4.2.6 Implementar processos que mantenham a integridade, precisão, temporalidade, consistência, padronização e o valor do dado;

4.2.7 Garantir através de procedimentos que o dado seja captado e utilizado de forma adequada;

4.2.8 Monitorar as atividades de acesso aos dados e notificar as exceções ao Diretor do DGTI.

4.3 Aos responsáveis pela gerência dos dados compete:

4.3.1 Implementar a segurança de acesso aos dados como especificado pelo Responsável pela Custódia do Dado, assim como de acordo com os padrões e orientação de acesso aos dados;

4.3.2 Prover acesso aos dados pelos usuários como especificado pelo Responsável pela Custódia do Dado;

4.3.3 Garantir que os mecanismos de proteção física dos dados estejam instalados e operando de forma satisfatória;

4.3.4 Monitorar a efetividade dos controles implantados contra tentativas de acesso não autorizado;

4.3.5 Acessar os dados, da forma autorizada pelo Responsável pela Custódia do Dado, para a execução das tarefas necessárias para garantir a disponibilidade e acessibilidade;

4.3.6 Garantir que todos os dados possuem um responsável pela sua custódia;

4.3.7 Prover e dar suporte aos sistemas e aplicações necessárias para atender às especificações dos Responsáveis pela Custódia do Dado para a manutenção e disseminação dos dados;

4.3.8 Proteger os dados contra destruição, modificações ou acessos durante as transferências eletrônicas ou físicas de um local para outro;

4.3.9 Documentar e promover o valor do dado para os objetivos do IFMA e facilitar o compartilhamento e a integração dos dados;

4.3.10 Gerenciar o uso de padrões comuns de definição de dados em toda o IFMA.

4.4 Aos usuários de dados compete:

4.4.1 Acessar os dados conforme a autorização dada pelo Responsável pela Custódia do Dado;

4.4.2 Garantir que os mecanismos de proteção física dos dados estejam instalados e operando de forma satisfatória.

4.5 É vetado aos usuários de dados divulgar qualquer dado sem a permissão do responsável pela custódia;

4.6 É política do IFMA manter os dados corporativos integrados e íntegros através de todas as suas instâncias, permitindo que os seus administradores acessem as informações que necessitam, dentro de um ambiente controlado;

4.7 Novos sistemas desenvolvidos ou adquiridos de terceiros devem se integrar dos sistemas corporativos existentes, atendendo requisitos técnicos para esta integração;

4.8 Ao responsável pela custódia dos dados cabe:

4.8.1 Identificar os itens de dados corporativos e a sua fonte primária;

4.8.2 Identificar e documentar a quem é permitido o acesso ao dado e o nível de acesso;

4.8.3 Autorizar acesso aos dados;

4.8.4 Especificar os requisitos de segurança de acesso;

4.8.5 Estabelecer procedimentos para a obtenção de autorização para acesso aos dados;

4.8.6 Implementar processos que mantenham a integridade, precisão, temporalidade, consistência, padronização e o valor do dado;

4.8.7 Garantir através de procedimentos que o dado seja captado e utilizado de forma adequada;

4.8.8 Monitorar as atividades de acesso aos dados e notificar as exceções ao Diretor da

DGTI.

4.9 Aos responsáveis pela gerência dos dados compete:

4.9.1 Implementar a segurança de acesso aos dados como especificado pelo Responsável pela Custódia do Dado, assim como de acordo com os padrões e orientação de acesso aos dados;

4.9.2 Prover acesso aos dados pelos usuários como especificado pelo Responsável pela Custódia do Dado;

4.9.3 Garantir que os mecanismos de proteção física dos dados estejam instalados e operando de forma satisfatória;

4.9.4 Monitorar a efetividade dos controles implantados contra tentativas de acesso não autorizado;

4.9.5 Acessar os dados, da forma autorizada pelo Responsável pela Custódia do Dado, para a execução das tarefas necessárias para garantir a disponibilidade e acessibilidade;

4.9.6 Garantir que todos os dados possuem um responsável pela sua custódia;

4.9.7 Prover e dar suporte aos sistemas e aplicações necessárias para atender às especificações dos Responsáveis pela Custódia do Dado para a manutenção e disseminação dos dados;

4.9.8 Proteger os dados contra destruição, modificações ou acessos durante as transferências eletrônicas ou físicas de um local para outro;

4.9.9 Documentar e promover o valor do dado para os objetivos do IFMA e facilitar o compartilhamento e a integração dos dados;

4.9.10 Gerenciar o uso de padrões comuns de definição de dados em todo o IFMA.

4.10 Aos usuários de dados compete:

4.10.1 Acessar os dados conforme a autorização dada pelo Responsável pela Custódia do Dado;

4.10.2 Garantir que os mecanismos de proteção física dos dados estejam instalados e operando de forma satisfatória;

4.10.3 É vetado aos usuários de dados divulgar qualquer dado sem a permissão do responsável pela custódia;

4.10.4 O IFMA é proprietário de todos os seus dados corporativos e detém os direitos autorais de todas as políticas, manuais e compilações destes dados;

4.10.5 É política do IFMA manter os dados corporativos integrados e íntegros através de todas as suas instâncias, permitindo que os seus administradores acessem as informações que necessitam, dentro de um ambiente controlado.

4.11 Os prestadores de serviços ao IFMA que, por força de contrato, tenham acesso a qualquer de seus dados corporativos deverão ser signatários de um ACORDO DE CONFIDENCIALIDADE que será firmado no ato da contratação dos serviços.

5 DISPOSIÇÕES GERAIS

5.1 Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Presidente do CSIC que, se considerar necessário fará convocação de reunião do Comitê.

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

Número da Norma	Revisão - Data	Emissão	Folha
06/IN06/CSIC/IFMA		01/09/2015	1/8

GESTÃO DE SENHAS

ORIGEM

Esta é uma norma complementar à Política de Segurança de Informação e Comunicações (POSIC) e foi elaborada pelo Comitê Gestor de Segurança da Informação e Comunicações (CSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão (IFMA) instituído pela Portaria número 5851 de 05 de dezembro de 2012.

REFERÊNCIA NORMATIVA

Conforme disposto no Regimento do Comitê Gestor de Segurança da Informação e Comunicação do IFMA compete ao CSIC determinar e orientar acerca do uso legal de recursos computacionais dentro de seu domínio.

CAMPO DE APLICAÇÃO

Esta norma aplica-se a todo o IFMA.

OBJETIVOS GERAIS

Estabelecer critérios geração e manutenção de senhas de usuários.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta norma observa a estrutura proposta pela Norma 01/IN01/CSIC/IFMA.

GESTÃO DE SENHAS

1 FUNDAMENTAÇÃO LEGAL E NORMATIVA

Conforme disposto na POSIC compete ao CSIC do IFMA determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFMA.

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFMA 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 infra legais aplicáveis, a saber:

GESTÃO DE SENHAS

- Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;
- Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;
- Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;
- Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010;
- Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 12/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 14/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 15/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 16/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 17/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 18/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 19/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 20 /IN01/DSIC/GSI/PR, de 15 de dezembro de 2014;
- Norma Complementar nº 21 /IN01/DSIC/GSI/PR, de 10 de outubro de 2014;
- Acórdão nº 1603/2008 – Plenário do Tribunal de Contas da União (TCU);
- Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;
- Norma ABNT NBR ISO Guia nº 73:2002: Gestão de Riscos / Vocabulário;
- Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;
- Norma ABNT NBR ISO/IEC nº 27002:2005: Código de Prática para a Gestão de Segurança da Informação;
- 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

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

Conforme disposto no seu Regimento Interno, compete ao CSIC do IFMA determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFMA.

2 GESTÃO DE SENHAS

2.1 O gerenciamento de senhas constitui o mecanismo básico para a autenticação de usuários dos sistemas computacionais do IFMA.

2.1.1 Senhas são confidenciais, intransferíveis e é responsabilidade do usuário mantê-la como tal, observando mecanismos de segurança e integridade.

2.2 Para fins desta norma considera-se senha temporária a senha gerada inicialmente pelo Administrador de Sistemas e Rede para um usuário.

2.3 Novas senhas serão fornecidas e senhas já existentes serão liberadas apenas quando a identidade do requisitante estiver univocamente assegurada.

2.4 Os usuários serão responsabilizados pelas ações de outros se, desrespeitando o item anterior, deliberadamente, compartilharem sua senha de acesso.

2.5 Senhas devem conter no mínimo oito caracteres incluindo números, letras e caracteres especiais e não devem possuir uma regra de formação perceptível.

2.6 Senhas devem ser trocadas periodicamente, num prazo não superior a seis (6) meses.

2.7 Os usuários devem trocar suas senhas imediatamente após suspeitarem que foram violadas.

2.8 Em caso de esquecimento da senha uma senha temporária pode ser fornecida, não sendo tecnicamente possível a recuperação da senha anterior.

2.9 A troca de senha temporária é obrigatória na primeira autenticação.

2.10 Cabe ao Administrador de Sistemas e Rede adotar procedimentos de administração de senhas específicos para o seu ambiente computacional, observando os critérios gerais anteriores.

2.11 A robustez das senhas poderá ser auditada pela Diretoria de TI com fins de localização de senhas fracas.

2.12 O usuário que tiver sua senha encontrada pelos testes de robustez será notificado para que as troquem por senha seguras em, no máximo, setenta e duas horas.

descumprimento desta determinação terá como consequência o bloqueio de seus acessos aos serviços do IFMA.

3 DISPOSIÇÕES GERAIS

3.1 Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Diretor do CSIC que, se considerar necessário fará convocação de reunião do Comitê.

GESTÃO DE SENHAS

ANEXO

Considerações e sugestões para elaboração de senhas fortes.

Uma boa senha possui de 8 a 12 dígitos. Mas, quanto mais longa, melhor.

Não utilize palavras e nomes conhecidos. Programas de quebra de senha possuem uma base bastante aprimorada com diversos dicionários, afim de testar cada uma destas palavras e tentar então quebrar essa senha.

Utilize caracteres alfanuméricos como números e sinais de pontuação, além de também alternar letras maiúsculas e minúsculas.

Evite anotar suas senhas em papéis ou divulgar para outras pessoas. Trabalhe num conjunto de caracteres que possam representar simbolicamente algo para você, e que possa ser facilmente lembrado.

Use senhas diferentes para suas contas. Obviamente é mais cômodo ter apenas uma boa senha, mas em caso de furto ou vazamento, todas as contas e sistemas nos quais você utiliza desta senha para acesso poderão ser facilmente acessados por quem se beneficiar.

Mude suas senhas com frequência. Isto com certeza pode te ajudar no caso de alguém estar bisbilhotando alguma conta sua (particular ou de trabalho) e não estiver deixando rastros.

A revista Businessweek publicou, no dia 27 de janeiro de 2011, um artigo mostrando a vulnerabilidade das senhas que usamos em nosso dia a dia. Segundo o artigo, as senhas mais usadas são: 123456, password, 12345678, qwerty, abc123.

A Tabela 1 representa o tempo necessário para quebrar uma senha, levando em conta seu tamanho e a regra de formação:

Tabela 1

Tamanho da senha	**Minúsculas**	**Maiúsculas**	**Nºs e Símbolos**	
6 caracteres	10 minutos	10 horas	18 dias	
7 caracteres	4 horas	23 dias	4 anos	
8 caracteres	4 dias	3 anos	463 anos	
9 caracteres	4 meses	178 anos	44.530 anos	

GESTÃO DE SENHAS

O gasto médio das empresas para tratar de problemas relativos a troca de senha é de U$ 10,00. 30% dos chamados feitos a serviços de helpdesk são relativos a senhas. 50% dos usuários escolhem senhas baseadas em palavras comuns, datas de aniversário, nomes de parentes, palavras de cunho religioso ou combinações simples de caracteres.

Sempre somos aconselhados a utilizar senhas seguras. Senhas seguras são aquelas que tem pelo menos 8 caracteres e são compostas por letras, números e caracteres especiais.

Mas isso é um problema. Temos sempre muitas senhas para guardar e senhas com as características citadas acima não são nada mnemônicas. Como proceder então? Como criar senhas difíceis de serem quebradas e ao mesmo tempo fáceis de serem lembradas?

Uma solução muito boa é o uso de uma frase, por exemplo:

Eu nasci as 14:00 da tarde de 1980.

Se pegarmos as primeiras letras de cada palavra (respeitando maiúsculas e minúsculas) e os números temos a seguinte senha:

Ena14:00dtd1980.

Prestem atenção ao ponto ao final da senha!

Uma outra técnica interessante é utilizar o endereço do usuário. Por exemplo, vamos supor de uma empresa fictícia: Rapidinho Encomendas

O endereço da Rapidinho Encomendas é rua da Glória, número 325, sala 45!

Isso geraria a seguinte senha:

OedREerdG,n325,s45!

Mais uma vez atenção à exclamação ao final da senha!

Poderíamos deixar esta senha mais segura trocando a palavra número pelo símbolo #, e teríamos:

OedREerdG,#325,s45!

Tudo certo? Quase... Cuidado existem senhas com muitos caracteres estranhos e coisa do tipo, mas que são muito manjadas como:

Uma arroba é 15 Kilos:

U@é15Kg

ou

"Batatinha quando nasce se esparrama pelo chão" podemos gerar a senha "!Bqnsepc" (o sinal de exclamação foi colocado no início para acrescentar um símbolo à senha). Esta senha encontra-se na Cartilha de Segurança disponibilizada no site do www.cert.br.

!BqnsepC"

Senhas desse tipo são muito usadas e fáceis de serem quebradas apesar da sua aparência de inquebrável.

A informação é um patrimônio inestimável da Instituição e cabe ao servidor zelar pela sua integridade, disponibilidade, autenticidade e veracidade.

Lei Nº 8.112, de 11 de dezembro de 1990, Art. 116: São deveres do servidor: ... VII - **zelar pela economia do material e a conservação do patrimônio público;**

Referências:

http://www.dicas-l.com.br/arquivo/o_problema_das_senhas.php. Acessado em 07/04/2011.

http://www.dicas-l.com.br/arquivo/administracao_de_senhas_for_dummies.php. Acessado em 07/04/2011.

http://cartilha.cert.br/. Acessado em 07/04/2011.

http://www.planalto.gov.br/ccivil_03/Leis/L8112cons.htm. Acessado em 07/04/2011.

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO
CONSELHO SUPERIOR

Número da Norma	Revisão	Emissão	Folha
07/IN07/CSIC/IFMA		01/09/2013	1/5

HOSPEDAGENS E PUBLICAÇÕES NA INTERNET

ORIGEM

Esta é uma norma complementar à Política de Segurança de Informação e Comunicações (POSIC) e foi elaborada pelo Comitê Gestor de Segurança da Informação e Comunicações (CSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão (IFMA) instituído pela Portaria número 5851 de 05 de dezembro de 2012.

REFERÊNCIA NORMATIVA

Conforme disposto no Regimento do Comitê de Segurança da Informação e Comunicação do IFMA compete ao CSIC determinar e orientar acerca do uso de hospedagens e publicações na internet dentro de seu domínio.

CAMPO DE APLICAÇÃO.

Esta norma aplica-se a todo o IFMA.

OBJETIVOS GERAIS.

Estabelecer critérios para hospedagem de páginas e publicações na internet.

SUMÁRIO

INFORMAÇÕES ADICIONAIS.

Esta norma observa a estrutura proposta pela Norma 01/IN01/CSIC/IFMA.

HOSPEDAGENS E PUBLICAÇÕES NA INTERNET

1 OBJETIVO

Estabelecer critérios para hospedagem de páginas e publicações na internet.

1 FUNDAMENTAÇÃO LEGAL E NORMATIVA.

Conforme disposto no Regimento do CSIC do IFMA compete a ele estabelecer estes critérios para normas de segurança da informação.

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFMA 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 infra legais aplicáveis, a saber:

- Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;
- Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;
- Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;
- Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
- Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010;
- Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 12/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 14/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 15/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 16/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 17/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 18/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 19/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 20 /IN01/DSIC/GSI/PR, de 15 de dezembro de 2014;
- Norma Complementar nº 21 /IN01/DSIC/GSI/PR, de 10 de outubro de 2014;
- Acórdão nº 1603/2008 – Plenário do Tribunal de Contas da União (TCU);
- Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;
- Norma ABNT NBR ISO Guia nº 73:2002: Gestão de Riscos / Vocabulário;
- Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;

- Norma ABNT NBR ISO/IEC nº 27002:2005: Código de Prática para a Gestão de Segurança da Informação;
- 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
- Norma ISO/IEC GUIDE nº 51:1999, que fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

Conforme disposto no seu Regimento Interno, compete ao CSIC do IFMA determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFMA.

3 HOSPEDAGENS E PUBLICAÇÕES NA INTERNET

3.1 Poderá ser disponibilizado aos usuários cadastrados, bem como aos setores ou grupos vinculados à instituição, espaço para publicação de páginas próprias na Internet (*websites*), com conteúdo e design de responsabilidade do usuário ou do responsável pelo setor ou grupo.

3.1.1 A área disponibilizada para a hospedagem de páginas é limitada em tamanho e para uso específico da publicação das páginas do setor/projeto, portanto em hipótese alguma deverá ser usada para outros fins, como por exemplo: backup, download de programas etc;

3.1.2 Todas as solicitações de publicações de páginas próprias na Internet, serão avaliadas tecnicamente pela DGTI, que se posicionará sobre a viabilidade de tal publicação.

3.1.3 Considerando que as páginas próprias são documentos públicos disponíveis para qualquer pessoa em qualquer lugar e que o domínio "ifma.edu.br" e sub-domínios relacionados a eles, ao qual tais páginas pertencem, é um bem intangível importante do IFMA, a ASSCOM reserva-se o direito de avaliar seu conteúdo, permitindo ou não sua publicação, já que tais documentos podem influenciar na formação da imagem da instituição e na sua reputação diante da comunidade.

3.2 É proibida a publicação de páginas próprias com os seguintes conteúdos ou links:

I. De cunho puramente pessoal, sem vinculação com suas atividades na instituição;

II. Comerciais ou de caráter publicitário;

III. De caráter político-partidário ou religioso;

IV. Caluniosos, difamatórios ou ameaçadores;

V. Que orientem a qualquer prática ou atividade ilegal;

VI. Que infrinjam a legislação sobre direitos autorais ou propriedade intelectual;

VII. Que provoquem a invasão de privacidade de qualquer cidadão, ou organização constituída;

VIII. Ofensivos ou que façam uso de linguagem ofensiva;

IX. Que incitem a qualquer tipo de discriminação;

X. Que incitem à violência;

XI. Pornográfico de qualquer natureza;

XII. Com imagens ou dados que possam ser considerados abusivos, profanos ou incômodos.

XIII. Que infrinjam a legislação vigente em todas as suas instâncias.

3.3 A Assessoria de Comunicação do IFMA (ASSCOM) é responsável pela divulgação de informações na página principal da instituição.

3.3.1 Outros setores da instituição poderão ter acesso à administração de determinados itens da página principal do IFMA para publicação de documentos oficiais da instituição de sua responsabilidade, desde que formalmente solicitado. A liberação de determinados itens poderá sofrer avaliação técnica da DGTI e de conteúdo da ASSCOM.

3.3.2 A DGTI é responsável pela permissão de acesso às áreas de administração da página principal do IFMA aos usuários que forem designados pela Reitoria para esse fim.

3.4 A hospedagem de páginas no domínio ifma.edu.br e seus subdomínios serão feitos exclusivamente pela DGTI. Domínios registrados por outros setores ou unidades administrativas não serão considerados oficiais e deverão ser cancelados por seu responsável;

4 DISPOSIÇÕES GERAIS

4.1 Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Diretor do CSIC que, se considerar necessário fará convocação de reunião do Comitê.