RESOLUÇÃO Nº 04, DE 14 DE MARÇO DE 2018

Dispõe sobre a Política de Segurança da Informação (PSI) da UFT.

O Egrégio Conselho Universitário (Consuni) da Universidade Federal do Tocantins (UFT), reunido em sessão ordinária no dia 14 de março de 2018, no uso de suas atribuições legais e estatutárias,

RESOLVE:

Art. 1° Aprovar a Política de Segurança da Informação (PSI) da UFT, conforme anexo a esta Resolução.

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

LUÍS EDUARDO BOVOLATO
Reitor

EMC

UNIVERSIDADE FEDERAL DO **TOCANTINS**

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) DA UFT.

Anexo da Resolução n° 04/2018 - Consuni
Aprovado pelo Conselho Universitário em 14 de março de 2018.

Palmas/TO
2018

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) DA UFT.

1. ORIGEM

Comitê Gestor de Tecnologia da Informação – CGTI.

2. REFERÊNCIA LEGAL E NORMATIVA

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

II. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III. Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

IV. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e demais normativas complementares;

V. ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos;

VI. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

3. CAMPO DE APLICAÇÃO

Esta Política de Segurança da Informação se aplica no âmbito da Fundação Universidade Federal do Tocantins (UFT).

4. FUNDAMENTO LEGAL DA POLÍTICA DE SEGURANÇA

Conforme o 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.

5. INSTÂNCIAS ADMINISTRATIVAS

5.1. Comitê Gestor de Tecnologia da Informação (CGTI): comitê responsável por apreciar e aprovar o Plano Estratégico de Tecnologia da Informação (PETI), o Plano Diretor de Tecnologia da Informação (PDTI) e a Política de Segurança da Informação (PSI) e demais normativas a esta última relacionadas ao disposto no Plano de Desenvolvimento Institucional (PDI) e Plano Estratégico Institucional (PEI);

5.2. Diretoria de Tecnologia da Informação (DTI): órgão executivo da Reitoria, que planeja, dirige, avalia e executa as políticas de tecnologia da informação (TIC) em toda a Instituição, em articulação com as Pró-Reitorias e as Direções Gerais dos Câmpus;

5.3. Núcleo de Tecnologia da Informação (NTI): setor formalmente instituído em um Câmpus ou Reitoria da UFT que é responsável pela manutenção local dos recursos e preservação da aplicação das políticas, diretrizes e regulamentações na área de informática e telecomunicações.

6. TERMOS E DEFINIÇÕES

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

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

6.3. 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;

6.4. 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.

6.5. Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante pra a segurança da informação [ISO/IEC TR 18044:2004];

6.6. 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];

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

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

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

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

6.11. Politica 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;

6.12. 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;

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

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

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

6.16. 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;

6.17. Politica de gerenciamento de incidentes - politica 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;

6.18. Política 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.

6.19. 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 política de recuperação viáveis e garantir a continuidade de fornecimento dos serviços.

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

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

6.22. 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;

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

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

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

6.26. Usuário interno: qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente à UFT;

6.27. Usuário externo: qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente à UFT;

6.28. Comunicação oficial: tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas da UFT, de atividades especiais ou ainda de projetos específicos;

6.29. 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.

7. PRINCÍPIOS

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

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

7.2. Integridade: somente operações de alteração, supressão e adição autorizadas pela UFT devem ser realizadas nas informações.

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

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

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

8. ESCOPO

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

8.1. Aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos demais documentos normativos que as incorporarão;

8.2. Aos requisitos de segurança humana;

8.3. Aos requisitos de segurança física;

8.4. Aos requisitos de segurança lógica;

8.5. À sustentação dos procedimentos, dos processos de trabalho e dos ativos que influirão diretamente nos produtos e serviços oriundos da informação e comunicação da UFT.

9. ESTRUTURA DA PSI

A PSI da UFT é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

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

9.2. Normativas de Segurança da Informação (Normativas): 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 Normativa será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normativas 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).

9.3. Procedimentos de Segurança da Informação (Procedimentos): instrumentalizam o disposto nas Normativas, permitindo a direta aplicação nas atividades da UFT, 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.

10. COMPETÊNCIAS E RESPONSABILIDADES

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

10.1.1. A autoridade máxima é o Reitor, responsável pela aprovação da Política de Segurança da Informação da UFT;

10.1.2. Ao Comitê Gestor da Tecnologia da Informação compete:

10.1.3. Propor, aprovar e implantar políticas, normativas e procedimentos gerais relacionados à segurança da informação;

10.1.4. Estabelecer diretrizes e oferecer suporte às iniciativas de segurança da informação na UFT;

10.1.5. Propor iniciativas para a melhoria contínua das medidas de proteção;

10.1.6. Apoiar a implantação de soluções para eliminação ou minimização de riscos;

10.1.7. Estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança;

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

10.1.9. Acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação;

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

10.1.11. Executar outras funções que, por sua natureza, lhe estejam afetas ou lhe tenham sido atribuídas.

10.2. Para fins de regulamentação de suas atividades, o Comitê de Gestor de Tecnologia da Informação e Comunicações poderá ter regulamento próprio, o qual deverá ser aprovado pelo Conselho Superior da UFT.

10.3. O Comitê Gestor de Tecnologia da Informação e o Comitê de Segurança da Informação e Comunicações serão compostos por:

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

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

III - Coordenadores de Gestão de Tecnologia da Informação dos câmpus ;

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

11. DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

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

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

11.2. As áreas deverão submeter suas propostas de normativas ao “Comitê Gestor de Segurança da Informação” para análise, discussão e aprovação no âmbito do Comitê;

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

12. DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação da UFT, devem ser direcionados ao Comitê Gestor de Tecnologia da Informação.

13. VIOLAÇÕES, PENALIDADES E SANÇÕES

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

a) Na Lei nº 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;

b) No Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171/1994;

c) No Código Penal, através do Decreto-Lei nº 2848/1940;

d) Da Lei 8159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

e) No Decreto nº 4553/2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

14. REVISÕES E ATUALIZAÇÃO

Esta PSI será revista e alterada sempre que as atribuições e normativas da UFT justificar tais alterações, sendo ainda obrigatória a sua revisão anual.

15. VIGÊNCIA

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

NORMATIVA PARA USO DO CORREIO ELETRÔNICO INSTITUCIONAL

1. ORIGEM

Comitê Gestor de Tecnologia da Informação – CGTI.

2. REFERÊNCIA LEGAL E NORMATIVA

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

II. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III. Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

IV. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e demais normativas complementares;

V. ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos;

VI. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

3. CAMPO DE APLICAÇÃO

Esta Normativa de Segurança da Informação se aplica no âmbito da Fundação Universidade Federal do Tocantins (UFT).

4. OBJETIVOS GERAIS

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

5. FUNDAMENTAÇÃO LEGAL E NORMATIVA.

Conforme disposto na PSI compete ao CGTI da UFT determinar critérios para uso seguro e direcionado dos recursos computacionais dentro e fora do domínio de rede da UFT.

6. DO DOMÍNIO

6.1. Todos os usuários dos serviços de correio eletrônico da UFT estarão inscritos no domínio uft.edu.br;

6.2. O domínio uft.edu.br será utilizado apenas para contas de correio eletrônico.de cunho institucional.

7. DO CORREIO ELETRÔNICO

7.1. Os serviços de correio eletrônico são oferecidos como um recurso para apoiar discentes, docentes e servidores técnico-administrativos no cumprimento de suas atribuições nas áreas de administração, ensino, pesquisa, extensão, comunicação e serviços;

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

7.3. O uso pessoal do correio eletrônico institucional não é priorizado, sendo permitido desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas atividades ou viole qualquer outra lei ou normativa vigente na UFT;

7.4. É vetado o uso de correio eletrônico nos seguintes casos:

a) produção ou transmissão de dados ou materiais considerados ilegais, entre outros, por caracterizarem: transgressão dos direito do autor, de proteção à criança e ao meio-ambiente; atentado à privacidade ou promoção à discriminação racial ou religiosa;

b) veiculação de propaganda comercial, política ou religiosa;

c) uso em atividades estritamente comerciais;

d) atividades que contribuam para ineficiência ou esgotamento dos recursos na rede sejam eles computacionais, comunicacionais ou humanos;

e) atividades que promovam a corrupção ou destruição de dados de usuários;

f) atividades que interrompam ou prejudiquem a utilização dos serviços de rede por outros usuários;

7.5. A UFT, 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;

7.6. Mensagens encadeadas (corrente), para fins deste item, são mensagens enviadas a certo número de pessoas pedindo para que cada uma delas retransmita para outras pessoas a mesma mensagem com o mesmo pedido e é considerada uma violação desta normativa de uso;

7.7. A concessão de uma conta de e-mail não atribui ao usuário poder de representação da UFT.

8. DA PRIVACIDADE DAS MENSAGENS DE CORREIO ELETRÔNICO

8.1. Os e-mails, na condição de arquivos armazenados ou gerados com os recursos de TIC para fins produtivos, também são de propriedade da UFT e, portanto, passíveis de auditorias;

8.2. A auditoria a que faz referência o caput deste item destina-se exclusivamente à manutenção da segurança da infraestrutura de TIC, bem como a resguardar os objetivos da Instituição;

8.3. 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;

8.4. À DTI fica assegurado o direito de, em casos nos quais a segurança dos recursos de TIC da Instituição seja ameaçada, eliminar e-mails e arquivos, bloquear conteúdos e usuários, temporariamente ou permanentemente;

8.5. Pedidos de auditoria devem ser encaminhados ao Setor de Auditoria Interna;

9. DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação da UFT, Comitê Gestor de Tecnologia da Informação.

10. REVISÕES E ATUALIZAÇÃO

Esta Normativa da PSI será revista e alterada sempre que as atribuições e normativas da UFT justificar tais alterações.

11. VIGÊNCIA

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

NORMATIVA PARA GESTÃO DE SENHAS

1. ORIGEM

Comitê Gestor de Tecnologia da Informação – CGTI.

2. REFERÊNCIA LEGAL E NORMATIVA

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

II. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III. Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

IV. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e demais normativas complementares;

V. ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos;

VI. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

3. CAMPO DE APLICAÇÃO

Esta Normativa de Segurança da Informação se aplica no âmbito da Fundação Universidade Federal do Tocantins (UFT).

4. OBJETIVOS GERAIS

Estabelecer critérios geração e manutenção de senhas de usuários da UFT.

5. FUNDAMENTAÇÃO LEGAL E NORMATIVA.

Conforme disposto na PSI compete ao CGTI da UFT determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede da UFT.

6. GESTÃO DE SENHAS

6.1. O gerenciamento de senhas constitui o mecanismo básico para a autenticação de usuários dos sistemas computacionais integrados da UFT;

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

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

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

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

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

6.5. Em caso de esquecimento da senha uma senha temporária pode ser fornecida, não sendo tecnicamente possível a recuperação da senha anterior. A troca de senha temporária é obrigatória na primeira autenticação.

7. DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação da UFT, devem ser direcionados ao Comitê Gestor de Tecnologia da Informação.

8. REVISÕES E ATUALIZAÇÃO

Esta Normativa da PSI será revista e alterada sempre que as atribuições e normativas da UFT justificar tais alterações.

9. VIGÊNCIA

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

NORMATIVA PARA GESTÃO DE SISTEMAS

1. ORIGEM

Comitê Gestor de Tecnologia da Informação – CGTI.

2. REFERÊNCIA LEGAL E NORMATIVA

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

II. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III. Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

IV. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e demais normativas complementares;

V. ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos;

VI. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

3. CAMPO DE APLICAÇÃO

Esta Normativa de Segurança da Informação se aplica no âmbito da Fundação Universidade Federal do Tocantins (UFT).

4. OBJETIVOS GERAIS

Estabelecer critérios que envolvem aquisição, desenvolvimento e manutenção de sistemas de informação no âmbito da UFT.

5. FUNDAMENTAÇÃO LEGAL E NORMATIVA.

Conforme disposto na PSI compete ao CGTI da UFT determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede da UFT.

6. DA SOLICITAÇÃO

6.1. Todo projeto de sistema de informação antes da sua concepção, inclusive aquele desenvolvido pelo usuário, deve ser submetido à área de TI correlata para

avaliação/homologação dos aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

6.2. Os sistemas de informação classificados como críticos deverão ser desenvolvidos levando em consideração requisitos para sua contingência.

6.3. Todos os usuários que utilizarão um sistema devem ser treinados e capacitados para exercer suas atividades.

7. REQUISITOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

7.1. Devem ser considerados requisitos de segurança na definição ou aquisição de novos sistemas.

7.2. Devem ser considerados requisitos de segurança em todas as fases de criação dos sistemas, ou seja, definição, projeto, desenvolvimento, implantação e manutenção.

8. PROCESSAMENTO CORRETO NAS APLICAÇÕES

8.1. Devem ser incorporados controles apropriados em projetos de aplicações para assegurar o processamento correto.

8.2. Os controles devem incluir os dados de entrada, o processamento interno e os dados de saída.

8.3. Controles adicionais para sistemas que processem informações sensíveis, valiosas ou críticas ou que nessas exerçam algum impacto devem ser determinados com base em requisitos de segurança e análise/avaliação de riscos.

8.4. Os dados de entrada de aplicações devem ser validados para garantir que são corretos e apropriados.

8.5. Devem ser incorporadas nas aplicações checagens de validação com o objetivo de detectar qualquer corrupção de informações por erros ou por ações deliberadas.

8.6. Devem ser identificados e implementados requisitos e controles apropriados para garantir a autenticidade e proteger a integridade das mensagens em aplicações.

8.7. Devem ser validados os dados de saída das aplicações para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.

8.8. A utilização dos recursos e as projeções feitas para a necessidade de capacidade futura devem ser monitoradas de modo a garantir o desempenho requerido do sistema de informação.

9. CONTROLES CRIPTOGRÁFICOS

9.1. Devem ser elaboradas e implementadas políticas de uso de criptografia nos sistemas.

9.2. Devem ser armazenadas em servidores de rede com nível de segurança elevado as chaves utilizadas nas soluções de criptografia.

10. SEGURANÇA DOS ARQUIVOS DO SISTEMA

10.1. Devem ser documentos os procedimentos para a instalação e atualização de softwares.

10.2. A massa de dados utilizados nos testes da fábrica de software deve ser diferente da utilizada no ambiente de produção.

10.3. O acesso aos códigos fontes dos sistemas deve ser controlado e autorizado pela área de TI correlata.

11. SEGURANÇA EM PROCESSO DE DESENVOLVIMENTO E DE SUPORTE

11.1. Deve ser documentado e implementado um processo de gestão de mudanças.

11.2. A área de TI correlata deve supervisionar o processo desde o seu planejamento até a implementação no caso de desenvolvimento de softwares por terceiros.

11.3. Deve ser implementado controle de versão para garantir a gestão dos códigos fontes.

11.4. Deve ser realizada a análises de riscos a fim de detectar falhas nos sistema que possam comprometer a segurança da informação.

11.5. O suporte dos sistemas somente poderá ser realizado após abertura de chamado (para registro dos eventos).

11.6. Devem ser protegidas as informações envolvidas em transações online, a fim de prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.

12. GESTÃO DE VULNERABILIDADES TÉCNICAS

12.1. Devem ser investigado e tratado de forma contínua as vulnerabilidades técnicas dos sistemas de informação em uso.

12.2. Devem ser avaliada e implementada medidas apropriadas para lidar com os riscos associados a uma eventual vulnerabilidade.

13. DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação e Comunicações da UFT, devem ser direcionados ao Comitê Gestor de Tecnologia da Informação.

14. REVISÕES E ATUALIZAÇÃO

Esta Normativa da PSI será revista e alterada sempre que as atribuições e normativas da UFT justificar tais alterações.

15. VIGÊNCIA

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

NORMATIVA DE SUBSTITUIÇÃO E ATUALIZAÇÃO TECNOLÓGICA DE COMPUTADORES

1. ORIGEM

Comitê Gestor de Tecnologia da Informação – CGTI.

2. REFERÊNCIA LEGAL E NORMATIVA

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

II. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III. Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

IV. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e demais normativas complementares;

V. ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos;

VI. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

3. CAMPO DE APLICAÇÃO

Esta Normativa de Segurança da Informação se aplica no âmbito da Fundação Universidade Federal do Tocantins (UFT).

4. OBJETIVOS GERAIS

4.1. A Normativa de Substituição e Atualização Tecnológica de Computadores visa garantir ao Ensino, Pesquisa, Extensão e Gestão da UFT a infraestrutura de tecnologia adequada para seu melhor funcionamento, de acordo com os recursos disponíveis.

4.2. A Normativa busca estabelecer uma métrica, que consolida diversos fatores, para aquisição e substituição dos computadores no âmbito da UFT. A política de atualização da UFT oferece acesso à alta tecnologia de *hardware* e *software* disponíveis no mercado.

4.3. As atualizações dos computadores são periódicas. Os equipamentos a serem aplicados na substituição terão origem em: a) aquisições de equipamentos novos; e b) remanejamento de Laboratórios Específicos (subitem 2.2) e de Departamentos Administrativos (subitem 2.3).

4.4. A meta é substituir anualmente os computadores com aquisição superior a 9 anos, nivelando a idade média do parque tecnológico. Assim, o parque tecnológico é completamente atualizado a cada ciclo de nove anos.

4.5. O quantitativo de equipamentos entregue a cada Campus, para substituição, deve equivaler ao montante de computadores e monitores em uso com data de aquisição superior a 9 (nove) anos, não incluindo nessa permuta dispositivos que não estejam sendo utilizados (sucatas e/ou outros inservíveis).

4.6. Esta Normativa tem por intento a atualização do parque. As ampliações e/ou alterações dos parques devem ser adquiridas valendo-se de outros instrumentos.

5. DA ATUALIZAÇÃO DO PARQUE TECNOLÓGICO POR ÁREA

5.1. **Laboratórios de Informática (Labins)**:

5.1.1. A UFT possui Laboratórios de Informática (Labins) de uso geral com uma fração significativa de microcomputadores, distribuídos em 7 câmpus. Os equipamentos são utilizados nas atividades práticas nos cursos de graduação, pós-graduação, pesquisa, extensão e gestão.

5.1.2. Parte das aquisições anuais de equipamentos é destinada aos Labins da UFT.

5.1.3. No âmbito interno do Labin, o critério de atualização é definido pelo tempo de uso dos equipamentos. Assim, serão substituídos os computadores que estão em uso há mais tempo.

5.2. **Laboratórios Específicos**:

5.2.1. Compreende Laboratórios Específicos aqueles em que as atividades desenvolvidas no mesmo demandem maior desempenho das máquinas, com uma necessidade de processamento elevada, maior capacidade de armazenamento ou de processamento de imagens (Ex.: edição e manipulação de vídeos), ou sistema operacional diferenciado dos demais Labins, que atendam especialmente a um número significativamente pequeno comparado ao montante de cursos ofertados pelo Câmpus.

5.2.2. A UFT possui Laboratórios de Específicos destinados a atender a diversos cursos munidos com uma parcela expressiva de equipamentos de Tecnologia da Informação que visão suprir as necessidades desses cursos espalhados em todos os câmpus da Universidade.

5.2.2.1. O CGTI pode qualificar outros laboratórios como Específico, sempre que preenchido o perfil “alto desempenho”.

5.2.3. As atualizações e aquisições dos computadores são periódicas e mediante demanda advinda dos Câmpus/Reitoria. Assim, somente será instruída a aquisição quando, tempestivamente, for demandado, uma vez, que é necessário apresentar a especificação mínima necessária para o desempenho da atividade.

5.2.4. Como a aquisição é específica e determinada, o equipamento será entregue ao responsável pelo Laboratório Específico, que deverá substituir o equipamento com maior tempo de uso ou em pior estado, nesse último caso, quando descoberto de garantia.

5.2.4.1. Os equipamentos em questão não poderão ser substituídos em tempo de uso inferior a nove anos.

5.3. **Departamentos Administrativos**:

5.3.1. A UFT possui, vários Departamentos Administrativos com elevado quantitativo de microcomputadores, distribuídos em 7 câmpus, além da Reitoria. Os equipamentos em questão atendem nas atividades administrativas e de gestão da UFT.

5.3.2. As atualizações dos computadores são periódicas. Todo ano equipamentos são adquiridos e, parte deles, destinados aos serviços administrativos da instituição.

5.3.3. A atualização tecnológica dos setores administrativos deverá possuir como critério o tempo de uso dos equipamentos, salva guarda nos casos de demandas especificas por desempenho. Assim, serão substituídos os computadores mais antigos.

5.3.4. O CGTI, na oportunidade de aplicar a prioridade prevista neste item, deverá observar, sempre que possível, as seguintes dimensões:

5.3.4.1. Estratégica: alocação de equipamento que melhor atenda aos serviços educacionais da instituição.

5.3.4.2. Técnica: levar em consideração o tempo de uso do equipamento; porcentagem de uso de recursos de processamento; capacidade de armazenamento; acesso à rede; demanda de manutenções corretivas; e uso de energia elétrica.

6. DA EXPANSÃO

6.1. A expansão da infraestrutura de TI deve ser prevista no Plano de Desenvolvimento Institucional (PDI/UFT), no Plano Diretor de Tecnologia da Informação (PDTI/UFT) e no Plano de Distribuição Orçamentária (PDO/UFT).

6.2. As expansões (diferentemente das aquisições para atualização tecnológica) visam atender a novos postos de trabalho, seja por novas contratações de servidores, seja por criação de novos cursos e laboratórios.

6.3. Após aprovação dos respectivos projetos, a necessidade de expansão deve ser encaminhada ao CGTI/UFT que irá deliberar sobre as configurações de *hardwares* e *softwares* necessárias, bem como o projeto de implantação, e encaminhará para o Grupo de Compra de TI.

7. DISPOSIÇÕES FINAIS

7.1. Cabe a Administração de cada Campus definir a área prioritária de substituição dos novos equipamentos, contudo o CGTI aconselha o atendimento inicial a setores de impacto crítico da instituição.

7.2. O CGTI recomenda a prática da troca rotativa, onde os setores ou serviços com atividades cruciais que necessitam de carga de processamento reforçada são preferenciais, os equipamentos oriundos dessa troca são passados para setores menos críticos, desde que apresentem condições de uso, e assim sucessivamente, mantendo o parque em constante atualização.

7.3. Considerando as atribuições previstas no art. 3º, IV, do Regimento Interno CGTI/UFT (Resolução CONSUNI n. 06, de 15.07.2015), somente o CGTI poderá propor revisão total ou parcial dessa POSATEC.

7.4. Os pedidos deverão ser encaminhados pelo interessado à Secretária Executiva do Comitê.

7.5. As dúvidas suscitadas na aplicação destas normas serão resolvidas pelo Presidente do CGTI/UFT.

8. REVISÕES E ATUALIZAÇÃO

Esta Normativa da PSI será revista e alterada sempre que as atribuições e normativas da UFT justificar tais alterações.

9. VIGÊNCIA

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

NORMATIVA DE USO DOS RECURSOS DE REDES

1. ORIGEM

Comitê Gestor de Tecnologia da Informação – CGTI.

2. REFERÊNCIA LEGAL E NORMATIVA

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

II. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III. Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

IV. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e demais normativas complementares;

V. ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos;

VI. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

3. CAMPO DE APLICAÇÃO

Esta Normativa de Segurança da Informação se aplica no âmbito da Fundação Universidade Federal do Tocantins (UFT).

4. OBJETIVOS GERAIS

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

5. FUNDAMENTAÇÃO LEGAL E NORMATIVA

Conforme disposto na PSI compete ao CGTI da UFT determinar critérios para uso seguro e direcionado dos recursos computacionais dentro e fora do domínio de rede da UFT.

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

O uso dos recursos de tecnologia da informação providos pela UFT devem observar os seguintes critérios:

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

6.2. Os recursos de Tecnologia da Informação e Comunicações (TIC) devem ser utilizados de maneira responsável, consistente com objetivos educacionais, de ensino, de pesquisa, extensão e finalidades administrativas da UFT.

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

6.4. 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.

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

6.5.1. Respeitar as políticas, normativas e procedimentos de uso dos recursos de TIC da UFT.

6.5.2. Exibir a comprovação de vínculo com a UFT 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.

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

6.5.4. 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;

6.5.5. Manter sigilo sobre sua conta e senha, salvo em casos específicos para os quais exigirem autorização expressa e por escrito do responsável pela Diretoria de Tecnologia da Informação.

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

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

6.5.8. Não tentar, permitir ou causar qualquer alteração ou dano aos ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na UFT, de sua propriedade ou sob sua responsabilidade;

6.5.9. Não ligar ou desligar fisicamente ou eletricamente um recurso de TIC, nenhum componente externo, como cabos, access points, impressoras, discos ou sistemas de vídeo, sem uma autorização específica emitida pela DTI ou NTI;

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

6.6. Constituem responsabilidades dos Administradores de TIC (Diretor, Coordenadores) da UFT:

6.6.1. Proteger os direitos dos usuários;

6.6.2. Propor políticas e normativas de segurança e uso dos recursos de TIC;

6.6.3. Controlar e, se for o caso, vetar o acesso ao usuário que violar as normativas de uso de recursos de TIC;

6.6.4. Garantir prioridade de acesso via rede aos serviços essenciais da Universidade, mesmo que para isto tenha que limitar banda para acesso a outros serviços;

6.7. A UFT caracteriza como não ético e considera como motivo de ação disciplinar, qualquer atividade através da qual um usuário:

6.7.1. Não observe estritamente os objetivos institucionais.

6.7.2. Interfira no uso correto dos recursos de informação.

6.7.3. Tente conseguir ou consiga acesso não autorizado a recursos de informação.

6.7.4. Sem autorização administrativa, destrua, altere, desmonte, desconfigure, impeça o acesso de direito ou interfira na integridade dos recursos de TIC.

6.7.5. 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.

6.7.6. Remova dos recursos computacionais da UFT algum documento de sua propriedade ou por ela administrado, sem uma autorização específica.

6.7.7. 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.

6.7.8. 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.

6.7.9. Intercepte ou tente interceptar transmissão de dados não destinados ao seu próprio acesso.

6.7.10. 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.

6.7.11. Obtenha benefícios financeiros ou de outra espécie, para si ou para terceiros através da utilização dos recursos de TIC da UFT.

6.8. 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 da UFT poderão suspender temporariamente qualquer conta, seja o responsável pela conta suspeita de alguma violação, ou não.

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

7. DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação e Comunicações da UFT, devem ser direcionados ao Comitê Gestor de Tecnologia da Informação.

8. REVISÕES E ATUALIZAÇÃO

Esta Normativa da PSI será revista e alterada sempre que as atribuições e normativas da UFT justificar tais alterações.

9. VIGÊNCIA

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