SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DA AMAZÔNIA
COMITÊ EXECUTIVO DE TECNOLOGIA DA INFORMAÇÃO
Avenida Presidente Tancredo Neves, 2501 – Terra Firme
CEP: 66077-530-Caixa Postal, 917-Belém – Pará
Tel.: (91) 3210-5165/3210-5166

ATO DO COMITÊ EXECUTIVO DE TECNOLOGIA DA INFORMAÇÃO: RC – Resolução do CETI

Resolução n°. 07, de 04 de julho de 2014.

APROVA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA UNIVERSIDADE FEDERAL RURAL DA AMAZÔNIA – UFRA.

O Vice Reitor da Universidade Federal Rural da Amazônia, Professor Paulo de Jesus Santos, no exercício da presidência do Comitê Executivo de Tecnologia da Informação, no uso das atribuições legais e estatutárias, e de acordo com a deliberação deste Conselho na 2ª Reunião Extraordinária de 04 de Julho de 2014, com base no que consta da respectiva Ata, resolve expedir a presente,

RESOLUÇÃO

Art. 1° Aprovar a Política de Segurança da Informação e Comunicações da Universidade Federal Rural da Amazônia – UFRA.

Art. 2° Revogam-se as disposições em contrário.

Art. 3° Esta Resolução entra em vigor na data de sua publicação no site da UFRA.

Belém, 04 de julho de 2014.

Prof. Paulo de Jesus Santos
Vice Reitor no exercício da Presidência do CETI/UFRA

SERVIÇO PÚBLICO FEDERAL

UNIVERSIDADE FEDERAL RURAL DA AMAZÔNIA

RESOLUÇÃO CETI Nº 07, DE 04 DE JULHO DE 2014.

Dispõe sobre a Política de Segurança da Informação e Comunicações da Universidade Federal Rural da Amazônia - UFRA.

CONSIDERANDO:

O normativo disposto na Lei nº 9.983, de 14 de julho de 2000 – que altera o Código Penal relativamente aos crimes eletrônicos contra a administração pública; na Medida Provisória nº 2.200-2, de 24 de agosto de 2001 – que institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e transforma o Instituto Nacional de Tecnologia da Informação (IT) em autarquia; no Decreto nº 3.505, de 13 de junho de 2000 – que institui a Política de Segurança da Informação nos órgão e entidades da Administração Pública Federal; no Decreto nº 3.996, de 31 de outubro de 2001 – que dispõe sobre a prestação de serviços de Certificação Digital no âmbito da Administração Pública Federal ; no Decreto nº 7.845, de 14 de novembro de 2012 – que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento; na Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 e normas complementares – que disciplinam a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal direta e indireta e a Estratégia Geral de Tecnologia da

Informação – EGTI 2011-2012 do Ministério do Planejamento, Orçamento e Gestão – Secretaria de Logística e Tecnologia da Informação – SLTI;

Esse documento orienta a Reitoria da UFRA no estabelecimento de uma política clara de segurança da informação, alinhada com os objetivos do negócio, com demonstração de seu apoio e comprometimento com a segurança da informação por meio da publicação, manutenção e divulgação da política para toda a Universidade.

DEFINIÇÃO:
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:

Conforme definição dada pela norma ABNT NBR ISO/IEC 27002:2005, "*A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.*"

De acordo com a mesma norma, "***Segurança da informação*** *é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.*".

Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:

a) Integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações;
b) Confidencialidade: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação;
c) Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Ainda de acordo com a norma ABNT NBR ISO/IEC 27002:2005, *"A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.".*

A Política de Segurança da Informação é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações, sendo sua elaboração essencial, pois nela são definidas as normas, procedimentos, ferramentas e responsabilidades para garantir o controle e a segurança da informação na Instituição.

A Política de Segurança da Informação é apenas a formalização dos anseios da Instituição quanto à proteção das informações e pode ser comparada com uma legislação que todos devem conhecer, de modo que o cumprimento desta nos assegure um padrão de conduta que deve ser respeitado. Por oportuno, este instrumento deve ser seguido por todos os servidores técnico-administrativos, prestadores de serviço, docentes, discentes e comunidade externa da Instituição garantindo assim a proteção da informação classificada e o sucesso do cumprimento da missão institucional da UFRA.

CLASSIFICAÇÃO DA INFORMAÇÃO

Segundo descrição do item 5.2 da NBR ISO 17799, que trata da classificação da informação, o objetivo da Classificação da Informação é assegurar que os ativos da informação recebam um nível adequado de proteção. A informação deve ser classificada para indicar a importância, a prioridade e o nível de proteção. A informação possui vários níveis de sensibilidade e criticidade. Desta forma, esse instrumento propõe a seguinte classificação:

- **Confidencial**

  Estas informações devem ficar restritas ao ambiente da Instituição, o acesso a esses sistemas e informações é feito de acordo com a sua estrita necessidade, ou seja, os usuários só podem acessá-las se estes forem fundamentais para o desempenho

satisfatório de suas funções na Instituição. A divulgação não autorizada dessa informação pode causar impactos de ordem legal, de imagem e operacional à UFRA, e ainda, sanções administrativas, civis e criminais aos servidores, prestadores de serviço, docentes, discentes e comunidade externa da Instituição. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por servidores, clientes e/ou fornecedores.

- **Interna**

  Essas informações não devem sair do âmbito da Instituição. Porém, se isto ocorrer as consequências não serão críticas, no entanto, podem denegrir a imagem da Instituição ou causar prejuízos indiretos não desejáveis. Pode ser acessada sem restrições por todos os servidores e prestadores de serviços da UFRA.

- **Públicas**

  Informações que a UFRA pode divulgar para o público em geral, incluindo clientes, fornecedores, imprensa, não possuem restrições para divulgação. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

Mediante tal embasamento e considerando o disposto em seu Plano Diretor de Tecnologia da Informação - PDTI, a Superintendência de Tecnologia da Informação e Comunicação – STIC, resolve propor a implantação da Política de Segurança da Informação - PoSIC, no âmbito da Universidade Federal Rural da Amazônia - UFRA, cuja estrutura e diretrizes são expressas neste documento.

OBJETIVO:

Seu propósito é formalizar o direcionamento estratégico acerca da gestão de segurança da informação na Instituição, estabelecendo as diretrizes a serem seguidas para implantação e manutenção da PoSIC, guiando-se, principalmente, pelos conceitos e orientações das normas ABNT ISO/IEC da família 27000.

CAPÍTULO I
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 1º Fica estabelecida a Política de Segurança da Informação e Comunicações da Universidade Federal Rural da Amazônia, também representada pela sigla PoSIC/UFRA contendo as diretrizes de segurança da informação e comunicações no âmbito da Instituição.

Parágrafo Único. As diretrizes estabelecidas na PoSIC/UFRA determinam as bases a serem seguidas pela UFRA à segurança dos recursos computacionais e as informações geradas na Universidade.

Art. 2º Entende-se como PoSIC/UFRA o conjunto de princípios que norteiam a gestão de segurança de informações e que devem ser observados pela comunidade acadêmica e demais usuários internos e externos que tiverem interação com os ativos de tecnologia da informação pertencentes à UFRA.

CAPÍTULO II
PRINCÍPIOS E DIRETRIZES GERAIS

Art. 3º Além de seguir todos os princípios que norteiam a Universidade a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

I - **Confidencialidade**: somente pessoas devidamente autorizadas pelo Comitê Executivo de TI – CETI devem ter acesso à informação armazenadas ou transmitidas por meio de redes de comunicações na UFRA.

II - **Integridade**: somente alterações, supressões e adições autorizadas pelo CETI devem ser realizadas nas informações.

III - **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre

que necessário ou demandado;

IV - **Autenticidade:** assegurar a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria.

Art. 4º São Diretrizes Gerais da Política de Segurança da Informação e Comunicações – PoSIC/UFRA:

I – Estabelecer procedimentos de uso aceitável dos serviços da rede corporativa;

II – Estabelecer os procedimentos e níveis de acesso a dados, informações e conhecimentos no âmbito da Instituição, nos limites necessários para atender a prestação de serviços;

III – Proteger todos os sistemas institucionais e as informações neles contidas contra acessos não autorizados;

IV – A integridade, disponibilidade, autenticidade, de todos os sistemas informatizados e a confiabilidade de qualquer informação contida dentro ou acessível por meio destes é de responsabilidade da Superintendência de Tecnologia da Informação e Comunicação (STIC), da Universidade;

V – Todas as violações de segurança a sistemas institucionais serão notificadas e investigadas pela Divisão de Sistemas de Informação – DSIN em conjunto com a Divisão de Suporte e Infraestrutura de Telecomunicações – DSIT da STIC;

VI – Todos os usuários têm a responsabilidade de relatar à STIC, qualquer incidente que poderá impactar na segurança da rede corporativa, sejam eles de mau uso, acesso não autorizado a sistemas e documentos e demais atividades que não dizem respeito às suas funções;

VII – Os usuários são responsáveis por adotar bom senso quanto ao uso pessoal dos recursos computacionais da Instituição.

VIII - Os servidores técnico-administrativos, prestadores de serviço, docentes da UFRA, devem

assumir uma postura proativa no que diz respeito à proteção das informações da UFRA e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade da UFRA;

IX - As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;

X - Assuntos confidenciais não devem ser expostos publicamente;

XI - Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;

XII - Somente softwares homologados podem ser utilizados no parque computacional da UFRA;

XIII - Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;

XIV - Todos os dados considerados como imprescindíveis aos objetivos da UFRA devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos a testes periódicos de recuperação;

XV - O acesso lógico a sistemas computacionais disponibilizados pela UFRA deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação, garantindo a rastreabilidade e a efetividade do acesso autorizado;

XVI - São de propriedade da UFRA todas as criações, códigos ou procedimentos desenvolvidos por qualquer servidor técnico-administrativo, prestadores de serviço, estagiário, docentes e discentes durante o curso de seu vínculo com a Instituição.

Art. 5º A PoSIC/UFRA, deverá ser revisada e atualizada em conformidade com normativas do Governo Federal.

CAPÍTULO II

DO ESCOPO

Art. 6º A presente PoSIC/UFRA, tem por objetivo estabelecer regras gerais para assegurar o sigilo, a integridade, a autenticidade e a disponibilidade de dados, informações no âmbito da Instituição, de modo a resguardar a legitimidade de sua atuação e contribuir para o cumprimento de suas atribuições legais, bem como preservar a imagem institucional.

Art. 7º O Escopo desta política engloba todos os sistemas de informação e comunicação de uso coletivo da Instituição e de suas unidades.

Art. 8º A elaboração desta Política está contemplada no PDTI da Instituição, e deverá ser complementada por Normas e Procedimentos que a referenciem na forma de anexos.

Parágrafo Único. Deverão ser elaboradas Normas específicas para:

1. Tratamento da Informação;
2. Tratamento de Incidentes de TI;
3. Gestão de Risco;
4. Gestão de Continuidade;
5. Auditoria e Conformidade;
6. Controles de Acesso;
7. Uso de correio eletrônico (e-mail);
8. Acesso à Internet e intranet;
9. Uso aceitável de recursos de TI.

Art. 9º Todos os recursos computacionais e de infraestrutura de rede gerenciados e supervisionados pela STIC bem como os dispositivos particulares de computação autorizados a se conectar à rede institucional estão sujeitos as regras deste documento.

Art. 10 A PoSIC/UFRA, alinha-se às estratégias da Universidade estabelecidas no Plano de Desenvolvimento Institucional - PDI, e no Plano Diretor de Tecnologia da Informação – PDTI.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 11 Para efeito da PoSIC/UFRA, ficam estabelecidos os significados dos seguintes termos e expressões:

I - **Ativo de Informação** – qualquer recurso que faça parte dos sistemas de informação e meios para geração de documentos que tenham valor para a UFRA;
II - **Ativo de Sistema** – patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução de sistemas e processos da UFRA;
III - **Ativo de Processamento** – patrimônio composto por todos os elementos de hardware, software, serviço, infraestrutura ou instalações físicas necessárias para a execução de sistemas e processos da UFRA, tanto aqueles produzidos internamente quanto os adquiridos pela Universidade;
IV - **Controle de Acesso** – restrições ao acesso às informações de um sistema informatizado exercido pela DSIN e DSIT;
V - **Custódia** – consiste na responsabilidade de se guardar um ativo para terceiros sem, contudo, permitir automaticamente o acesso ao ativo ou o direito de conceder acesso a outros;
VI - **Direito de Acesso** – privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;
VII - **Ferramentas** – conjunto de equipamentos, programas, procedimentos, normas e demais recursos por meio dos quais se aplica a Política de Segurança da Informação da UFRA;
VIII- **Incidente de Segurança** – qualquer evento ou ocorrência que promova uma ou mais ações que comprometa, ou que seja uma ameaça à integridade, autenticidade ou disponibilidade de qualquer ativo da UFRA;
IX - **Proteção dos Ativos** – processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade, sendo que o meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;
X - **Responsabilidade** – obrigações e deveres da pessoa que ocupa determinada função em relação ao acervo de informações.

XI - **Recursos de Tecnologia da Informação e Comunicação**: são todos os serviços computacionais disponibilizados aos usuários, como computadores, impressoras, programas, sistemas institucionais (acadêmico, administrativo e governamental), área de armazenamento de arquivos, serviço de internet, correio eletrônico, dentre outros;

XII - **Rede Corporativa:** conjunto de ativos de tecnologia disponível no âmbito da Instituição, seus campi e suas unidades, que permite a comunicação via rede aos diversos serviços de tecnologia da informação e comunicação.

XIII – **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independente do suporte em que resida ou da forma pela qual seja veiculado;

XIV – **Segurança da Informação**: proteção da informação contra ameaças para garantir a continuidade do negócio, minimizar os riscos e maximizar a eficiência e a efetividade das ações do negócio;

XV – **Incidente em Segurança da Informação**: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação.

XVI – **Usuário:** qualquer indivíduo que tenha acesso a informações e serviços produzidos ou custodiados pela Instituição.

CAPÍTULO IV
DA ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO

Art. 12 A estrutura normativa da Segurança da Informação da Instituição será composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

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

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

Procedimentos de Segurança da Informação (Procedimentos): instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da

Instituição.

CAPÍTULO V
APROVAÇÃO E REVISÃO

Art. 13 Os documentos integrantes da estrutura normativa da Segurança da Informação da Instituição deverão ser aprovados e revisados conforme os seguintes critérios:

Política
Nível de Aprovação: CETI, Reitor da UFRA
Periodicidade de Revisão: anual

Normas
Nível de Aprovação: CETI
Periodicidade de Revisão: anual

Procedimentos
Nível de Aprovação: CETI, STIC
Periodicidade de Revisão: anual

CAPÍTULO VI
DOS DEVERES E DAS RESPONSABILIDADES

Art. 14 É dever de todo usuário dos ativos de informação:

I. Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de tecnologia da informação (TI);
II. Cumprir a PoSIC/UFRA, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
III. Utilizar os Sistemas de Informações da UFRA e os recursos a ela relacionados somente para os fins previstos pelo CETI;
IV. Cumprir as regras, normas e procedimentos de proteção estabelecidos aos ativos de informação pelo CETI;
V. Responder por todo e qualquer acesso aos recursos de TI da UFRA, bem como pelos efeitos desses acessos efetivados através do seu código de identificação ou outro atributo

empregado para esse fim;

VI. Abster-se de utilizar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação à legislação de propriedade intelectual pertinente;

VII. Comunicar ao seu superior imediato qualquer irregularidade ou desvio.

Art. 15 Entendem-se como responsabilidades das Chefias as seguintes atividades:

I. Gerenciar o cumprimento da PoSIC/UFRA, por parte de seus servidores técnico-administrativos, prestadores de serviço e docentes;

II. Identificar os desvios praticados e adotar as medidas corretivas apropriadas;

III. Proteger, em nível físico e lógico, os ativos de informação e de processamento da UFRA relacionados com sua área de atuação;

IV. Garantir que o servidor sob sua supervisão compreenda e colabore para com a proteção dos ativos de informação da UFRA;

V. Solicitar à STIC a concessão de acesso privilegiado a usuários sob sua supervisão que podem acessar as informações em sistemas informatizados da unidade administrativa e acadêmica sob sua responsabilidade.

Parágrafo Único. Cada área que detém os ativos de processamento e de informação será responsável por esses ativos, provendo a sua proteção de acordo com as normas e procedimentos previstos na PoSIC/UFRA.

Art. 16 Entendem-se como responsabilidades da STIC da UFRA:

I. Estabelecer, em conjunto com o CETI, as regras de proteção dos ativos de informação da UFRA;

II. Decidir quanto às medidas a serem adotadas em caso de violação das regras estabelecidas, de acordo com as Normas e Procedimentos de Segurança da Informação vigentes;

III. Revisar, em conjunto com o CETI, periodicamente as políticas, normas e procedimentos de segurança da informação da UFRA;

IV. Elaborar e manter atualizado o Plano de Continuidade de Negócio da UFRA;

V. Executar as regras de proteção estabelecidas por esta Política de Segurança;

VI. Detectar, identificar, registrar e comunicar a Reitoria e ao Centro de Atendimento a

Incidentes de Segurança (CAIS) e/ou ao órgão responsável as violações ou tentativas de acesso não autorizadas;

VII. Fornecer acesso aos serviços de TI, mantendo-se o devido registro e controle.

Art. 17 Entendem-se como responsabilidades dos prestadores de serviço toda e qualquer ação prevista em contrato ou cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento da PoSIC/UFRA e suas normas e procedimentos.

CAPÍTULO VII
DAS PENALIDADES

Art. 18 A não observância aos dispositivos da PoSIC/UFRA, pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções educativas, administrativas, civis e penais, assegurados aos envolvidos, o contraditório e a ampla defesa.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 19 O CETI, em conjunto com as demais unidades da estrutura organizacional da Universidade, promoverá a comunicação e a ampla divulgação da norma de que trata esta Resolução, para que todos a conheçam e a cumpram no âmbito de suas atividades e atribuições.

Art. 20 Todos os usuários estão sujeitos ao cumprimento das regras gerais estabelecidas nesta documentação e deverão aderir a sua implementação em sua área de atuação.

Art. 21 Os processos de aquisição de bens e serviços relacionados à Tecnologia da Informação pela UFRA deverão estar em conformidade com este documento.

Art. 22 Revogam-se as disposições em contrário.

Art. 23 Os casos omissos serão resolvidos pelo CETI.

Art. 24 A presente Resolução entra em vigor na data de sua publicação.