ANEXO F: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (NTI/UFAL)

1. OBJETIVO

A Política de Segurança da Informação da Universidade Federal de Alagoas estabelece as diretrizes para a Segurança da Informação, visando preservar a integridade, a confidencialidade e a disponibilidade dos ativos de informação da Ufal, sendo o compromisso com o seu cumprimento de responsabilidade de todos os servidores, tanto efetivos como substitutos, temporários, colaboradores, consultores externos, estagiários, bolsistas e prestadores de serviços.

2. FUNDAMENTOS LEGAIS E NORMATIVAS

Referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação da Ufal.

a) Constituição Federal de 1988, reformada em 2008;
b) Lei nº 9.983, de 14 de julho de 2000 – Altera o Decreto Lei nº 2.848/40 – Código Penal – tipificação de crimes por computador contra a Previdência Social e a Administração Pública;
c) Decreto nº 1.171, de 24 de junho de 1994 – Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;
d) Lei nº 3.689, de 03 de outubro de 1941, atualizada até as alterações introduzidas pela Lei nº 11.900, de 08 de janeiro de 2009;
e) Lei nº 5.869, de 11 de janeiro de 1973;
f) Lei nº 7.232, de 29 de outubro de 1984 – Política Nacional de Informática, e dá outras providências;
g) Lei nº 8.027, de 12 de abril de 1990 – Normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências;
h) Lei nº 8.112, de 11 de dezembro de 1990 – Regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

    Lei nº 8.429, de 2 de junho de 1992 – 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, e dá outras providências;

i) Decreto nº 6.029, de 01 de fevereiro de 2007 – Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;

j) Lei nº 8.159, de 8 de janeiro de 1991 – política nacional de arquivos públicos e privados, e dá outras providências;

k) Decreto nº 7.579, de 11 de outubro de 2011 – Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp), do Poder Executivo Federal, e dá outras providências;

l) 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;

m) 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;

n) Normas e Resoluções do Gabinete de Segurança Institucional da Presidência da República:

   i. Instrução Normativa GSI nº 01, de 13 de junho de 2008;
   ii. Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 outubro de 2008;
   iii. Norma Complementar nº 03/IN01/DSIC/GSIPR, de 03 julho de 2009;
   iv. Norma Complementar nº 04/IN01/DSIC/GSIPR, de 17 agosto de 2009;
   v. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 agosto de 2009;
   vi. Norma Complementar nº 06/IN01/DSIC/GSIPR , de 23 novembro de 2009;

o) Acórdão nº 1.603/2008 do Plenário do Tribunal de Contas da União (TCU);

p) ABNT NBR ISO 17.799:2005 – Código de Práticas para a Gestão da Segurança da Informação;

q) ABNT NBR ISO Guia 73:2002 – Gestão de Riscos/Vocabulário;

r) ABNT NBR ISO/IEC 27.001:2005 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;

s) ABNT NBR ISO/IEC 27.002:2005 – Código de Prática para a Gestão de Segurança da Informação;

t) ISO/IEC TR 13.335-3:1998 – fornece técnicas para a gestão de segurança na área de Tecnologia da Informação. Baseada na norma ISO/I EC 13.335-1 e TR ISO/IEC 13.335-2;

u) ISO/IEC GUIDE 51:1999 – fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos;

v) Lei nº 12.527, de 18 de novembro de 2011 – regula o acesso a informações;

w) Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

3. TERMOS E DEFINIÇÕES

Para os efeitos desta política e das normas nela originadas, entende-se por:

a) **Ativo de Informação**: qualquer informação que tenha valor para a instituição [ISO/IEC 13.335-1:2004];

b) **Recursos de Tecnologia da Informação**: equipamento de Tecnologia da Informação e seus acessos, bem como também sistemas, serviços e infraestrutura;

c) **Segurança da Informação**: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas;

d) **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;

e) **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 18.044:2004];

f) **Incidente de Segurança da Informação**: indicado por um simples evento 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 18.044:2004];

g) **Risco**: combinação da probabilidade de ocorrência de um evento e de suas consequências;

h) **GRSIC**: Gestão de Riscos de Segurança da Informação e Comunicações;

i) **Ameaça**: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a instituição [ISO/IEC 13.335-1:2004];

j) **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

k) **PSI**: Política de Segurança da Informação;

l) **CTIR.GOV**: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República DSIC/GSI/PR;

m) **Custodiante do Ativo de Informação**: é aquele que, de alguma forma, zela pelo armazenamento, pela operação, pela administração e pela preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

a) **Confidencialidade**: devem ter acesso à informação não pública somente pessoas devidamente autorizadas pelo gestor da informação;

b) **Integridade**: devem ser realizadas nas informações somente operações de alteração, supressão e adição autorizadas pela Ufal;

c) **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;

d) **Autenticidade**: assegura ser do autor a responsabilidade pela criação ou pela divulgação de uma dada informação;

e) **Criticidade**: define a importância da informação para a continuidade da atividade-fim da instituição;

f) **Não-repúdio**: é a garantia de que o emissor da mensagem não irá negar, posteriormente, a autoria da mensagem ou transação, permitindo a sua identificação;

g) **Responsabilidade**: devem ser claramente definidas as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança. Todos os servidores da Ufal são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação e Comunicação advindas dessa política;

h) **Ciência**: devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições, sem comprometer a segurança, todos os servidores, colaboradores, consultores externos, estagiários, bolsistas e prestadores de serviço;

i) **Ética**: devem ser respeitados todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, bolsistas, prestadores de serviço e usuários do Sistema de Informação da Ufal;

j) **Legalidade**: levarão em consideração as ações de Segurança da Informação e Comunicação, além de observar os interesses da Ufal, leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e aos direitos de uso.

5. ESCOPO

O escopo do Plano de Segurança da Informação da Ufal refere-se:

a) aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos demais documentos normativos que as incorporarão;

b) aos requisitos de segurança humana;

c) aos requisitos de segurança física;

d) aos requisitos de segurança lógica;

e) à sustentação dos procedimentos, dos processos de trabalho e dos ativos que influirão diretamente nos produtos e serviços oriundos da informação e da comunicação da Ufal.

6. DIRETRIZES GERAIS

a) O zelo pela Segurança da Informação é dever de todos;

b) A Ufal, como usuária dos serviços providos pela Rede Nacional de Pesquisa (RNP), é, por princípio, signatária de suas Políticas e Normas de Segurança;

c) Compete à direção-geral do Núcleo de Tecnologia da Informação (NTI), com o apoio da Pró-Reitoria de Gestão de Pessoas (Progep) e das demais Pró-reitorias pertinentes, instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em Segurança da Informação e Comunicação, buscando parcerias com outros órgãos e entidades;

d) Os usuários internos e externos devem observar que:

   i. o acesso à informação será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Ufal é considerada seu patrimônio e deve ser protegida;

   ii. os recursos disponibilizados pela Ufal, de sua propriedade, são fornecidos com o propósito único de garantir o desempenho das suas atividades;

   iii. as normas para as operações de armazenamento, divulgação, reprodução, 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;

e) Um serviço de Gestão de Incidentes será estabelecido: consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências;

f) Um processo de Gestão de Riscos será estabelecido, contínuo e aplicado na implementação e na 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;

g) Os aspectos legais de segurança aos quais as atividades da Ufal estão submetidas, de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão, deverão ser levantados regularmente;

h) A criação de controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos da Ufal e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo a entrada e a saída de visitantes, pessoal interno, equipamentos e mídias e estabelecendo perímetros de segurança serão efetivados;

i) O serviço de correio eletrônico disponibilizado pela Ufal constitui recurso do Instituto disponibilizado na rede de comunicação de dados para aumentar a agilidade, a segurança e a economia da comunicação oficial e informal. O correio eletrônico constitui bem da Ufal e, portanto, passível de auditoria;

j) O acesso à Internet será concedido para todos os servidores, 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 e, portanto, passível de auditoria;

k) As informações, os sistemas e os métodos criados pelos servidores da Ufal, no exercício de suas funções, são patrimônios intelectuais da instituição, não cabendo a seus criadores qualquer forma de direito autoral, exceto em casos regulamentados pela área competente;

l) O Termo de Responsabilidade e Sigilo é documento oficial que compromete os servidores, colaboradores, terceirizados e prestadores de serviço com a Política de Segurança da Informação da Ufal;

m) Fica instituída a Estrutura de Gestão de Segurança da Informação e Comunicação da Ufal, composta pelo Comitê de Segurança da Informação e Comunicações (Csic) e pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Etir), que serão solidariamente responsáveis pelas seguintes atividades:

i. executar os Processos de Segurança da Informação e Comunicações;
ii. desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos da Ufal;
iii. avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação e desenvolver ações de conscientização dos usuários a respeito da implementação desses controles;
iv. fornecer subsídios visando à verificação de conformidade de segurança da informação e comunicações; e
v. promover a melhoria contínua nos processos e controles de Gsic;

n) Os membros da Estrutura da Gsic devem receber regularmente capacitação especializada nas disciplinas relacionadas à SIC, de acordo com suas funções;
o) A Gsic da Ufal deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da instituição e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências;
p) Os contratos firmados pela Ufal devem conter cláusulas que determinem a observância da PSI e seus respectivos documentos.

7. DIRETRIZES ESPECÍFICAS

Para cada uma das diretrizes constantes das seções deste capítulo, devem ser elaboradas normas táticas específicas, manuais e procedimentos.

7.1 Gestão de Ativos

7.1.1 Os ativos de informação devem:

a) ser inventariados e protegidos;
b) ter identificados os seus proprietários e custodiantes;
c) ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
d) ter a sua a entrada e saída nas dependências da Ufal autorizadas e registradas por autoridade competente;

e) ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

f) ser regulamentados por norma específica quanto à sua utilização; e

g) ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

7.1.2 O Gsic deve criar, gerir e avaliar critérios de tratamento e classificação da informação, de acordo com o sigilo requerido, a relevância, a criticidade e a sensibilidade, observando a legislação em vigor.

7.1.3 Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos e falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

7.1.4 Os sistemas de informação e as aplicações da Ufal devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

7.1.5 O acesso dos usuários aos ativos de informação e sua utilização, quando autorizado, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

7.2 Gestão de Riscos

7.2.1 O gestor dos ativos de informação deve estabelecer processos de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) que possibilitem identificar ameaças e reduzir vulnerabilidades e impactos dos ativos de informação.

7.2.2 A GRSIC é um processo contínuo e deve ser aplicada na implementação e na operação da Gestão de Segurança da Informação e Comunicações, levando em consideração o planejamento, a execução, a análise crítica e a melhoria da SIC na Ufal.

7.3 Segurança Física e do Ambiente

7.3.1 A entrada de pessoas em áreas de segurança deve ser controlada, para que apenas pessoas autorizadas tenham acesso.

7.3.2 O acesso às áreas de segurança, uma vez concedido deve ter registrado data e hora de entrada e saída de visitantes.

7.3.3 Fica proibido o consumo de comidas ou bebidas, ao se manipular algum ativo de informação, bem como ao se ter acesso a alguma área de segurança.

7.3.4 Em áreas de segurança, temperatura, umidade, poeira e gazes devem ser controlados por dispositivos automatizados e sob manutenção regular para garantir seu perfeito funcionamento.

7.3.5 A Estrutura de Gsic deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

7.3.6 As proteções devem estar alinhadas aos riscos identificados.

7.4 Gerenciamento das Operações e Comunicações

7.4.1 A Estrutura de Gsic deve estabelecer parâmetros adequados, relacionados à SIC, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais da Ufal. Os acordos de nível de serviço devem ser compatíveis com padrões de mercado e requisitos de segurança;

7.4.2 Deverá descrever procedimentos e responsabilidades operacionais, incluindo gestão de mudanças, segregação de funções e separação dos ambientes de produção, desenvolvimento e testes;

7.4.3 Deverá fornecer diretrizes para:

a) gerenciamento de serviços terceirizados;

b) planejamento e aceitação de sistemas;

c) proteção contra códigos maliciosos e móveis;

d) cópias de segurança;

e) gerenciamento da segurança em redes;

f) manuseio de mídias;

g) troca de informações;

h) serviços de correio eletrônico; e

i) monitoramento.

7.5 Controle de Acessos

7.5.1 Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações;

7.5.2 Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação;

7.5.3 Os usuários da Ufal são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico institucional e certificado digital;

7.5.4 A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento;

7.5.5 A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação;

7.5.6 Todos os sistemas de informação da Ufal, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações;

7.5.7 Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento da Ufal ou bloqueados em caso de afastamento;

7.5.8 Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que regrem o controle de acesso quanto:

a) ao acesso às suas bases de dados;

b) à extração, carga e transformação de dados; e

c) aos serviços acessíveis via linguagem de programação.

7.5.9 Os sistemas estruturantes devem possuir mecanismos automáticos para:

a) revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentadoria e falecimento do servidor;

b) bloquear as contas de acesso do servidor nos casos de licença, afastamento, cessão e disponibilidade do servidor; e

c) tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes na norma de controle de acesso ao sistema.

7.6 Aquisição, Desenvolvimento e Manutenção de Sistemas

7.6.1 A Estrutura de Gsic deve estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

7.6.2 O processo de aquisição de sistemas e aplicações corporativas deve atender a requisitos de segurança previstos em norma específica.

7.7 Gestão de Incidentes de Segurança da Informação

7.7.1 A Estrutura de Gsic deve instituir metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança, de forma a observar o disposto no arcabouço técnico normativo do CTIR.GOV.

7.7.2 Deve ser instituída a Equipe de Tratamento e Resposta a Incidentes de Segurança.

7.8 Gestão da Continuidade do Negócio

A Estrutura de Gsic deve instituir metodologias ou normas que estabeleçam a Gestão de Continuidade do Negócio.

7.9 Conformidade

7.9.1 Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SIC da Ufal e de suas unidades administrativas com esta PSI e suas normas e procedimentos complementares, bem como com a legislação específica de SIC.

7.9.2 A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a Ufal.

7.9.3 A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pela Estrutura de Gsic e aprovado pelo Csic.

7.9.4 O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

7.9.5 Nenhuma unidade administrativa poderá permanecer sem verificação de conformidade de suas práticas de SIC por período superior a 2 (dois) anos.

7.9.6 A execução da verificação de conformidade será realizada pela Estrutura de GSIC, podendo, com a prévia aprovação do Csic, ser subcontratada no todo ou em parte.

7.9.7 É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

7.9.8 A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, análise de tráfego de rede, entrevistas e testes de invasão.

7.9.9 Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de SIC ao Gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

8. COMPETÊNCIAS E RESPONSABILIDADES

8.1 Cabe ao Gestor de SIC

a) promover cultura de segurança da informação e comunicações;
b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
c) propor recursos necessários às ações de SIC;
d) coordenar o Csic e a Etir;
e) comunicar ao Csic os resultados e outras informações pertinentes;
f) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

g) manter contato direto com o Dsic/GSI/PR para o trato de assuntos relativos à segurança da informação e comunicações; e

h) propor normas relativas à SIC.

8.2 Cabe ao Csic

a) normatizar e supervisionar a SIC no âmbito da Ufal;

b) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

c) propor alterações na PSI;

d) solicitar apurações quando da suspeita de ocorrências de quebras de SIC;

e) avaliar, revisar e analisar criticamente a PSI e suas normas complementares, visando à sua aderência aos objetivos institucionais da Ufal e às legislações vigentes;

f) dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PSI da Ufal;

g) constituir grupo de trabalho para realizar verificações de conformidade;

h) aprovar o plano de investimentos em SIC da Ufal;

i) monitorar e avaliar periodicamente o plano de SIC, assim como determinar os ajustes cabíveis;

j) definir e atualizar seu Regimento Interno; e

k) baixar normas e procedimentos complementares a esta PSI.

8.3 Cabe à Etir

a) facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

b) promover a recuperação de sistemas;

c) agir proativamente, com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

d) realizar ações reativas, que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

e) analisar ataques e intrusões na rede da Ufal;

f) executar as ações necessárias para tratar quebras de segurança;
g) obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
h) cooperar com outras equipes de Tratamento e Resposta a Incidentes; e
i) participar em fóruns, redes nacionais e internacionais relativos à SIC.

8.4 Cabe ao Gestor de Ativo da Informação

a) garantir a segurança dos ativos de informação sob sua responsabilidade;
b) definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta PoSIC;
c) conceder e revogar acessos aos ativos de informação;
d) comunicar à Etir a ocorrência de incidentes de SIC; e
e) designar custodiante dos ativos de informação, quando aplicável.

8.5 Cabe ao Custodiante de Ativo da Informação

a) proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta PSI.

8.6 Cabe aos diretores de Unidades Acadêmicas e/ou Administrativas

a) corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua responsabilidade;
b) conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;
c) incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;
d) tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;
e) informar ao NTI a movimentação de pessoal de sua unidade, para que seus acessos sejam revistos;
f) realizar o tratamento e a classificação da informação;

g) autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;
h) comunicar à Etir os casos de quebra de segurança; e
i) manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

8.7 Cabe aos Terceiros e Fornecedores

a) tomar conhecimento desta PSI;
b) fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e
c) fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

8.8 Cabe aos Usuários

a) conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta PSI, bem como os demais normativos e resoluções relacionados à SIC;
b) obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação e fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades;
c) comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à Etir.

9. DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

a) A Política e os Regulamentos de Segurança da Informação devem ser divulgados a todos os servidores da Ufal, e dispostos de maneira que o seu conteúdo possa ser consultado a qualquer momento;
b) As áreas atingidas por esta Política são imediatamente responsáveis pela classificação da informação, elaboração e proposição de normas, procedimentos e atividades necessárias ao cumprimento;
c) As áreas deverão elaborar os seus regulamentos com base nas diretrizes propostas pelo “Comitê Gestor de Segurança da Informação”, submetendo-os para análise, discussão e aprovação no âmbito do Comitê;

d) Após aprovação, estas normas e procedimentos serão divulgados aos interessados pela área responsável por sua proposição e manutenção.

10. REVISÃO E ATUALIZAÇÃO

Esta Política será revista anualmente e alterada sempre que as atribuições e normas da Ufal justificarem tais alterações.

Modelo de referência: PoSIC do Ministério do Planejamento, Orçamento e Gestão Portaria MP nº 27, de 03/02/2012 (DOU 06/02/2012).

11. VIOLAÇÕES, PENALIDADES E SANÇÕES

Nos casos em que houver o descumprimento ou a violação de um ou mais itens da Política ou de seus regulamentos, procedimentos ou atividades pertinentes à Segurança da Informação, estes serão tratados conforme legislação, podendo também ser revogado o acesso aos ativos de informação na forma da lei vigente.

12. VIGÊNCIA

Esta política entra em vigor na data de sua publicação.