Política de Segurança da Informação (POSIC)

1 Fundamentação Legal

1.1 Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 (Disciplina a Gestão de Segurança da Informação e Comunicações)

1.2 LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011 (Regula o acesso a informações)

1.3 DECRETO No 3.505, DE 13 DE JUNHO DE 2000 (Institui a Política de Segurança da Informação)

1.4 Norma Complementar nº 03/IN01/DSIC/GSIPR (Diretrizes para elaboração da POSIC)

1.5 Decreto Nº 7.724, de 16 de maio de 2012 (Dispõe sobre o acesso a informações)

2 Disposições Preliminares

2.1 A Política de Segurança da Informação e Comunicação da Universidade Federal do Amapá (POSIC/UNIFAP) observará os princípios, objetivos e diretrizes estabelecidos nesta política, bem como às disposições constitucionais, legais e regimentais vigentes.

2.2 A POSIC/UNIFAP alinha-se às estratégias da Universidade e tem por objetivo garantir a **autenticidade, confidencialidade, disponibilidade e integridade** das informações produzidas ou custodiadas pela Universidade, através de ações que objetivam a criar e manter um ambiente seguro quanto ao uso dos recursos computacionais da Universidade Federal do Amapá (UNIFAP).

2.3 Define-se como **recursos computacionais** o conjunto de equipamentos de rede, telecomunicações, computadores, programas, banco de dados, sistemas e serviços administrados, mantidos e operados pela UNIFAP.

2.4 Para os efeitos desta POSIC, entende-se por:
I-Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculada;
II-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;
III-Gestor da informação: unidade ou projeto da Universidade que, no exercício de suas competências, produz informações ou obtém, de fonte externa à Universidade, informações de propriedade de pessoa física ou jurídica;

IV-Custodiante: entidade detentora da posse, mesmo que transitória, de informação produzida ou recebida pela Universidade, bem como dos recursos de informação para sua manipulação;
V-Incidente em Segurança da Informação: evento que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;
VI-Rótulo: identificação física ou eletrônica da classificação atribuída à informação;
VII-Documento de natureza pública: documento relativo ou pertencente à coletividade, de uso comum a todos, universalmente conhecido ou sem restrição de acesso a qualquer pessoa;
VIII-Documento de domínio público: documento ou obra (artística, invenção, desenho industrial, etc.) que pode ser livremente reproduzido, representado ou explorado sem necessidade de autorização ou de pagamento de direitos autorais, por esgotamento do prazo previsto em lei ou por outro motivo que tenha feito expirar a propriedade intelectual.

2.5 A UNIFAP manterá os recursos computacionais disponibilizados sem interrupções, exceto em casos de imprevistos, corte e manutenção técnica na rede elétrica, manutenção no link Internet programada pela RNP e/ou operadora de telecomunicações, além de interrupções técnicas não programadas próprias de equipamentos da rede de dados e telecomunicações.

2.6 Define-se como usuário todos servidores (docentes e técnico-administrativos), assim como os discentes (graduação, pós-graduação e extensão universitária) autorizados a fazer uso dos recursos computacionais da UNIFAP.

2.7 Enquadram-se na definição do item 2.6, também, os usuários de empresas juniores, terceirizados, convidados e visitantes com acesso autorizado aos recursos (solicitado pelo custodiante ao NTI), além de usuários da comunidade de entorno que venham fazer uso dos recursos computacionais.

2.8 Constituem responsabilidades do Usuário (itens 2.6 e 2.7) relativamente ao uso dos Recursos Computacionais da UNIFAP:

2.8.1 Respeitar todas as políticas e procedimentos da UNIFAP incluindo, mas não limitado, às normas e procedimentos de uso dos recursos de Tecnologias da Informação e Comunicação (TIC).

2.8.2 Respeitar os direitos de outros usuários, incluindo os direitos garantidos em outras políticas da UNIFAP para alunos, docentes e funcionários.

2.8.3 Para usuários enquadrados no item 2.7 faz-se necessário para utilizar qualquer Recurso Computacional da UNIFAP somente após obter uma autorização por escrito do Núcleo de Tecnologia da Informação (mediante solicitação do custodiante) e assinar o

Termo de Responsabilidade, no qual declara conhecer as políticas e normas em vigor e se compromete a cumpri-las.

2.8.4 Exibir a comprovação de vínculo com a UNIFAP ou autorização especial expedida pelo Núcleo de Tecnologia da Informação (NTI), sempre que solicitado pelo custodiante, durante a utilização dos recursos, sob pena de imediata suspensão da conexão, sem prejuízo das disposições legais pertinentes.

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

2.8.6 Qualquer atividade desenvolvida com o auxílio dos recursos computacionais da UNIFAP e pelos eventuais prejuízos dela decorrentes, em qualquer nível.

2.8.7 A conta e a respectiva senha são atribuídas a um único usuário e não devem ser compartilhadas com mais pessoas, salvo o caso de laboratórios de informática, onde ocorrerá a autorização por escrito do Núcleo de Tecnologia da Informação (NTI).

2.8.9 Informar imediatamente a Núcleo de Tecnologia da Informação (NTI) qualquer suspeita de tentativa de violação de segurança, em qualquer nível.

2.8.10 Não permitir ou colaborar com o acesso aos Recursos Computacionais da UNIFAP por parte de pessoas não autorizadas, sob pena de ser co-responsabilizado pelos eventuais problemas que esses acessos vierem a causar.

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

2.8.12 Respeitar a integridade dos recursos computacionais da UNIFAP. Os usuários, a menos que tenham uma autorização específica para esse fim, não podem tentar, permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na Universidade, de sua propriedade ou de qualquer outra pessoa ou instituição.

2.8.13 Não ligar ou desligar fisicamente ou eletricamente a um recurso computacional da UNIFAP, nenhum componente externo, como cabos, impressoras, discos ou sistemas de vídeo, sem uma autorização específica.

2.8.14. Respeitar os direitos de propriedade intelectual, de acordo com a regulamentação pertinente, em particular a lei de direitos autorais de "hardware".

2.8.15. Utilizar apenas produtos de "hardware" com as licenças de uso válidas, bem como equipamentos autorizados pelo Núcleo de Tecnologia da Informação (NTI)

2.8.16 Respeitar todas as obrigações contratuais da UNIFAP, inclusive com as limitações definidas nos contratos de "hardware" e outras licenças no uso dos Recursos Computacionais.

2.8.17 Comunicar ao Custodiante ou ao Núcleo de Tecnologia da Informação (NTI) qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros, de qualquer natureza.

2.9 A presente política aplica-se a toda Universidade Federal do Amapá (UNIFAP), englobando corpo docente, técnicos administrativos, alunos, terceirizados e quaisquer outros que venham fazer uso autorizado dos recursos computacionais.

2.10 O presente documento possui sua construção realizada pelo Núcleo de Tecnologia da Informação (NTI) e aprovado/revisado pelo Comitê Gestor de Tecnologia da Informação (CGTI).

2.11 O conteúdo desta norma será progressivamente atualizado em função de novas necessidades de segurança, serviços e tecnologias adotadas pela UNIFAP.

2.12 São responsabilidades do gestor da informação, no que concerne às informações sob sua gestão, produzidas ou custodiadas pela Universidade:
2.12.1 Adotar as medidas e procedimentos necessários para garantir a segurança das informações.
2.12.2 Definir procedimentos, critérios de acesso e classificar as informações,observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes.
2.12.3 Propor regras específicas ao uso das informações.

2.13 São responsabilidades do custodiante da informação:
2.13.1 Garantir a segurança da informação sob sua posse, conforme os critérios definidos pelo respectivo gestor da informação.
2.13.2 Comunicar tempestivamente ao gestor sobre situações que comprometam a segurança das informações sob custódia.
2.13.3 Comunicar eventuais limitações para cumprimento dos critérios definidos pelo gestor para segurança da informação, para que este decida quanto à cessão ou não da informação.

3 Do sigilo das informações

3.1 Quanto à confidencialidade, as informações produzidas ou custodiadas pela Universidade classificam-se nos seguintes graus:
I-Públicas: informações que podem ser divulgadas a qualquer pessoa;
II-Restritas: informações que, por sua natureza ou por interesse da Universidade, só podem ser divulgadas a um grupo restrito de pessoas;

III-Sigilosas: informações que, em razão de lei, interesse público ou para a preservação de direitos individuais, devam ser de conhecimento reservado;
IV-Pessoais: informações relativas à intimidade privada, vida privada, honra e imagem das pessoas.

3.2 Para a classificação da informação em determinado grau de sigilo deverá ser utilizado o critério menos restritivo possível.

3.3 Ao conjunto de informações que não possa sofrer fracionamento para fins de acesso deverá ser atribuído o grau de confidencialidade da sua parte cuja classificação seja a mais restritiva.

3.4 Todas as partes, seções, anexos, páginas, planilhas, gráficos ou quaisquer outros componentes de informação não pública, independentemente do suporte em que residam ou da forma pela qual sejam veiculados, devem ter seus graus de confidencialidade identificados por meio de rótulos padronizados, em consonância com as regras de identidade visual da Universidade, ressalvados os limites de fracionamento indicados no item 3.3.

3.5 Informações classificadas como sigilosas terão os prazos de restrição de acesso definidos de acordo com a legislação vigente, a saber: 5 (cinco) anos para informações reservadas, 15 (quinze) anos para informações secretas e 25 (vinte e cinco) anos para informações ultrassecretas. (redação dada pelo Decreto Nº 7.724, de 16 de maio de 2012)

3.6 O acesso às informações produzidas ou custodiadas pela Universidade, que não seja de domínio público, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários internos, discentes ou colaboradores.

3.7 Qualquer outra forma de uso que extrapola as atribuições necessárias ao desempenho das atividades dos usuários internos, discentes ou colaboradores necessitará de prévia autorização formal, pelo custodiante (item 2.4).

3.8 O acesso, quando autorizado, dos usuários discentes, colaboradores ou externos a informações produzidas ou custodiadas pela Universidade que não sejam de domínio público é condicionado ao aceite a termo de sigilo e responsabilidade.

3.9 As informações produzidas ou custodiadas pela Universidade serão classificadas em função do seu grau de confidencialidade, disponibilidade, integridade e prazo de retenção.

3.10 A classificação disposta por esta política contempla critérios quanto à confidencialidade, disponibilidade e integridade das informações.

3.11 A classificação quanto ao prazo de retenção se dá por meio do Sistema de Acervos e Arquivos da UNIFAP.

3.12 A autorização, o acesso e o uso das informações produzidas ou custodiadas pela Universidade devem ser controlados de acordo com a respectiva classificação.

3.13 Cabe ao gestor da informação (item 2.4) classificá-la quanto à confidencialidade no momento em que a informação for produzida ou obtida .
3.14 No ato da classificação da informação, o gestor deve considerar a legislação em vigor, os controles administrativos e tecnológicos necessários ao tratamento da confidencialidade da informação, as necessidades de compartilhamento ou restrição de acesso e os custos de proteção.

3.15 O gestor da informação, ao classificá-la como sigilosa ou restrita, deve indicar, necessariamente, o grupo de pessoas, projetos ou unidades da Universidade com permissão para acessá-la.

3.16 As informações produzidas pela Universidade podem ser reclassificadas pelo gestor da informação ou pela autoridade competente, por iniciativa própria ou por solicitação de qualquer usuário, cabendo comunicação imediata da alteração aos custodiantes da informação para correta rotulação.

3.17 As informações recebidas de pessoa física ou jurídica externa à Universidade serão submetidas, adicionalmente, a medidas de segurança da informação compatíveis com os requisitos pactuados com quem as forneceu.

3.18 O Reitor, os Pró-Reitores e os Diretores de Unidade podem indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem garantir a segurança da informação, nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação pertinentes.

4 Das violações de Segurança da Informação

4.1 A UNIFAP caracteriza como não ético e inaceitável e considera como motivo de ação disciplinar prevista em seus estatutos qualquer atividade através da qual um indivíduo:

4.1.1 Viole questões tais como direitos autorais ou proteção de patentes e autorizações da UNIFAP ou de terceiros, como também licenças de uso e outros contratos.

4.1.2 Interfira no uso correto dos recursos de informação.

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

4.1.4 Sem autorização, destrói, altera, desmonta, desconfigura, impede o acesso de direito ou interfere na integridade dos recursos computacionais.

4.1.5 Sem autorização, invade a privacidade de indivíduos ou entidades que são autores, criadores, usuários ou responsáveis pelos recursos computacionais.

4.1.6 Remova dos recursos computacionais da UNIFAP algum documento de propriedade da UNIFAP ou por ela administrado, sem uma autorização específica.
4.1.7 Se faça passar por outra pessoa ou esconda sua identidade na utilização dos Recursos Computacionais da UNIFAP com exceção dos casos em que o acesso anônimo é explicitamente permitido.

4.1.8 Viole ou tente violar os sistemas de segurança dos recursos computacionais da UNIFAP, como quebrar ou tentar adivinhar identificação ou senhas de terceiros, interferir em fechaduras automáticas ou sistemas de alarme.

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

4.1.10 Tente interferir ou interfira em serviços de outros usuários ou o seu bloqueio, provocando, por exemplo, congestionamento da rede, inserindo vírus ou tentando a apropriação dos Recursos Computacionais da UNIFAP.

4.1.11 Consiga benefícios financeiros ou de outra espécie diretos, para si ou para terceiros fora da Universidade, através da utilização dos recursos computacionais da UNIFAP exceto quando autorizado explicitamente pelo custodiante (item 2.2) para os recursos locais ou pelo Núcleo de Tecnologia da Informação no caso dos recursos computacionais corporativos.

4.2 As penalidades a serem aplicadas às condutas elencadas no item 4.1, sem prejuízo de outras penas previstas em lei ou em normas da Universidade, são: Redução ou eliminação, temporárias ou permanentes, de privilégios de acesso, tanto aos Recursos Computacionais, quanto às redes, salas de computadores da UNIFAP e outros serviços ou facilidades.

4.3 Qualquer violação ou suspeita de violação dessas normas deve ser comunicada imediatamente ao responsável direto pelo recurso computacional no local onde o fato tenha ocorrido.

4.4 A infração ou tentativa de infração às regras constantes desta norma ou às regras previstas em lei serão apuradas por meio de sindicância administrativa, processo administrativo disciplinar ou processo sumário, nos termos do Regimento Geral e Estatuto dos Servidores da UNIFAP.

4.5 Sempre que julgar necessário para a preservação da integridade dos Recursos Computacionais da UNIFAP, dos serviços aos usuários ou dos dados, o Administrador de

Sistemas e Rede poderá suspender temporariamente qualquer conta, seja o responsável pela conta suspeito de alguma violação, ou não.

4.6 Esta Norma se aplica a qualquer membro da comunidade universitária, quer ele esteja dentro da UNIFAP ou fora, e se refere a todos os recursos computacionais, controlados individualmente ou compartilhados, isolados ou em rede.

4.7 Os Unidades Organizacionais da UNIFAP podem definir condições de uso específicas para os recursos sob seu controle, consistentes com a política geral, mas com detalhes, diretrizes e/ou restrições adicionais.

4.8 Cabe ao Órgão tratar das violações de restrições adicionais de acordo com as normas internas vigentes e onde não houver estes mecanismos específicos, o exposto nesta Norma deve prevalecer.

4.9 No caso do uso de redes externas, às políticas envolvendo este tipo de uso também são aplicáveis e precisam ser adotadas.