POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PATOS DE MINAS

2026

A **PRESIDENTE DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO DA FEPAM/UNIPAM**, no uso de suas atribuições e tendo em vista o disposto na Portaria FEPAM N. 443/2024,

R E S O L V E:

Aprovar a presente Política, que passa a vigorar a partir de sua publicação, nos termos e condições a seguir apresentados, devendo ser observada por todos os seus funcionários, professores, estagiários, jovens aprendizes, alunos, parceiros e demais partes a ela vinculadas.

1. OBJETIVO

O objetivo da Política de Segurança da Informação é estabelecer diretrizes aos usuários de informações e dados que a Fundação Educacional de Patos de Minas (FEPAM), o CENTRO UNIVERSITÁRIO DE PATOS DE MINAS (UNIPAM) e o Colégio Universitário detém sob a sua responsabilidade e determinar padrões de comportamento relacionados à segurança, proteção e privacidade de dados pessoais e estratégicos, bem como demais informações necessárias ao desempenho de suas atividades de negócio.

A FEPAM, o UNIPAM e o Colégio Universitário fazem uso da tecnologia e da internet para promover um ensino de maior qualidade à sua comunidade acadêmica e estudantil, sempre priorizando o acesso ao conhecimento e ao aprendizado. Contudo, em um cenário marcado pela mobilidade e pela ausência de fronteiras físicas bem definidas — características da sociedade atual impulsionada pelos avanços tecnológicos — torna-se indispensável adotar cuidados redobrados para prevenir incidentes que possam comprometer a segurança de alunos e colaboradores.

Nesse cenário, a segurança da informação se apresenta como uma atividade estratégica para a proteção de todos os ativos, sejam eles tangíveis ou intangíveis, da FEPAM e de suas mantidas UNIPAM e Colégio Universitário, como imagem institucional, reputação, conhecimento, patrimônio e, principalmente, a própria informação. Por isso, é essencial que todos os membros da instituição, tanto da área administrativa quanto do corpo docente e discente, adotem práticas seguras e colaborem na disseminação da cultura de segurança digital.

Esta política constitui também uma declaração formal desta instituição, sobre o seu compromisso com a proteção e privacidade de dados pessoais e estratégicos, bem como outras informações de sua propriedade ou que estejam sob sua responsabilidade.

A Política de Segurança da Informação (PSI) aplica-se aos contextos estudantil, acadêmico e administrativo, tendo como objetivos:

- definir diretrizes estratégicas e princípios voltados à proteção dos ativos tangíveis e intangíveis, como imagem institucional, reputação, marca, propriedade intelectual, bases de dados e

conhecimento, além dos recursos de tecnologia da informação e comunicação (TI) do UNIPAM, bem como das informações dos alunos;

- orientar a tomada de decisões e a execução de atividades profissionais e educacionais por parte de todos os colaboradores do UNIPAM e instituições associadas, tanto em ambientes físicos quanto digitais, em conformidade com as normas internas e a legislação vigente no país;
- estabelecer fundamentos para a condução de práticas educacionais seguras, minimizando riscos que possam comprometer a imagem da UNIPAM e de suas mantidas;
- promover uma cultura de segurança da informação, incentivando comportamentos responsáveis e conscientes no uso de dados e tecnologias na sociedade digital;
- assegurar a confidencialidade, integridade, disponibilidade, autenticidade e conformidade legal das informações e dos recursos de TI da FEPAM e suas mantidas;
- servir como base para a criação de normas e procedimentos específicos relacionados à segurança da informação, bem como para a implementação de controles e processos necessários ao seu cumprimento.

2. ESCOPO

Na FEPAM, no UNIPAM e no Colégio Universitário visamos que segurança é parte principal da cultura e DNA da instituição. Entendemos e acreditamos em uma abordagem de segurança, onde toda a construção do negócio é feita em uma base sólida em segurança de todas as informações e ativos que hospedam informações na instituição. Qualquer sistema, processo, procedimento e controle são concebidos em torno da segurança.

A cultura da segurança da informação deve ser adotada internamente por todos os colaboradores da instituição. Para fornecedores, alunos, terceiros, esta previsão deve estar explícita em cláusulas contratuais, assim como suas cadeias de relacionamento entre si e a instituição.

Todos esses esforços convergem para a proteção dos ativos de informação do ecossistema institucional, principalmente seus alunos, professores, funcionários, estagiários, jovens aprendizes, parceiros de negócios e membros do conselho.

Segurança da Informação é crítica para o negócio da FEPAM e de suas mantidas UNIPAM e Colégio Universitário, e, por isso, carregamos a segurança como mais que um requisito para o negócio da instituição. Sendo assim, temos como principal objetivo deste documento estabelecer as diretrizes necessárias para orientar a todos os colaboradores e alunos da instituição, os cuidados a serem observados para a manutenção de nossas informações em um padrão de segurança superior.

Entende-se por usuário toda e qualquer pessoa física ou jurídica, contratada, cedida pela instituição, ou prestadora de serviço, que exerça alguma atividade dentro ou fora da instituição, tais como, administradores (Diretores e Gestores), comitês e grupos de trabalho de assessoramento, colaboradores, alunos, bem como os prestadores de serviço.

Dentre os propósitos que se baseiam esta política, destaca-se a garantia da qualidade dos dados e informações da Empresa quanto à:

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3. TERMOS E DEFINIÇÕES

Para fins deste documento devem ser consideradas as seguintes definições:

ADMINISTRADORES: Diretoria, Gestores e Conselhos.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados em todo o território nacional.

ANONIMIZAÇÃO: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

ATIVOS: entende-se como qualquer componente (seja humano, tecnológico, software ou etc.) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

COMITÊ DE SEGURANÇA DA INFORMAÇÃO: comitê multidisciplinar responsável por definir e apoiar estratégias necessárias à implantação e manutenção da Política de Segurança da Informação.

CONSENTIMENTO: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

DADO PESSOAL: toda informação relacionada a pessoa natural “identificada” ou “identificável”.

DADO PESSOAL SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

DPO (DATA PROTECTION OFFICER): trata-se do encarregado pela proteção de dados que deverá ser indicado pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).

ELIMINAÇÃO: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

COLABORADOR: pessoa física que mantenha relação trabalhista direta com a Empresa.

INCIDENTE DE SEGURANÇA: quebra de segurança que leva a acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, ou qualquer forma de tratamento inadequado ou ilícito, que possa causar risco ou dano relevante aos titulares.

INFORMAÇÃO: um conjunto organizado de dados, que proporciona decisões otimizadas e estratégicas sobre como resolver problemas, tomar decisões e mudar a direção de um negócio ou de uma vida.

LGPD (LEI GERAL DE PROTEÇÃO DE DADOS) OU LEI 13.709/2018: foi criada para regulamentar o tratamento de dados pessoais pelas empresas com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade de pessoas físicas. A referida Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio do país de sua sede ou do país onde estejam localizados os dados.

RESPONSÁVEL PELA SEGURANÇA DA INFORMAÇÃO: responsável por organizar regras para salvaguardar a informação gerida na organização.

PRESTADORES DE SERVIÇO E FORNECEDORES: pessoas físicas ou jurídicas com as quais a FEPAM e suas mantidas possuem relação comercial.

TITULAR: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

TRATAMENTO: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

USO COMPARTILHADO DE DADOS: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

USUÁRIOS: entende-se por usuário toda e qualquer pessoa física ou jurídica, contratada ou prestadora de serviço, que exerça alguma atividade dentro ou fora da empresa, incluindo colaboradores e seus administradores.

4. REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Este documento está fundamentado nos Objetivos de Controle elencados pela norma ABNT NBR ISO/IEC 27002, assim como as publicações NIST e seu Framework de Segurança da Informação.

- **Confidencialidade:** não permitindo disponibilização ou exposição da informação a indivíduos, entidades ou processos não autorizados expressamente, seja por contratos ou outros instrumentos formais.
- **Integridade:** informações armazenadas com exatidão, íntegras em seu volume e por completo das mesmas, tais como foram criadas ou recebidas utilizando tecnologias, controles e processos que garantam esse requerimento pelos próprios serviços da FEPAM, do UNIPAM e do Colégio Universitário.
- **Disponibilidade:** os sistemas e informações pertencentes ao ecossistema tecnológico da FEPAM, do UNIPAM e do Colégio Universitário deverão estar disponíveis para seus alunos, colaboradores e demais usuários da instituição, atendendo também a confidencialidade das informações e integridade de seu conteúdo, formando, assim, uma tríade de segurança de qualidade superior.
- **Privacidade e Proteção de Dados Pessoais:** os dados pessoais contidos nas Informações devem ser protegidos com a adoção de medidas técnicas e organizacionais de Segurança da Informação, nos termos impostos pela Lei nº 13.709/2018, conhecida por LGPD ou Lei Geral de Proteção de Dados e que estará disciplinada em conjunto com o Procedimento de Tratamento de Dados Pessoais e o Código de Conduta Ética.

Orientação	**Seção**
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados Regulamenta o tratamento de dados pessoais no Brasil, estabelecendo direitos dos titulares de dados, obrigações para os controladores e operadores, além de prever sanções para o descumprimento.	Capítulo VII - Seção I - Art. 46, Seção II art. 50
ABNT NBR ISO/IEC 27701: 2019. Técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação - Requisitos e Diretrizes	Itens 6 - 6.6.2 (Página 16)
Marco Civil da Internet - Lei nº 12.965/2014 Define os princípios, garantias, direitos e deveres para o uso da internet no Brasil, com enfoque na privacidade, proteção de dados pessoais e segurança.	Lei na sua integralidade

5. DECLARAÇÕES DA POLÍTICA

A Política de Segurança da Informação estabelece diretrizes, regras e procedimentos e controles necessários para garantir a proteção de dados pessoais e informações confidenciais na instituição, em conformidade com a legislação vigente, incluindo a LGPD e normas correlatas. As declarações desta política visam garantir a segurança, a confidencialidade, e a integridade das informações, além de orientar as demais políticas institucionais cujas diretrizes se relacionam à segurança da informação.

Dos Princípios Gerais

I. A Política de Segurança da Informação da FEPAM, do UNIPAM e do Colégio Universitário constitui o instrumento normativo central, servindo de referência para a elaboração, a revisão e a aplicação das demais políticas e procedimentos vinculados à segurança da informação.

II. A Política de Segurança da Informação deve estar em consonância com uma gestão de continuidade de negócios em nível organizacional.

CAPÍTULO I
ORGANIZAÇÃO E ESTRUTURA ORGANIZACIONAL APLICADAS À SEGURANÇA DA INFORMAÇÃO

Art. 1º Os Gestores, em nível estratégico, apoiam ativamente a cultura de Segurança da Informação do UNIPAM como valor estratégico na empresa, por meio de um claro direcionamento, demonstrando o seu comprometimento, tal como demonstrado na aprovação formal desta Política de Segurança da Informação.

Art. 2º São atribuições específicas do DPO:

I. definir a estratégia de Segurança da Informação para o UNIPAM, alinhando a mesma às demais estratégias do negócio;

II. deliberar sobre a criação, organização, estrutura e regulamentação de um grupo de trabalho de Segurança da Informação e Privacidade de Dados;

III. convocar e coordenar, a seu critério, reuniões periódicas e emergenciais deste grupo de trabalho de Segurança da Informação;

IV. aprovar os documentos estratégicos relacionados à Segurança da Informação.

Art. 3º São atribuições específicas do Comitê de Segurança da Informação:

I. elaboração e revisões da Política de Segurança da Informação e demais políticas relacionadas à segurança do UNIPAM, o qual servirá como guia para as ações de educação e difusão cultural do tema de Segurança da Informação e os controles técnicos aplicáveis;

II. revisão das ações educacionais já existentes no UNIPAM, como treinamento específico sobre sistemas de informação para novos colaboradores quando este se faz necessário, além de iniciativas recorrentes de atualização para os demais colaboradores, objetivando uma reciclagem total em até 18 meses para todos os colaboradores e alunos do UNIPAM;

III. revisão dos procedimentos para continuidade dos negócios do UNIPAM vide CATÁLOGO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO DO UNIPAM,

bem como a produção e implantação de novos procedimentos que garantam a operação contínua dos negócios da instituição e do UNIPAM frente aos riscos mapeados pelo comitê se segurança da informação;

IV. participação ativa nas revisões dos procedimentos de Gerenciamento de Mudanças no ambiente de tecnologia da informação do UNIPAM;

V. fomento à cultura de Segurança da Informação dentro do UNIPAM e em toda a cadeia de relacionamentos, incluindo alunos, fornecedores, parceiros de negócios, colaboradores e membros do conselho.

Art. 4º Todos os colaboradores, alunos, parceiros e demais usuários de sistemas de informações ou ativos relacionados à tecnologia da informação, incluindo terceiros ou quaisquer prestadores de serviços recorrentes do UNIPAM, independentemente da relação contratual estabelecida e do nível hierárquico, são responsáveis:

I. por conhecer e cumprir rigorosamente a Política de Segurança da Informação do UNIPAM, bem como toda a documentação correlata;

II. pela ótica da responsabilidade pela segurança, todos no UNIPAM são colaboradores e devem se atentar e reportar ao se deparar com práticas em não conformidade com a Política de Segurança, ajudando, inclusive, na reeducação dos hábitos em não conformidade;

III. por reportar ao Comitê de Segurança da Informação, ou ao canal disponibilizado pela mesma, a suspeita ou confirmação de descumprimentos de toda a documentação de Sistemas de Informações e seus objetivos de controle, bem como de tentativas de burla de recursos e ferramentas de sistemas de informação e quaisquer incidentes de SI. As seguintes práticas podem ser entendidas como incidentes de SI:

a) acesso não autorizado a recursos de TI, sistemas e banco de dados do UNIPAM, ou de terceiros;

b) vírus;

c) ataques de navegação de serviços (DoS ou DDoS);

d) violação a esta Política ou procedimentos de SI correlatos;

e) acesso não autorizado ou vazamento de dados, inclusive de dados pessoais que estejam sob custódia do UNIPAM; (vide uso impróprio de informações);

f) pirataria;

g) falha de equipamentos do UNIPAM.

CAPÍTULO II
CLASSIFICAÇÕES DA INFORMAÇÃO

Art. 5º A informação é tida como um ativo e possui valor diferente dependendo do seu conteúdo. Os controles de proteção desses ativos podem aumentar de acordo com seu valor. A classificação das informações também pode definir quais controles de proteção precisam ser implementados. Podemos entender a classificação da informação também como uma escala de proteção a ser aplicada na mesma.

Art. 6º Para a FEPAM e suas mantidas, são cinco os níveis de classificação da informação em ordem crescente de importância e sigilo:

I. **PÚBLICAS:** são todas as informações que já sejam de conhecimento público e estejam disponibilizadas para alunos, colaboradores e público em geral através da internet, ou veiculadas em documentos publicados em jornais, revistas, folders, redes sociais, panfletos, avisos ou palestras autorizadas. Somente as áreas de Assessoria de Comunicação poderão publicar Informações sobre a empresa ou em nome do UNIPAM, bem como definir e orientar porta-vozes do negócio da instituição;

II. **INTERNAS:** são informações que estão disponíveis aos colaboradores por meio das ferramentas aprovadas, com armazenamento interno, em servidores do UNIPAM ou terceiros autorizados (na nuvem, por exemplo o Google Drive). Qualquer informação classificada como “INTERNA” não poderá ser encaminhada, divulgada ou publicada em quaisquer meios para terceiros não autorizados, devendo a sua disponibilização ser restrita ao ambiente de trabalho do UNIPAM e uso limitado aos Colaboradores ou terceiros;

III. **RESTRITAS:** os documentos classificados como “INFORMAÇÃO RESTRITA” somente poderão ser acessados pela área, departamento, setor ou função dentro do UNIPAM que classificou tais informações. Normalmente são informações de uma determinada área que não deve ser acessada por outros setores da empresa, por exemplo, os documentos do setor de RH ou departamento financeiro e/ou contábil da empresa;

IV. **CONFIDENCIAL:** todas as informações classificadas como confidenciais deverão ser mantidas em arquivos físicos ou eletrônicos com níveis de segurança compatíveis com a relevância da informação, tais como cofres, armários com chaves, diretórios criptografados ou envio dos arquivos somente após a inclusão de mecanismos de segurança (senha ou criptografia). A transmissão de arquivos confidenciais só deverá ser feita utilizando meios de transmissão seguras, para as partes previamente autorizadas, com contrato de sigilo claro e dentro da validade,

sejam as partes: funcionários, colaboradores, conselheiros, fornecedores ou qualquer tipo de parceiro de negócios que precisam: criar, armazenar ou processar qualquer tipo de informação CONFIDENCIAL;

a) deverão ser classificadas como CONFIDENCIAIS as informações que por sua origem, natureza ou importância não devam ser compartilhadas ou colocadas à disposição de pessoas não autorizadas. Consideram-se informações confidenciais todas as que assim forem classificadas, bem como – indistintamente – dados recebidos ou compilados de/sobre clientes, senhas, informações financeiras ou de salários, código fonte de softwares utilizados pela instituição, informações sensíveis de alunos, usuários, entre outras;

V. **SECRETAS:** as informações classificadas como SECRETAS possuem o mais alto nível de sensibilidade e criticidade para o negócio. Chaves de criptografia (certificados SSL ou chaves SSH) e credenciais de acesso em geral são exemplos de informações SECRETAS. Outras Informações estratégicas com alto nível de confidencialidade também podem ser classificadas como SECRETAS a critério do proprietário da informação;

a) informações em que seu possível vazamento implica em impacto financeiro direto ao negócio ou ponha em risco a continuidade dos negócios é um indício para que ela receba a classificação máxima de proteção: SECRETA.

CAPÍTULO III
TRATAMENTO DE DADOS PESSOAIS E OBSERVÂNCIA À LGPD

Art. 7º Todos os processos da instituição que realizam o tratamento de dados e informações pessoais devem estar em conformidade com a LGPD e suas bases legais que legitimam o tratamento de dados pessoais e garantem direitos aos seus titulares.

Art. 8º As atividades de tratamento, armazenamento e transferência de dados pessoais e/ou sensíveis, sejam de beneficiários, empregados e prestadores de serviço de qualquer natureza, nas operações da instituição devem observar os princípios e diretrizes apresentados a seguir:

I. os dados e informações pessoais tratados pela instituição devem ser coletados de forma ética, com o conhecimento do titular, para propósitos específicos;

II. devem ser tomadas medidas razoáveis para garantir que os dados dos titulares sejam tratados dentro da necessidade e apoiados nas bases legais – LGPD Art. 7º, 8º, 11º e 14º;

III. deve-se minimizar os dados, limitados ao que é necessário em relação aos propósitos para os quais são processados, utilizando-se o Framework “*Privacy by*

Design". Caso não seja possível, deve ser justificado, conforme Art. 52 – VIII da Lei Geral de Proteção de Dados – LGPD;

IV. deve-se garantir a segurança dos dados pessoais tratados pela instituição e comunicar incidentes de segurança da informação à Agência Nacional de Proteção de Dados – ANPD, sendo que, dependendo da gravidade do incidente, o titular dos dados também deverá ser comunicado;

V. devem ser mantidos todos os dados coletados (nas formas e canais cabíveis) enquanto o cadastro do titular do dado estiver ativo e conforme seja necessário para as atividades da empresa, observando-se o período de retenção estabelecido em contrato ou em outra lei que suporte a retenção;

VI. o descarte de dados pessoais deve ser feito com segurança, de forma que os dados sejam irrecuperáveis, seguindo a Política de Retenção e Descarte Institucional;

VII. o armazenamento deve utilizar bancos de dados internos da instituição ou em "nuvem" pelo(s) prestador(es) de serviço(s) contratado(s);

VIII. a Gerência de Tecnologia da Informação – TI deve avaliar, monitorar e gerenciar as permissões de usuários, administradores e desenvolvedores, considerando a necessidade de acesso a cada Sistema de Gestão de Banco de Dados, aplicando essas permissões de acesso aos usuários de maneira adequada aos serviços realizados;

IX. os prestadores de serviços deverão estar em conformidade com a legislação de proteção de dados vigente e cumprir as cláusulas contratuais estabelecidas adotando procedimentos de segurança para proteger a confidencialidade, segurança e integridade dos dados;

X. qualquer informação ou documento corporativo somente poderá ser armazenado em um banco de dados homologado ou ativo da instituição;

XI. é vedado o compartilhamento de dados pessoais ou sensíveis com terceiros, sem a avaliação e aprovação do DPO e da Segurança da Informação;

XII. as informações classificadas como RESTRITA, CONFIDENCIAL ou SECRETA, devem sofrer tratamento especial no seu descarte;

XIII. qualquer evento de perda, extravio ou roubo de informações, devem ser reportados IMEDIATAMENTE ao departamento de Redes e Segurança, por meio do email rs@unipam.edu.br e/ou ao Comitê de Segurança da Informação pelo email comiteseguranca@unipam.edu.br.

CAPÍTULO IV
EQUIPAMENTOS E FERRAMENTAS/SOFTWARES/UTILITÁRIOS

Art. 9º Quanto ao uso de equipamentos e ferramentas corporativas (ativos de TI), fica definido que:

I. o UNIPAM poderá fornecer ao colaborador conta de correio eletrônico, acesso à internet e outras ferramentas de comunicação e produtividade para a dinamização do trabalho ou utensílios como aparelho e linha celular, gavetas, armários e quaisquer dispositivo, físico ou lógico, para a execução do trabalho;

II. o uso destas ferramentas estará sujeito a esta política e restrições de acesso, de acordo com o nível de acesso outorgado ao usuário e deliberações do departamento de Informática e de Redes e Segurança;

III. como política de nível de acesso à informação, utilizamos a premissa de “menor privilégio possível”. O colaborador somente terá acesso as aplicações e informações que forem estritamente necessários para a realização do seu trabalho;

IV. é expressamente proibido o uso de qualquer recurso corporativo, computadores, redes, acessos bem como quaisquer meios de comunicação corporativas para uso pessoal e/ou prática de qualquer ato ilícito, sob pena de responsabilização civil ou até criminal;

V. o colaborador é responsável pelos ativos de TI do UNIPAM que são utilizados para desempenho das suas atividades no ambiente de trabalho, bem como pelas informações que inserir em tais ativos.

Art. 10º Quanto ao acesso e ao uso da internet, fica estabelecido que:

I. o Centro Universitário de Patos de Minas - UNIPAM, poderá permitir acesso à internet e a navegação em sites de conteúdo, sempre de acordo com a sua política de Segurança da Informação e bloqueios de sites classificados como inseguros ou não confiáveis;

II. é explicitamente proibido a transferência de arquivos por meio de quaisquer protocolos, aplicativos ou ferramentas que não forem previamente e explicitamente aprovados pela área de Redes e Segurança da instituição;

a) essa aprovação é uma análise de segurança da ferramenta adquirida/contratada para determinado uso e do fornecedor do produto/software, a fim de garantirmos que somente ferramentas e fabricantes que possuam alta maturidade em Segurança da Informação, proteção de dados e políticas claras de privacidade, sejam incorporados à lista de ferramentas armazenadas no NAS do setor de

Redes e Segurança e fornecedores aprovados. Isso evita a herança de vulnerabilidades por meio de ferramentas não seguras e não testadas, assim como parcerias com fornecedores que possam não seguir as boas práticas de Segurança da Informação;

b) da mesma forma, não será permitido o download de materiais protegidos por direitos autorais ou a instalação de softwares não homologados pela área de Segurança da Informação / Informática. O colaborador deve consultar o departamento de Informática em Primeiro Nível e posteriormente o departamento de Redes e Segurança antes de fazer o download de qualquer software de terceiros.

Art. 11º Quanto à rede sem fio (Wi-Fi), dispõe-se que:

I. o UNIPAM, sempre que possível, disponibiliza à comunidade acadêmica e administrativa, em ambientes autorizados e restritos ao perímetro físico da instituição, uma rede sem fio (Wi-Fi) destinada exclusivamente a fins educacionais e administrativos;

II. o acesso à rede sem fio (Wi-Fi) é permitido apenas a alunos ativos e colaboradores previamente autorizados, os quais devem comprometer-se a utilizá-la de forma segura e responsável seguindo as diretrizes do uso do mesmo contidas em https://wifi.unipam.edu.br;

III. em situações excepcionais, visitantes e fornecedores poderão acessar a rede sem fio mediante autorização prévia do gestor imediato, da equipe de Tecnologia da Informação (TI), mais especificamente do Departamento de Redes e Segurança ou do departamento de Assessoria de Comunicação (ASCOM) mediante aviso prévio via UniChamados.

Art. 12º Quanto ao e-mail (correio eletrônico), determina-se que:

I. os e-mails da instituição, assim como todas as plataformas de comunicação utilizadas na empresa, são ferramentas de trabalho, não devendo ser utilizados para outros fins de forma pessoal;

II. as informações contidas nas mensagens eletrônicas de e-mail são de propriedade da instituição, podendo ser monitoradas a qualquer tempo sem aviso ou notificação prévia para fins de auditoria de conformidade e segurança às normas internas, regulamentações ou boas práticas aplicadas ao negócio do UNIPAM;

III. é expressamente proibido o envio de informações classificadas como “INTERNAS” e “CONFIDENCIAIS” para endereços de e-mail de outros domínios além do

unipam.edu.br, exceto para terceiros (alunos, fornecedores, parceiros comerciais) diretamente envolvidos no respectivo assunto da mensagem;

IV. quando um colaborador da instituição for desligado, deverão ser observados os seguintes procedimentos de desligamento de colaboradores via UniChamados, onde é enviado as áreas responsáveis o desligamento do colaborador e feito os bloqueios necessários nos sistemas utilizados pelo mesmo; em relação ao seu e-mail corporativo:

a) contas inativas: toda e qualquer credencial de acesso que não tiver atividade após o desligamento ou por algum motivo seja solicitado a inatividade da conta, a mesma será feita o bloqueio pelos departamentos responsáveis.

Art. 13º Quanto à autenticação de dois fatores, também chamado de MFA (Múltiplo Fator de Autenticação), define-se que:

I. o uso de autenticação multifator (MFA) será avaliado e implementado conforme as diretrizes estabelecidas na **Política de Gestão de Identidades e Senhas** da instituição. Sempre que aplicável, a MFA deve ser utilizada como camada adicional de segurança no acesso a sistemas e serviços críticos, reforçando a proteção contra acessos não autorizados;

II. é obrigatório o uso de autenticação multifator (MFA MultiFactor Authentication) no Portal UNIPAM.

III. é recomendado o uso de autenticação multifator (MFA MultiFactor Authentication) nos sistemas, nas aplicações, nas contas de e-mail e nos serviços onde a opção estiver disponível.

Art. 14º Quanto ao acesso remoto, fica determinado que:

I. colaboradores previamente cadastrados e autorizados, mediante aprovação explícita dos seus gestores diretos, poderão obter acesso remoto ao ambiente computacional do UNIPAM para trabalho fora de seu ambiente normal (regime home office);

II. esse processo deve utilizar apenas equipamentos corporativos fornecidos pela instituição com a aplicação dos controles de segurança vigentes. A conexão será estabelecida por meio de VPN privada corporativa.

Art. 15º Quanto ao uso restrito da VPN institucional fica definido que:

I. o acesso à VPN institucional é estritamente reservado a colaboradores previamente autorizados pela Diretoria Executiva e pelo Departamento de Tecnologia da

Informação. Esta medida visa garantir a segurança dos dados e a integridade dos sistemas internos da instituição;

II. o uso da VPN destina-se exclusivamente a atividades de natureza administrativa e institucional, sendo vedado seu uso para fins pessoais ou não autorizados. Além disso, é expressamente proibido o compartilhamento de credenciais de acesso (usuário e senha), sob pena de responsabilização conforme as normas internas e políticas de segurança da informação. Esse controle reforça as práticas de segurança e o compromisso com a proteção das informações da instituição.

Art. 16º Quanto aos documentos físicos, fica estabelecido que:

I. todos os colaboradores devem manter seu ambiente de trabalho organizado e seguro, zelando pela proteção de informações sensíveis que, por sua natureza, exigem sigilo e tratamento adequado. Isso inclui mesas, agendas, documentos físicos, rascunhos, anotações e quaisquer meios de comunicação impressos ou manuscritos;

II. é expressamente proibido divulgar, compartilhar ou armazenar credenciais de acesso de forma inadequada, incluindo, mas não se limitando a: afixar senhas em post-its nos monitores ou em locais visíveis, registrar senhas em planilhas ou documentos pessoais, bem como armazená-las nos diretórios de armazenamento fornecidos pela instituição sem o devido controle de segurança;

III. a exposição indevida dessas informações representa risco à integridade dos sistemas institucionais e compromete a segurança da informação como um todo, sendo responsabilidade de cada colaborador adotar práticas seguras no desempenho de suas atividades;

IV. os documentos impressos e anotações que precisem estar em um papel (impresso ou “post it”) devem permanecer nas mesas em caráter temporário devendo ser recolhidos em compartimentos fechados disponíveis em seu departamento ou qualquer dependência da empresa que forneça segurança e proteção a esses materiais;

V. os documentos órfãos notoriamente importantes (que possuem assinaturas, por exemplo) deverão ser descartados seguindo medidas previstas na Política de Retenção e Descarte Institucional e o diretório RSGI no SVN de cada departamento, para que possam ser revisados posteriormente antes de sua destruição. Esta ação de exposição de documentos impressos é válida para o ambiente de trabalho, incluindo a estação de trabalho, mesa, gavetas, arquivos, impressões esquecidas e lixo.

Art. 17º Quanto aos dispositivos pessoais, dispõe-se que:

I. não é permitido a conexão de dispositivos não corporativos às redes internas, cabeadas ou sem fio, salvo redes sem fio cuja finalidade seria o acesso ao ambiente não corporativo;

II. aos colaboradores que precisem fazer uso de dispositivos móveis para o desempenho de funções e tarefas específicas, o farão utilizando equipamentos fornecidos pela empresa, com os devidos controles e proteções técnicas aplicadas geridas pelo Comitê de Segurança da Informação (CSI).

Art. 18º Quanto às redes sociais e às mídias sociais, determina-se que:

I. é expressamente proibido que qualquer colaborador emita qualquer comunicado, opinião ou comentário em nome do Centro Universitário de Patos de Minas – UNIPAM sem a expressa aprovação e alinhamento com as áreas de marketing e comunicação;

II. as interações de resposta, réplica aos comentários feitos por terceiros sobre a empresa e afins, só podem ser feitas pelas áreas específicas de comunicação e gestão de mídias sociais, mesmo sendo postadas em redes pessoais;

III. o uso de redes sociais por colaboradores, quando realizado a partir do ambiente institucional e durante o horário de trabalho, deve estar estritamente vinculado às atribuições profissionais e aos objetivos do UNIPAM. Toda conduta nesse contexto, seja por ação ou omissão, é de inteira responsabilidade do colaborador, que deve zelar pela imagem institucional e adotar uma postura ética, responsável e compatível com os valores da instituição;

IV. a publicação de fotos em áreas internas com informações institucionais confidenciais ou não também deve ser evitada, para evitar que informações restritas contidas nas áreas internas da empresa ou ambiente de trabalho remoto sejam publicadas indevidamente, a não ser que seja previamente autorizada pela área de comunicação.

Art. 19º Quanto aos softwares, aos aplicativos, aos plugins e às extensões, define-se que:

I. não é permitida a instalação de softwares não aprovados pela área de Informática e/ou Comitê de Segurança da Informação (CSI) em quaisquer dispositivos que acessam os sistemas de informação da instituição que inclui: computadores, notebooks e dispositivos portáteis como tablets e celulares. Inclusive software, aplicativos, plugins pagos ou gratuitos, extensões de navegadores e similares;

II. os departamentos de Informática e Redes e Segurança, devem possuir um portfólio de ferramentas e aplicativos para atender as demandas do negócio incluindo ferramentas de produtividade e afins;

III. as ferramentas já são previamente instaladas em todos os dispositivos corporativos para atendimento de suas atividades laborais.

Art. 20º Quanto à postura geral de privacidade de dados, fica determinado que:

I. todos os acessos aos sistemas internos devem ter como justificativa um propósito real de negócio. É expressamente proibido o acesso a quaisquer informações de clientes, colaboradores ou qualquer registro nos sistemas de informações da instituição sem um propósito claro de negócio, e ligado diretamente ao exercício das funções atribuídas na relação de trabalho entre o colaborador e a empresa;

II. é expressamente proibido o acesso a dados de alunos, colaboradores, fornecedores, parceiros, por mera curiosidade, como por exemplo:

a) acessar contas de celebridades, pessoas públicas, parentes, amigos ou qualquer outro cliente sem que haja um propósito de negócio e principalmente, um chamado relacionado ao caso;

b) acessar contas de alunos, fornecedores, parceiros mediante consulta de honorários, valores pagos vide contrato, salários e qualquer outro tipo de dado financeiro que possa ser considerável particular e sensível;

III. caso precise resolver algum problema na sua própria conta, como alterar uma informação de cadastro, abra um chamado e peça que um colega faça a alteração ao invés de si próprio.

CAPÍTULO V
CONTROLES DE ACESSOS FÍSICOS E LÓGICOS

Art. 21º Os dados e informações devem ser acessados somente por pessoas autorizadas e capacitadas para que o uso seja adequado. Além disso, o acesso deve ser específico e restrito à necessidade de execução da sua atividade. O acesso lógico aos sistemas computacionais, disponibilizados pela instituição, deve ser controlado, garantindo a rastreabilidade e a efetividade do acesso autorizado, salvo os acessos de conteúdo de caráter público.

Art. 22º Todo usuário deverá possuir chave e senha previamente cadastrados, sendo esta, pessoal e intransferível, sendo proibida a utilização de códigos de acesso genéricos ou comunitários, exceto quando devidamente autorizado pelo superior imediato e pelo Comitê de Segurança da Informação, por meio de registro de chamado.

Art. 23º Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados, exceto quando devidamente autorizados.

Art. 24º Nenhum usuário deve ter, por padrão, acesso de “Administrador” em estações de trabalho e/ou notebooks. Caso seja necessário tal acesso, deverá ser feita uma solicitação a área responsável por meio de abertura de chamado na área responsável, com a devida finalidade destacada para avaliação e poderão ser autorizadas ou negadas.

Art. 25º Não é permitido o compartilhamento de dados pessoais e sensíveis dentro e fora das dependências da instituição por qualquer meio de comunicação, exceto para execução dos serviços, por meio de termos, contratos ou cláusulas, devidamente assinados, destacando claramente a finalidade específica para esta liberação.

Art. 26º As informações e dados confidenciais constantes nos cadastros da instituição podem ser disponibilizados às empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento desta Política e diretivas de segurança e privacidade de dados, formalizado por meio de assinatura do Contrato de Prestação de Serviços. Além disso, a Redes e Segurança coletará a assinatura do prestador de serviço no Termo de Confidencialidade e Proteção às Informações para Prestadores de Serviço e fará o armazenamento do documento.

Art. 27º Para acesso às dependências do Datacenter da instituição deve ser realizado controle para identificação e registro dos usuários, visando a rastreabilidade. Adicionalmente é recomendado, sempre que possível, que um colaborador da instituição/departamento de Redes e Segurança o acompanhe o visitante durante o seu período de permanência nas dependências da empresa.

Art. 28º O acesso físico aos Servidores e “Appliances” são autorizados somente aos colaboradores da área de Redes e Segurança.

Art. 29º Em auditoria, os auditores são autorizados a terem acesso sempre acompanhados por um colaborador da área de Redes e Segurança.

Art. 30º Em caso de serviços de terceiros a serem realizados a Servidores e “Appliances” faz-se necessário o acompanhamento e aprovação da área de TI e Comitê de Segurança da Informação.

Art. 31º Todo acesso à Servidores e “Appliances” deve ser registrado de forma manual ou automatizada em sistema de controle de acesso.

Art. 32º É proibida a utilização de câmeras fotográficas ou filmadoras, sejam elas acopladas ao smartphone ou não, para fotografar ou filmar dados e informações classificadas como confidenciais, secretas e internas para divulgação ou compartilhamento com terceiros, em qualquer uma das dependências da Empresa salvo em situações inerentes à rotina de trabalho, confraternizações oficiais previamente autorizadas, e/ou situações de emergência em que o uso se faça necessário.

CAPÍTULO VI
MONITORAMENTO E SEGURANÇA

Art. 33º Visando garantir as regras de segurança, a instituição deverá monitorar periodicamente seus processos e sistemas de informação, considerando os procedimentos apresentados:

I. implantação de sistemas de monitoramento nas estações de trabalho, servidores, emails, conexões com a internet, dispositivos móveis ou *wireless* e componentes da rede;

II. informações geradas por sistemas de monitoramento e *logs*, poderão ser usadas para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

III. realização de inspeções físicas nas máquinas de sua propriedade;

IV. instalação de sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações, do ambiente de infraestrutura e dos perímetros de acesso;

V. execução de testes de vulnerabilidade periódicos, com frequência mínima pré acordada pelo Comitê de Segurança da Informação.

CAPÍTULO VII
COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art. 34º O Comitê CSI é um grupo multidisciplinar de diversas áreas da instituição, indicados pela Diretoria, com o intuito de responsável por definir e apoiar estratégias necessárias à implantação e manutenção da Política de Segurança da Informação, sendo suas responsabilidades:

I. validar e propor ajustes, aprimoramentos e modificações desta Política e demais Normas de Segurança da Informação, submetendo a aprovação da Diretoria;

II. estabelecer, revisar e aplicar os conceitos de classificação das informações pertencentes ou sob a guarda da instituição e grupos de acesso a serem aplicados pelos usuários na execução de suas atividades;

III. receber, documentar e analisar casos de violação da Política e das Normas de Segurança da Informação encaminhando-os à Diretoria, quando for o caso;

IV. notificar os gestores e diretores quanto a casos de violação da Política e das Normas de Segurança da Informação;

V. propor projetos e iniciativas relacionadas à melhoria da segurança da informação e privacidade de dados da instituição;

VI. deliberar sobre os temas relacionados à segurança da informação, privacidade e proteção de dados pessoais a ele reportados.

Art. 35º Os critérios de constituição e coordenação, atribuições e funcionamento deste Comitê serão definidos em norma aprovada pela Diretoria.

CAPÍTULO VIII
COMUNICAÇÃO E TREINAMENTOS

Art. 36º As regras e diretrizes definidas nesta Política serão divulgadas a todos usuários por meios oficiais de divulgação da instituição, de maneira que seu conteúdo possa ser consultado a qualquer momento.

Art. 37º Os treinamentos serão realizados pelos departamentos de Informática, Redes e Segurança, Desenvolvimento de Sistemas, OSM/LGPD e DPO quando estes se fazem necessários.

Art. 38º Cabe a cada usuário manter-se atualizado em relação a esta Política e às normas relacionadas, buscando orientação junto ao DPO e/ou ao responsável pela Segurança da Informação, sempre que não estiver seguro quanto à aquisição, uso ou descarte de informações.

CAPÍTULO IX
SANÇÕES

Art. 39º A violação desta política poderá acarretar sanções administrativas e/ou legais, mediante sanções trabalhistas da CLT no caso de colaboradores da instituição, entre o aluno, fornecedor, consultor, assim como qualquer entidade com relação contratual direta ou indireta com a instituição.

Art. 40º A observação do descumprimento desta política deve ser imediatamente reportada por meio do e-mail: comiteseguranca@unipam.edu.br .

CAPÍTULO X
DA SEGURANÇA DA INFORMAÇÃO

Art. 41º A Segurança da Informação é um elemento essencial para a proteção dos ativos de informação da FEPAM, do UNIPAM e do Colégio Universitário, garantindo a confidencialidade, integridade, disponibilidade e autenticidade das informações utilizadas em suas atividades acadêmicas, administrativas e estratégicas. Sua aplicação visa assegurar que documentos institucionais, contratos, registros acadêmicos, informações financeiras e demais dados relevantes sejam protegidos contra acessos não autorizados, perdas, alterações indevidas, vazamentos ou qualquer outra forma de uso inadequado.

Art. 42º No contexto institucional, a Segurança da Informação também desempenha papel fundamental na proteção dos dados pessoais tratados pela instituição, em conformidade com a legislação vigente e as boas práticas de governança. Por meio da adoção de controles, normas e

procedimentos adequados, busca-se preservar a privacidade dos titulares de dados, mitigar riscos operacionais e fortalecer a confiança da comunidade acadêmica, parceiros e demais partes interessadas na gestão responsável das informações.

CAPÍTULO XI
AUDITORIAS E CONFORMIDADES

Art. 43º Como parte de seu modelo de governança, a instituição adotará processos de auditoria e conformidade destinados a avaliar a observância desta Política de Segurança da Informação, dos normativos internos e dos requisitos legais aplicáveis. As auditorias poderão abranger processos, sistemas, recursos tecnológicos e procedimentos relacionados ao tratamento, armazenamento, compartilhamento e proteção das informações institucionais, buscando assegurar a efetividade dos controles de segurança implementados e a adequada gestão dos riscos.

Art. 44º Os processos de monitoramento e conformidade deverão ser realizados periodicamente, sempre que tecnicamente possível, contemplando a manutenção de registros, evidências e demais informações necessárias para demonstrar a observância dos requisitos institucionais, regulatórios e legais. Quando identificadas não conformidades, vulnerabilidades ou oportunidades de melhoria, deverão ser adotadas medidas corretivas e preventivas apropriadas, visando o fortalecimento contínuo da segurança da informação e a proteção das informações institucionais e dos dados pessoais tratados pela instituição.

CAPÍTULO XIII
RESPONSABILIDADES

Art. 45º Quanto às responsabilidades acerca da atribuição da classificação da informação, fica definido que:

I. caberá ao colaborador AUTOR da informação em conjunto com o setor de Redes e Segurança, definir os acessos, níveis de permissão e formas de proteção quando se tratar de uma informação RESTRITA, CONFIDENCIAL ou SECRETA;

II. será considerado como AUTOR da informação o colaborador que primeiro produzir ou manipular a informação dentro do ambiente do UNIPAM;

III. todo colaborador será responsável pela sua classificação e armazenamento, seguindo as recomendações contidas neste documento;

IV. caberá a área de Informática / Redes e Segurança, prover o suporte técnico aos autores das informações geradas e realizar os devidos treinamentos sobre proteção e armazenamento seguro de dados;

V. o Departamento de Redes e Segurança é o provedor dos recursos e meios de armazenamentos seguro dessas informações, assim como as ferramentas de controle de acesso, proteção e disponibilidade;

VI. caberá ao colaborador armazenar os arquivos digitais da instituição obrigatoriamente nos meios fornecidos pela instituição e não nos seus meios pessoais. O Departamento de Redes e Segurança não realiza nenhum tipo de backup de dados armazenados de forma local nos equipamentos e não se responsabiliza por arquivos salvos nos mesmos.

Art. 46º Quanto às responsabilidades referentes às diretrizes de Segurança e Proteção de Dados e Informações, fica estabelecido que:

I. a segurança, proteção e privacidade de dados e informações da instituição ou sob sua responsabilidade são consideradas fatores primordiais nas atividades profissionais do UNIPAM;

II. é responsabilidade de todos os usuários assegurar a integridade e disponibilidade das informações, seja administrador, colaborador ou prestador de serviço da empresa;

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

IV. informações confidenciais, secretas e internas não devem ser expostas publicamente;

V. as informações recebidas pela instituição, devem ser tratadas e armazenadas de forma segura e íntegra;

VI. para as informações em meio digital, os *backups* são feitos diretamente pelo prestador de serviço contratado pela instituição e uma cópia deles deve ser armazenada semanalmente utilizando mecanismos de segurança tecnológica e administrativa suficientes para proteger todos os dados e informações armazenadas;

VII. todos os dados inerentes à instituição devem ser protegidos por meio de rotinas sistemáticas, documentadas, com cópia de segurança, devendo ser submetidos a testes periódicos de recuperação, utilizando mecanismos de segurança tecnológica e administrativa suficientes para proteger todos os dados e informações armazenadas, nos termos estabelecidos na Lei Geral de Proteção de Dados e legislação vigente;

VIII. documentos impressos e arquivos contendo dados pessoais e/ou informações confidenciais, secretas e internas devem ser armazenados e descartados de forma segura, conforme normas internas da instituição;

IX. não é permitido envio de informações ou documento corporativo para e-mails pessoais de colaboradores nem terceiros;

X. de acordo com as regras de permissão de acesso, para aqueles que não tiverem autorização definida, as cópias de qualquer informação ou documento corporativo em dispositivos removíveis, tais como pen drive, HD externo e itens da mesma categoria, deverão ser previamente autorizadas pelo responsável pela Segurança da Informação, tais como Comitê de Segurança da Informação (CSI);

XI. os *softwares* corporativos poderão ser utilizados no ambiente do UNIPAM, somente após homologação do Comitê de Segurança da Informação e validação do DPO, caso aplicável;

XII. os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às devidas permissões de acesso.

Art. 47º Quanto às responsabilidades relacionadas ao descarte de informação classificada, fica estabelecido que:

I. o descarte de informações, armazenadas em meio físico ou digital, deverá ser realizado segundo o procedimento de descarte (vide Política de Retenção e Descarte Institucional, a documentação armazenada no SVN na pasta de cada departamento e, posteriormente, no diretório RSGI aplicável) para garantir que a informação descartada não possa ser recuperada de qualquer forma;

II. além dos demais procedimentos aplicáveis:

a) todas as informações impressas deverão ser trituradas antes de seu descarte; aparelhos eletrônicos devem ser “resetados por padrão de fábrica” antes de seu descarte;

b) informações digitais deverão ser deletadas mediante o uso de ferramentas apropriadas ao descarte de dados mediante auxílio de suporte do departamento de Redes e Segurança.

Art. 48º É responsabilidade de todos aqueles a quem se aplicam esta política:

I. compreender, respeitar e promover os princípios e diretrizes estabelecidos na Política de Segurança da Informação do UNIPAM;

II. assegurar a proteção dos ativos institucionais, sejam eles físicos ou digitais, sob a posse ou responsabilidade da FEPAM e suas mantidas, incluindo todas as

informações e conteúdos, independentemente do formato ou meio de armazenamento, contra qualquer forma de acesso, uso, alteração ou divulgação não autorizados;

III. proteger os recursos institucionais, a identidade visual, a reputação, o capital intelectual e o conhecimento da FEPAM e de suas mantidas, com ênfase na integridade das informações e conteúdos produzidos ou gerenciados pela instituição;

IV. utilizar com responsabilidade e zelo os recursos materiais, tecnológicos e informacionais disponibilizados pela FEPAM, contribuindo para a conservação do patrimônio institucional;

V. não expor de forma indevida, inclusive em redes sociais e na internet, informações institucionais, projetos, atividades e ambientes do UNIPAM. Espera-se uma postura ética e consciente no uso das tecnologias da informação e comunicação;

VI. adotar práticas que previnam ou minimizem os impactos decorrentes de incidentes de segurança, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e conformidade legal das informações da instituição;

VII. manter-se atualizados em relação a esta Política, ao Regimento Interno e às demais normas de segurança da informação do UNIPAM, cumprindo integralmente seus preceitos;

VIII. proteger informações institucionais contra qualquer tipo de acesso indevido, alteração não autorizada, destruição acidental ou proposital, ou divulgação sem o consentimento expresso da FEPAM;

IX. atuar proativamente na prevenção e no combate à intimidação sistemática (bullying), adotando medidas educativas e corretivas que promovam o respeito e a integridade no ambiente acadêmico e profissional;

X. comunicar imediatamente qualquer evento ou suspeita de incidente que possa comprometer a segurança da informação, por meio do canal oficial do UNIPAM destinado a esse fim (e-mail do Comitê de Segurança da Informação comiteseguranca@unipam.edu.br) ou aos departamentos responsáveis.

Art. 49º Quanto às responsabilidades de Gestores e de Coordenadores, dispõe-se que:

I. devem orientar continuamente suas equipes quanto ao uso seguro e responsável dos recursos institucionais, promovendo e fortalecendo a cultura de segurança da informação entre os colaboradores;

II. são responsáveis por garantir que suas equipes cumpram esta política e demais normas aplicáveis, assumindo as consequências das atividades delegadas e supervisionando sua correta execução;

III. devem colaborar com investigações de incidentes de segurança sob sua responsabilidade e participar, quando convocados, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos necessários.

Art. 50º Quanto às responsabilidades dos colaboradores, determina-se que devem:

I. preservar o sigilo profissional e zelar pela imagem e reputação do UNIPAM e de toda a comunidade acadêmica;

II. adotar sempre uma postura respeitosa e apropriada nas interações presenciais ou virtuais com colegas, alunos, visitantes, fornecedores e demais públicos, evitando linguagem ambígua, inapropriada ou que possa caracterizar intimidação, discriminação, abuso de autoridade, ou qualquer forma de assédio;

III. utilizar redes sociais com responsabilidade, evitando publicações que possam comprometer sua própria imagem ou a do UNIPAM, agindo com bom senso e discernimento no ambiente digital.

CAPÍTULO XIV
DISPOSIÇÕES GERAIS

Art. 51º Esta Política de Segurança da Informação reflete o compromisso do UNIPAM com a proteção dos seus ativos, informações e valores institucionais, promovendo um ambiente acadêmico e administrativo seguro e responsável. Todos os colaboradores, alunos e demais integrantes da comunidade devem cumprir rigorosamente suas diretrizes, contribuindo para a preservação da integridade, confidencialidade e disponibilidade dos recursos institucionais. O descumprimento das normas aqui estabelecidas poderá acarretar medidas disciplinares, conforme previsto nas regulamentações internas.

Art. 52º Esta política entrará em vigor a partir da data de sua aprovação pela Diretoria Executiva e permanecerá em vigor por prazo indeterminado.

CAPÍTULO XV
CONFORMIDADE DE REVISÃO

Art. 53º A política será revisada sempre que houver alterações relevantes nos processos, legislações ou tecnologias aplicáveis. Na ausência de mudanças, a revisão será realizada anualmente, garantindo sua atualização e efetividade contínua. O Comitê de Segurança da Informação será responsável pela revisão. Declara-se o compromisso da organização em manter a conformidade com todas as regulamentações aplicáveis relacionadas à segurança de acessos.

ANEXOS

F-55/04 Termo de Confidencialidade e Proteção às Informações para Prestadores de Serviços

HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Alteração Realizada	Motivo da Alteração
Emissão Inicial	10/06/2026	–	–