Política de Segurança da Informação do UNIPAM

LISTA DE ACRÔNIMOS

RS - Redes e Segurança

UNIPAM - Centro Universitário de Patos de Minas

PC - Plano de Contingência
PSI - Política de Segurança da Informação

DS - Desenvolvimento de Sistemas (departamento de desenvolvimento e suporte a ERP e afins)
INFO - Informática (departamento de informática)
ERP - Enterprise Resource Planning (Sistema integrado de gestão empresarial)
CFTVIP - Circuito Fechado de Televisão sobre IP

VPN - Virtual Private Networks

PoP - Point of Presence (Ponto de Presença)

SVN - Sistema de arquivamento e controle de versões de documentos

1. INTRODUÇÃO

1.1. Este documento tem por finalidade estabelecer as diretrizes de segurança da informação que são adotadas pelo UNIPAM.

1.2. Para o cumprimento da finalidade acima mencionada são estabelecidos os objetivos a seguir.

2. OBJETIVOS

A PSI do UNIPAM tem por objetivo:

a. Definir o escopo da segurança da informação do UNIPAM;

b. Orientar as ações de segurança da informação da entidade, reduzindo os riscos e garantindo a integridade, o sigilo e a disponibilidade das informações e recursos;

c. Servir de referência para auditoria, apuração e avaliação de responsabilidades.

3. ABRANGÊNCIA

A PSI abrange:

a. Requisitos de Segurança do Ambiente Físico;

b. Requisitos de Segurança Lógica para as redes (Data Center, CFTVIP, Wi-Fi, DADOS);

c. Requisitos de Segurança de Software para portais e sistemas.

4. TERMINOLOGIA

As diretrizes de segurança devem ser interpretadas de forma que todas as suas determinações sejam obrigatórias e cogentes. Para auxiliar neste propósito, os conceitos e definições utilizadas nesta política são estabelecidos a seguir.

5. CONCEITOS E DEFINIÇÕES

a. **Ativo de Informação** – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos dos departamentos e órgãos ligados ao UNIPAM;

b. **Ativo de Processamento** – é o patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas, serviços e processos dos departamentos e órgãos ligados ao UNIPAM;

c. **Controle de Acesso** – são restrições de acesso às informações de um sistema ou serviço;

d. **Custódia** – consiste na responsabilidade de se guardar um ativo para terceiros. Não necessariamente a custódia permite, automaticamente, o acesso ao ativo, tão pouco o direito de conceder acesso a terceiros;

e. **Direito de Acesso** – é o privilégio associado a um cargo, pessoa, departamento ou processo para ter acesso a um ou mais ativos;

f. **Ferramentas** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a PSI aos departamentos do UNIPAM;

g. **Incidente de Segurança** – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo do UNIPAM;

h. **Política de Segurança da Informação** – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos ou colaboradores do UNIPAM;

i. **Proteção dos Ativos** – é o processo que classifica os ativos quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

j. **Responsabilidade** – são as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

k. **Senha Fraca ou Óbvia** – é aquela que se utiliza de caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tais como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, sequências numéricas simples, palavras com significado em qualquer língua, ou qualquer outro padrão de fácil dedução.

6. REGRAS GERAIS

6.1. Gestão de Segurança

6.1.1. A PSI do UNIPAM aplica-se a todos os recursos humanos, administrativos e tecnológicos a ele relacionados de modo permanente ou temporário;

6.1.2. Esta política é comunicada a todo o pessoal envolvido e largamente divulgada através dos meios de comunicação disponíveis no UNIPAM, garantindo que todos tenham consciência da PSI e a pratiquem na organização;

6.1.3. Todo o pessoal recebe as informações necessárias para cumprir adequadamente o que está determinado na PSI;

6.1.4. O UNIPAM mantém serviços e repositório centralizado para armazenamento de *logs* e demais informações de incidentes, eventos e alertas. A RS é acionada, uma vez que uma tentativa de violação seja detectada, tomando as medidas cabíveis para prover uma defesa ativa e corretiva contra ataques empreendidos contra seus ativos;

6.1.5. Os processos de aquisição de bens e serviços devem estar em conformidade com esta PSI;

6.1.6. É considerada proibida qualquer ação que não esteja explicitamente permitida na PSI do UNIPAM ou que não tenha sido previamente autorizada pela RS.

6.1.7. As violações desta política, salvas as exceções descritas neste documento, são tratadas conforme normas e regimentos descritos nos estatutos do UNIPAM e da FEPAM.

6.2. Gerenciamento de Riscos

O UNIPAM implementa análises de risco periodicamente através de sua própria estrutura.

O processo de gerenciamento de riscos é revisto, no mínimo, a cada 3 (três) meses, para prevenção contra riscos, inclusive advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção dos ativos ameaçados.

6.3. Inventário de ativos

6.3.1. Os ativos de informação e processamento pertencentes à infraestrutura de dados, tais como *switches*, *gateways*, *firewalls*, *proxies*, CFTVIP e servidores que administram esses ativos são inventariados pela RS;

6.3.2. Os inventários relativos a estações de trabalho, monitores e impressoras são mantidos pela Informática;

6.3.3. Os ativos relativos a servidores *web*, sistemas de informação, ERP's e códigos-fonte são mantidos pela DS;

6.4. Plano de Contingência

6.4.1. O UNIPAM possui planos de gerenciamento de incidentes e de ação de resposta aos incidentes aprovados pela diretoria;

6.4.2. Incidentes de alta criticidade são reportados de modo sigiloso ao Time de Gerenciamento de Crises do UNIPAM, definido no Plano de Contingência.

7. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

7.1. Definição

Ambiente físico é aquele composto por todo o ativo permanente do UNIPAM.

7.2. Diretrizes Gerais

7.2.1. A responsabilidade pela segurança física dos ambientes aos cuidados da RS, quando há compartilhamento de ambientes, é definida, em documento próprio, indicando os demais responsáveis e suas atribuições;

7.2.2. Essas instalações são identificadas, de acordo com a natureza de cada local e de acordo com os normativos de identificação vigentes;

7.2.3. Perdas de chaves de acesso são imediatamente comunicadas à RS e ao outro departamento responsável. Ambos adotarão medidas apropriadas para prevenir acessos não-autorizados;

7.2.4. Recursos e instalações críticas ou sensíveis devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência, com barreiras de segurança e controle de acesso. A proteção deve ser proporcional aos riscos identificados.

7.2.5. O acesso aos componentes da infraestrutura, atividade fundamental ao funcionamento dos sistemas do UNIPAM, como painéis de controle de energia, comunicações e cabeamento, é restrito ao pessoal da RS e a outros departamentos e terceiros, identificados e autorizados, previamente, pela RS.

7.2.6. São utilizados sistemas de detecção de intrusão (ex.: câmera ou sensor) para monitorar e registrar os acessos físicos aos componentes críticos da infraestrutura, conforme classificação feita pela RS;

7.2.7. O inventário de todo o conjunto de ativos de processamento é registrado e mantido atualizado, trimestralmente;

7.2.8. Quaisquer equipamentos, relacionados às redes (DADOS e Wi-Fi), ao CFTVIP e ao Data Center ou outro tipo de equipamento similar, só são utilizados a partir de autorização formal da RS;

7.2.9. Nas instalações ou ambientes de acesso restrito do UNIPAM, todos utilizam crachá de identificação e devem informar à RS e à Vigilância Patrimonial sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado nas áreas de acesso restrito;

8. Requisitos de segurança do ambiente lógico para rede Wi-Fi, rede DADOS, CFTVIP e Data Center

8.1. Definição

Ambiente lógico é composto por todo o ativo de informações do UNIPAM que se encontra no domínio das redes (Wi-Fi, CFTVIP, DADOS e Data Center).

8.2. Diretrizes gerais

8.2.1. Os dados, as informações e os sistemas de informação do UNIPAM e sob sua guarda são protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens;

8.2.2. As violações de segurança são registradas e esses registros são analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria;

8.2.3. Cada tipo de registro (*log*) é analisado com forma e periodicidade própria de acordo com sua natureza, procedimento este realizado pela RS.

8.2.4. Os sistemas e recursos que suportam funções críticas para operação do UNIPAM asseguram a capacidade de recuperação nos prazos e condições definidas em situações de contingência;

8.3. Diretrizes específicas

8.3.1. Sistemas

8.3.1.1. Os sistemas possuem controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização é claramente definido e registrado. As autorizações devem ser realizadas segundo sua criticidade:

- ❏ Usuários só poderão ter acesso a sistemas se estiverem de posse de suas credenciais (usuário e senha);
- ❏ Credenciais de acesso só podem ser obtidas por meio dos sistemas UNISEGURANÇA ou UNIUSUÁRIOS ou por sistemas automatizados de cadastro de usuários (ex.: biometria);
- ❏ Exceções só poderão ser autorizadas pela RS.

8.3.1.2. Os arquivos de *logs* são definidos de forma a permitir recuperação nas situações de falhas, auditorias nas situações de violações de segurança e auditoria do uso de recursos. Os *logs* são analisados periodicamente, para identificar tendências, falhas ou usos indevidos. Os

logs devem ser protegidos e armazenados de acordo com sua classificação;

8.3.1.3. Alterações ou modificações, de qualquer natureza, bem como autorizações de acesso, sob os cuidados da DS, dependem de autorização formal e expressa da mesma.

8.3.2. Máquinas servidoras

8.3.2.1. O acesso lógico ao ambiente ou serviços disponíveis em servidores é controlado e protegido. O responsável pela autorização ou confirmação da autorização é claramente definido e registrado. Todas as exceções devem ser aprovadas pela RS.

8.3.2.2. Os arquivos de *log* são armazenados em servidor específico. O tempo de retenção desse logs é de 1 (um) ano. Nesse servidor o sistema de controle de acesso aos *logs* é feito através de mecanismos de autenticação.

8.3.2.3. São adotados procedimentos para monitorar a segurança do ambiente operacional. Todos os registros são mantidos pela RS em local seguro e centralizado.

8.3.2.4. São utilizados somente *softwares* autorizados pelo UNIPAM nos seus equipamentos. É realizado o controle da distribuição e instalação dos mesmos.

8.3.2.5. O acesso remoto a máquinas servidoras é realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço.

8.3.2.6. Os procedimentos de cópia de segurança (*backup*) e de recuperação estão documentados, atualizados e são regularmente testados, de modo a garantir a disponibilidade das informações.

8.3.2.7. A conexão de novos servidores às redes, sejam físicos ou virtuais, dependem de ação, análise e autorização prévia da RS.

8.3.3. Redes do UNIPAM

8.3.3.1. O tráfego das informações no ambiente de rede é protegido contra danos ou perdas, bem como acesso, uso ou exposição indevido.

8.3.3.2. Componentes críticos das redes são mantidos em salas protegidas e com acesso físico e lógico controlados, sendo protegidos contra danos, furtos, roubos e intempéries. Os servidores devem ser mantidos no mesmo nível de segurança das informações que eles armazenam.

8.3.3.3. Serviços vulneráveis são eliminados ou trocados por similares mais seguros, quando cabível. Exceções a este item devem ser devidamente justificadas e registradas.

8.3.3.4. O acesso lógico aos recursos das redes é realizado por meio de sistema de controle de acesso. O acesso é concedido e mantido pela RS, baseado nas responsabilidades e tarefas de cada usuário.

8.3.3.5. A utilização de qualquer mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, monitoração sobre os dados, os sistemas e dispositivos que compõem a rede, só ocorrem a partir de autorização formal da RS e mediante supervisão.

8.3.3.6. A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração são formalmente documentadas e mantidas, de forma a permitir registro histórico, e tem a autorização da RS. A configuração e o inventário dos recursos são mantidos atualizados.

8.3.3.7. São definidos relatórios de segurança (*logs*) periódicos de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Tais relatórios são disponibilizados e armazenados de maneira segura. As anormalidades identificadas nestes relatórios são tratadas segundo a sua severidade. Entre elas, inclui-se:

- ❏ Ataques Externos e Internos;
- ❏ Utilização indevida de Recursos.

8.3.3.8. São adotadas proteções físicas adicionais para os recursos de rede considerados críticos.

8.3.3.9. Proteção lógica adicional é adotada para evitar o acesso não autorizado às informações.

8.3.3.10. O tráfego de informações é monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.

8.3.3.11. Devem ser observadas as questões envolvendo propriedade intelectual quando da cópia de *software* ou arquivos de outras localidades.

8.3.3.12. Todo serviço de rede não explicitamente autorizado deve ser bloqueado ou desabilitado.

8.3.3.13. Mecanismos de segurança baseados em sistemas de proteção de acesso (*firewall*) são utilizados para proteger as transações entre redes externas e as redes do UNIPAM.

8.3.3.14. Os registros de eventos são analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados.

8.3.3.15. Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, fazem uso de tal controle.

8.3.3.16. A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) é resultante de uma análise de riscos. No mínimo os seguintes aspectos são considerados:

- ❏ Requisitos de segurança definidos pelo serviço;
- ❏ Objetivo do serviço;
- ❏ Público-alvo;
- ❏ Classificação da informação;
- ❏ Forma de acesso;
- ❏ Frequência de atualização do conteúdo;
- ❏ Forma de administração do serviço;

- ❏ Volume de tráfego.

8.3.3.17. Ambientes de rede considerados críticos são isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança.

8.3.3.18. Conexões originadas em redes externas, com destino às redes do UNIPAM, estão restritas somente àquelas que visem efetivar os processos necessários à operação do UNIPAM.

8.3.3.19. A infraestrutura do UNIPAM é segmentada em diversos *gateways* e *firewalls*, que realizam a proteção e conectividade entre os blocos e departamentos.

8.3.3.20. Alterações ou modificações, de qualquer natureza, aplicadas às redes de Wi-Fi, DADOS, CFTVIP ou Data Center, são realizadas ou acompanhadas pela RS.

8.3.4. Controle de acesso lógico

8.3.4.1. Usuários e aplicações que necessitem ter acesso a recursos do UNIPAM são identificados e autenticados.

8.3.4.2. É expressamente proibido que um usuário obtenha direitos de acesso de outro usuário.

8.3.4.3. As autorizações são definidas de acordo com a necessidade de desempenho das funções e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas);

8.3.4.4. As senhas são individuais, secretas, intransferíveis e protegidas com grau de segurança compatível com a informação associada;

8.3.4.5. A distribuição de senhas (iniciais ou não) aos usuários é feita de forma segura.

8.3.4.6. O sistema de controle de acesso permite ao usuário alterar sua senha sempre que desejar.

8.3.4.7. Os usuários e administradores do sistema de controle de acesso são formal e expressamente conscientizados de

suas responsabilidades, mediante assinatura de termo de compromisso.

8.3.5. Computação pessoal

8.3.5.1. O termo computação pessoal refere-se a equipamentos geridos pelo UNIPAM e que são usados por usuários finais (*endpoints*).

8.3.5.2. As informações armazenadas em meios eletrônicos são protegidas contra danos, furtos ou roubos, sendo adotados procedimentos de *backup*, definidos em documento específico.

8.3.5.3. O acesso às informações atende aos requisitos de segurança, considerando o ambiente e a forma de uso do equipamento (individual ou coletivo).

8.3.5.4. Apenas *softwares* licenciados pelo fabricante podem ser utilizados nos equipamentos do UNIPAM.

8.3.5.5. O inventário dos recursos é mantido atualizado.

8.3.5.6. A movimentação ou a instalação de estações de trabalho, na rede cabeada, só podem ser feitas pela Informática ou com autorização formal da mesma. A RS deve ser comunicada formalmente e, somente após a atualização cadastral dessa estação, a liberação é realizada.

8.3.5.7. Cabe à Informática realizar alterações físicas ou lógicas em estações de trabalho. Dispositivos de rede que provêm conectividade para as estações são permitidos somente após autorização formal da RS. Tal medida visa garantir a integridade e a segmentação de redes com controles de acesso e riscos distintos.

8.3.5.8. O uso da rede Wi-Fi está sujeito a condições adicionais de uso, conforme documentação disponível em https://wifi.unipam.edu.br.

8.3.6. Computação em nuvem

8.3.6.1. Computação em nuvem refere-se a sistemas, aplicações e afins, executados em sistemas computacionais não

controlados diretamente pelo UNIPAM. Podem ser aplicações isoladas e com finalidades específicas (ex.: sistema VETUS) bem como aplicações de propósito geral (ex.: Google Suite para Educação).

8.3.6.2. A adoção de sistemas desta natureza deverá ser avaliada por comissão nomeada e autorizada pela direção do UNIPAM. Os casos que não cumpram esta PSI deverão ser autorizados, em caráter de exceção e formalmente identificados e a RS deverá ser notificada.

8.3.7. Combate a Vírus de Computador

Os procedimentos de combate a processos destrutivos (*vírus, ransomwares e worms*) são sistematizados e englobam servidores (quando justificado) e estações de trabalho.

8.3.8. Controle e filtro de endereços

O UNIPAM realiza o filtro de endereços *web* (filtro de *URL*), na rede DADOS, impedindo o acesso a endereços da *internet* que podem prejudicar seus ativos, seus serviços ou aos colaboradores. Com esse intuito, é definido que:

8.3.8.1. Colaboradores sem credenciais de acesso possuem sua navegação bloqueada.

8.3.8.2. Exceções ao item 8.3.8.1 devem ser devidamente justificadas e registradas através de uma solicitação formal para a RS.

8.3.8.3. Endereços da internet que endossam atos, conteúdos ou práticas consideradas como criminosas perante a legislação vigente, são considerados como proibidos mesmo que não estejam previamente filtrados.

8.3.8.4. Políticas de uso complementares poderão ser definidas em documento próprio, visando determinar condições adicionais de uso.

9. AUDITORIA

9.1. As atividades do UNIPAM estão associadas ao conceito de padronização de procedimentos. A auditoria periódica representa um dos instrumentos que permite a identificação de processos que podem

ser aperfeiçoados. Um dos objetivos desses processos é verificar a capacidade do UNIPAM em atender a comunidade acadêmica e a sociedade.

9.2. O UNIPAM possui um Sistema de Gestão Integrada (SGI), que trata-se de um conjunto de práticas inter-relacionadas e em constante comunicação, que permite a melhoria contínua dos processos da instituição, o desenvolvimento de políticas e práticas ambientalmente sustentáveis, o gerenciamento dos riscos ocupacionais e a aplicação de técnicas socialmente aceitáveis no ambiente de trabalho.

9.3. São realizadas auditorias internas e externas, periodicamente, no UNIPAM. O UNIPAM mantêm capacitada uma equipe de colaboradores que realizam as auditorias internas. Também existe uma auditoria externa, anualmente, para comprovar a melhoria dos processos. Os critérios estabelecidos para as atividades de auditorias podem ser verificados no PS-8.2.2/01 Auditorias Internas do SGI, disponível no SVN do UNIPAM. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

10. GERENCIAMENTO DE RISCOS

10.1. Definição

Processo que visa à proteção dos serviços do UNIPAM, por meio da eliminação, redução ou transferência dos riscos. Os seguintes pontos principais são identificados:

a. O que deve ser protegido;

b. Análise de riscos (contra quem ou contra o quê deve ser protegido);

c. Avaliação de riscos (análise da relação custo/benefício).

10.2. Fases Principais

O gerenciamento de riscos consiste das seguintes fases principais:

a. Identificação dos recursos a serem protegidos – *hardware*, rede, *software*, dados, informações pessoais, documentação, suprimentos etc;

b. Identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligências) ou de qualquer outro tipo (incêndios);

c. Análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;

d. Avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais;

e. Tratamento dos riscos (medidas a serem adotadas) - como lidar com as ameaças. As principais alternativas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco;

f. Reavaliação periódica dos riscos em intervalos de tempo não superiores a 6 (seis) meses.

10.3. Riscos relacionados ao UNIPAM

Os principais riscos avaliados para o UNIPAM compreendem, dentre outros, os seguintes:

Segmento	Riscos
Informação	Indisponibilidade, Interrupção (perda), interceptação, modificação, fabricação, destruição.
Pessoas	Omissão, erro, negligência, imprudência, imperícia, desídia, sabotagem, perda de conhecimento.
Rede	*Hacker*, acesso não autorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço.
Hardware	Indisponibilidade, interceptação (furto ou roubo) ou falha.
Software	Interrupção, interceptação, modificação, desenvolvimento ou falha.

10.4. Considerações Gerais

10.4.1. Os riscos que não podem ser eliminados têm seus controles documentados pelos responsáveis e são levados ao conhecimento da RS;

10.4.2. Um efetivo gerenciamento dos riscos permite decidir se o custo de prevenir um risco (medida de proteção) é mais alto que o custo das consequências do risco (impacto da perda);

10.4.3. É necessária a participação e o envolvimento da alta administração do UNIPAM.

11. Plano de Contingência

11.1. Definição

Plano cujo objetivo é manter em funcionamento os serviços e processos críticos do UNIPAM, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.

11.2. Diretrizes Gerais

11.2.1. Dispositivos redundantes estão disponíveis para garantir a continuidade da operação do Data Center.

11.2.2. O UNIPAM possui seu Plano de Contingência que estabelece o tratamento adequado dos seguintes eventos de segurança:

a. Invasão do sistema e da rede interna do UNIPAM;

b. Incidentes de segurança física e lógica;

c. Indisponibilidade da Infraestrutura;

d. Indisponibilidade de Portais e Sistemas.

11.2.3. O UNIPAM possui um plano de ação de resposta a incidentes prevendo o tratamento adequado dos seguintes eventos:

a. Procedimentos para interrupção ou suspensão de serviços e investigação;

b. Análise e monitoramento de trilhas de auditoria.