Política de Segurança da Informação da Universidade Progressus

Versão: 1.0

Classificação: Interna

Última revisão: 15 de Junho de 2024

Índice

1. Introdução

A Universidade Progressus é uma instituição de ensino, que tem por finalidade a formação de qualidade, pesquisa, inovação, desenvolvimento econômico e cultural, tem como missão a contribuição para o progresso social e individual. Através do ensino de excelência, pesquisas e extensões.

Com o avanço tecnológico e a crescente aplicação da internet no dia a dia da instituição, é essencial estabelecer parâmetros para padronizar e normatizar a segurança no âmbito humano e tecnológico, para que seja garantida a qualidade de ensino e o acesso à informação.

Portanto, como forma de reconhecer a importância da segurança da informação para a proteção de dados e ativos contra as ameaças e vulnerabilidades, a Universidade Progressus apresenta neste documento diretrizes, normas e procedimentos propostos à proteção da informação.

2. Objetivos

A Política de Segurança da Informação (PSI) é aplicável ao ambiente estudantil, acadêmico e administrativo e tem por objetivos:

- Estabelecer diretrizes estratégicas e princípios para a proteção dos ativos tangíveis e intangíveis.
- Nortear a tomada de decisão e a realização das atividades profissionais e educacionais de todos os colaboradores.
- Construir uma cultura de uso seguro das informações.
- Preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade das informações.
- Definir normas e procedimentos específicos de segurança da informação.

3. Abrangência

Esta PSI é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os alunos e colaboradores, para os ambientes estudantil, acadêmico e administrativo, que venham a ter acesso e/ou utilizam as informações, os recursos de TIC e/ou demais ativos tangíveis ou intangíveis da universidade.

4. Diretrizes Gerais

4.1 Interpretação

4.1.1 Para efeito desta PSI, são adotadas as siglas, os termos e definições constantes no Apêndice A.

4.1.2 Esta PSI deve ser interpretada de forma restritiva, com casos excepcionais necessitando autorização prévia.

4.2 Propriedade

4.2.1 As informações geradas, acessadas, recebidas, manuseadas e armazenadas são de propriedade e de direito de uso exclusivo da universidade.

4.2.2 Os recursos de TIC fornecidos para atividades educacionais e profissionais são de propriedade da universidade.

4.2.3 Todos os ativos tangíveis e intangíveis da universidade devem ser utilizados apenas para fins institucionais. 4.2.4 A utilização das marcas, identidade visual e demais sinais distintivos da universidade devem ser autorizados previamente.

4.3 Classificação da Informação

4.3.1 As informações devem ser classificadas como:

- **Públicas**: Podem ser divulgadas sem restrições.
- **Internas**: Devem ser acessadas apenas por membros da universidade.
- **Confidenciais**: Requerem tratamento especial e acesso restrito.

4.3.2 Informações não públicas devem ser rotuladas no momento de sua criação.

4.3.3 Colaboradores devem tratar todas as informações não rotuladas como internas até que a classificação correta seja determinada.

4.3.4 Dados pessoais e informações sensíveis devem ser protegidos com mecanismos de segurança adequados, como criptografia.

4.4 Controle de Acesso

4.4.1 Cada aluno e colaborador receberá uma identidade digital individual e intransferível.

4.4.2 Identidades digitais são monitoradas e controladas pela equipe de TI.

4.4.3 O acesso a áreas físicas críticas é restrito a indivíduos autorizados e deve ser protegido por medidas de segurança apropriadas, como controle de acesso por crachá.

4.4.4 Logs de acesso devem ser mantidos para auditoria e revisão periódica.

4.5 Internet

4.5.1 O acesso à internet é concedido para fins educacionais e administrativos, e deve ser utilizado em conformidade com as leis vigentes e políticas institucionais.

4.5.2 É proibido o acesso a sites com conteúdo impróprio, ilegal ou que possam comprometer a segurança da informação.

4.6 Correio Eletrônico

4.6.1 O uso do correio eletrônico deve ser restrito a atividades educacionais e profissionais.

4.6.2 Correios eletrônicos devem ser protegidos contra spam, phishing e outras ameaças.

4.6.3 Mensagens de correio eletrônico devem ser arquivadas de acordo com as políticas de retenção de dados.

4.7 Rede Sem Fio (Wi-Fi)

4.7.1 A universidade oferece rede sem fio para finalidades educacionais e administrativas.

4.7.2 Apenas usuários autorizados podem acessar a rede sem fio.

4.7.3 Redes sem fio devem ser protegidas por senhas fortes e mecanismos de criptografia.

4.8 Recursos de TIC Institucionais

4.8.1 Recursos de TIC são destinados a finalidades educacionais e profissionais.

4.8.2 É vedado o armazenamento de arquivos pessoais nos recursos de TIC da universidade.

4.8.3 Os arquivos institucionais devem ser armazenados em servidores dedicados, com backup regular.

4.8.4 A equipe de TI é responsável pela manutenção e atualização dos recursos de TIC.

4.9 Recursos de TIC Particulares

4.9.1 A conexão de recursos de TIC particulares à rede da universidade é restrita e deve seguir diretrizes específicas.

4.9.2 Dispositivos móveis particulares devem ser protegidos com senhas e softwares de segurança.

4.9.3 É proibido o uso de dispositivos particulares para armazenar informações confidenciais da universidade sem autorização.

4.10 Armazenamento de Informações

4.10.1 Informações devem ser armazenadas nos locais apropriados e destinados a esse fim.

4.10.2 A universidade pode solicitar a remoção de conteúdos que ofereçam riscos ou violem normas.

4.10.3 Dados sensíveis devem ser armazenados com criptografia e acesso restrito.

4.11 Repositórios Digitais

4.11.1 Repositórios digitais são destinados ao armazenamento e compartilhamento de informações institucionais.

4.11.2 É vedado armazenar informações institucionais em repositórios digitais particulares.

4.11.3 Acesso a repositórios digitais deve ser controlado e monitorado.

4.12 Mídias Sociais

4.12.1 O uso de mídias sociais deve ser responsável e conforme os direitos e deveres estabelecidos pela universidade.

4.12.2 É proibido compartilhar informações confidenciais ou sensíveis da universidade em mídias sociais.

4.13 Mesa Limpa e Tela Limpa

4.13.1 Informações da universidade não devem ficar expostas em áreas comuns ou de trânsito de pessoas.

4.13.2 Colaboradores devem bloquear suas estações de trabalho ao se afastar.

4.13.3 Documentos confidenciais devem ser guardados em locais seguros quando não estiverem em uso.

4.14 Áudio, Vídeos e Fotos

4.14.1 A captura de imagens, vídeos ou áudios deve ser previamente autorizada pela universidade.

4.14.2 É proibido compartilhar gravações sem autorização expressa.

4.15 Uso de Imagem, Som da Voz e Nome

4.15.1 A universidade pode usar a imagem dos alunos para fins institucionais, respeitando a integridade dos envolvidos.

4.15.2 O uso de imagens deve ser feito de forma a não expor os indivíduos ao ridículo ou constrangimento.

4.16 Aplicativos de Comunicação

4.16.1 O uso de aplicativos de comunicação deve ser feito de forma responsável e segura.

4.16.2 Informações sensíveis não devem ser compartilhadas por aplicativos de comunicação sem medidas de segurança adequadas.

4.17 Monitoramento

4.17.1 A universidade realiza o monitoramento de atividades para proteger seus ambientes físicos e lógicos.

4.17.2 Logs de monitoramento são mantidos para análise e auditoria.

4.18 Combate à Intimidação Sistemática (Bullying)

4.18.1 Todos devem participar de campanhas contra a violência e intimidação sistemática.

4.18.2 Incidentes de bullying devem ser reportados imediatamente às autoridades competentes da universidade.

4.19 Contratos de Trabalho e de Prestação de Serviços

4.19.1 A GTI deve desativar as identidades digitais de alunos ou colaboradores desligados.

4.19.2 Alunos ou colaboradores devem excluir informações institucionais de dispositivos particulares ao término do contrato.

4.19.3 Contratos de prestação de serviços devem incluir cláusulas de confidencialidade e segurança da informação.

4.20 Segurança da Informação

4.20.1 Informações devem ser transmitidas com cautela, confirmando a identidade do solicitante.

4.20.2 A universidade mantém processos de salvaguarda e restauração de arquivos críticos.

4.20.3 Dados descartados devem ser destruídos de forma segura para impedir a recuperação.

5. Papéis e Responsabilidades

5.1 Todos

5.1.1 Conhecer e disseminar as regras da Política de Segurança da Informação.

5.1.2 Proteger os ativos tangíveis e intangíveis da universidade.

5.1.3 Reportar incidentes de segurança imediatamente.

5.1.4 Participar de programas de treinamento e conscientização sobre segurança da informação.

5.2 Gestores e Coordenadores

5.2.1 Orientar suas equipes quanto ao uso seguro dos ativos e informações da universidade.

5.2.2 Assegurar o cumprimento das políticas de segurança da informação em suas áreas de responsabilidade.

5.2.3 Participar da investigação de incidentes de segurança relacionados às suas equipes.

5.3 Colaboradores

5.3.1 Utilizar mídias sociais com responsabilidade e preservar a imagem da universidade.

5.3.2 Cumprir todas as diretrizes e práticas estabelecidas na política de segurança da informação.

5.3.3 Reportar imediatamente qualquer incidente ou suspeita de violação de segurança.

6. Disposições Finais

Este documento deve ser interpretado conforme as leis brasileiras e em conjunto com outras normas da universidade. Quaisquer infrações estão sujeitas a sanções previstas nos contratos e normas institucionais.

7. Documentos de Referência

- ABNT NBR ISO/IEC 27001:2013
- ABNT NBR ISO/IEC 27002:2013
- ABNT NBR ISO/IEC 27014:2013
- Norma ISO/IEC 27005:2011
- COBIT 5® Foundation

8. Apêndice

A – Siglas, Termos e Definições

A

- **Ativo**: Qualquer coisa que tenha valor para a instituição e precisa ser adequadamente protegida.
- **Ameaça**: Causa potencial de um incidente indesejado, que pode resultar em dano à instituição.

B

- **Backup**: Salvaguarda de sistemas ou arquivos, realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de retorno.

C

- **Confidencialidade**: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e sejam devidamente protegidas do conhecimento alheio.
- **CRC**: Centro de Recursos Computacionais, vinculado ao ICEI.

D

- **Dados**: Conjunto de fatos, valores ou ocorrências em estado bruto, que, quando processados ou agrupados, produzem informações.
- **Datacenter**: Ambiente altamente crítico, projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede.

E

- **Encriptação**: Processo de codificação de informações para proteger seu conteúdo durante a transmissão e armazenamento.

F

- **Firewall**: Dispositivo de segurança de uma rede de computadores que monitora, autoriza e bloqueia o tráfego que entra e sai da rede.

I

- **Integridade**: Garantia de que as informações estejam íntegras durante o seu ciclo de vida.
- **Identidade Digital**: Identificação do usuário em ambientes lógicos, sendo composta por login e senha ou por outros mecanismos de identificação e autenticação.

M

- **Monitoramento**: Processo de registro e análise de atividades em sistemas de informação para garantir segurança e conformidade.

R

- **Risco**: Possibilidade de uma ameaça explorar uma vulnerabilidade de um ativo para prejudicar a instituição.
- **Recursos de TIC**: Todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação.

S

- **Segurança da Informação**: Preservação da confidencialidade, integridade e disponibilidade da informação na instituição.

W

- **Wi-Fi**: Abreviação de Wireless Fidelity, tecnologia de comunicação sem fio.

A – Procedimentos

Controle de Acesso: O controle de acesso tem como objetivo a restrição do acesso de dados confidenciais da Universidade para usuários devidamente autorizados, para seu cumprimento, sendo necessário a aplicação das seguintes medidas:

- **Autenticação Multifator (MFA):** Autenticação através de dois ou mais fatores, por senhas, biometrias, tokens físicos, aplicativos de autorização, em que o usuário somente terá seu acesso liberado após cumprir todas as exigências de autenticação;

- **Níveis de Acesso:** Os usuários terão seus níveis atribuídos de acordo com sua atuação dentro da universidade, podendo haver bloqueios de acesso caso não tenha o acesso autorizado;

- Monitoramento: Documentos de acompanhamento das atividades que foram realizadas, cada acesso devidamente registrado para que o setor responsável analise, verifique e gere relatórios.

Segurança Cibernética: A segurança cibernética tem como objetivo proteger os servidores da Universidade Progressus contra os ataques cibernéticos, como malwares, spywares, DoS, phishing e invasões, sendo necessário a aplicação das seguintes medidas:

- **Softwares de Segurança:** A instalação de softwares de segurança que analisem e verifiquem os possíveis ataques que podem ocorrer aos servidores da universidade, como antivírus, firewall e anti-malwares;

- **Testes de Vulnerabilidade:** Deve ser feito periodicamente pela Universidade testes que verifiquem falhas de segurança nos servidores, para que possam ser identificados e corrigidos;

- **Políticas de Segurança da Rede:** A rede deve ter regras que possam proteger e limitar os acessos de pessoas e serviços não autorizados, para que evite possíveis ataques.

Backup de Dados: O backup de dados tem como objetivo a garantia da recuperação e manutenção dos dados da Universidade de maneira segura, para cenários de perda, sinistros ou falhas do sistema, sendo necessário a aplicação das seguintes medidas:

- **Rotina de Backup:** O backup deve ser feito periodicamente, podendo sendo escolhido o tipo incremental, sua frequência deverá ser diária e os dados serão mantidos em um servidor físico interno da Universidade, e um servidor na nuvem pago;

- **Teste de Backups:** Os backups feitos anteriormente devem ser verificados e analisados se estão com os dados corretos, e se estão podendo ser recuperados do seu servidor de origem para outro servidor, como forma de garantir a sua qualidade;

- **Plano de Recuperação de Sinistros:** A Universidade deve ter um plano visando o acontecimento de desastres, no qual pode ocorrer a perca massiva de dados armazenados no servidor in loco, tendo que ser feita a recuperação de dados de acordo com o armazenamento em nuvem pago.

Proteção de Informações Estratégicas: A existência de dados estratégicos da Universidade mostra a necessidade de aplicação de regras que tenham como objetivo a garantia da confidencialidade e integridade dessas informações, para a sua aplicação devem ser aplicadas as seguintes medidas:

- **Classificação de Informações:** Os dados contidos no armazenamento dos servidores da Universidade devem ser classificados como dados de pessoas, financeiros, pesquisas, infraestrutura, ensino, reputação e segurança, para que possam ser distinguidos de acordo com a sua confidencialidade;

- **Controle de Acesso:** A visualização dos dados deve ser permitida de acordo com o nível atribuído a pessoa, para que haja a restrição de acesso caso o usuário não possua autorização;

- **Criptografia de Informações:** As informações dos tipos: pessoas, financeiros, infraestrutura e segurança devem ser criptografados;