UNIVERSIDADE
PROGRESSUS

CARTILHA DE SEGURANÇA DA INFORMAÇÃO

O QUE É A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)?

A Política de Segurança da Informação (PSI) da Universidade Progressus estabelece diretrizes e responsabilidades para proteger nossos dados e ativos de informação contra ameaças e vulnerabilidades. Esta política é aplicável a todos os funcionários, alunos, contratados e parceiros que utilizam nossos recursos de informação.

• ABRANGÊNCIA

A PSI se aplica a todos os alunos, colaboradores, contratados e parceiros da Universidade Progressus, abrangendo todos os ambientes estudantis, acadêmicos e administrativos.

• OBJETIVOS DA PSI

- **Proteção de Ativos:** Garantir a proteção de todos os ativos tangíveis e intangíveis, como dados, sistemas, redes e a reputação da universidade.
- **Cultura de Segurança:** Promover uma cultura de segurança da informação entre todos os membros da universidade.
- **Conformidade Legal:** Assegurar que todas as práticas de segurança da informação estejam em conformidade com as leis e regulamentos aplicáveis.
- **Confidencialidade, Integridade e Disponibilidade:** Proteger a confidencialidade, integridade e disponibilidade das informações.

DIRETRIZES GERAIS

1. Interpretação

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

2. Propriedade

Todas as informações geradas, acessadas, recebidas, manuseadas ou armazenadassão de propriedade da universidade. Os recursos de TIC devem ser utilizados apenas para fins institucionais.

3. Classificação da Informação

Informações devem ser classificadas como públicas, internas ou confidenciais. Dados pessoais e informações sensíveis devem ser protegidos adequadamente.

4. Controle de Acesso

Cada usuário recebe uma identidade digital individual e intransferível. Acesso a áreas físicas e digitais é monitorado e controlado.

5. Uso da Internet

O acesso à internet deve ser utilizado para fins educacionais e administrativos,respeitando as leis e políticas institucionais. É proibido acessar sites com conteúdo impróprio ou ilegal.

6. Correio Eletrônico

O uso do correio eletrônico é restrito a atividades educacionais e profissionais. Proteja suas contas de e-mail contra ameaças como spam e phishing.

7. Rede Sem Fio (Wi-Fi)

A rede Wi-Fi da universidade é destinada a fins educacionais e administrativos. Acesso à rede é permitido apenas a usuários autorizados e deve ser protegido por senhas fortes.

8. Recursos de TIC Institucionais

Recursos de TIC são para uso educacional e profissional. Arquivos institucionais devem ser armazenados em servidores dedicados com backup regular.

DIRETRIZES GERAIS

9. Recursos de TIC Particulares

A conexão de dispositivos pessoais à rede da universidade é restrita e deve seguir diretrizes específicas. Dispositivos pessoais não devem armazenar informações confidenciais sem autorização.

10. Armazenamento de Informações

Informações devem ser armazenadas em locais apropriados e seguros. Dados sensíveis devem ser protegidos com criptografia.

11. Repositórios Digitais

Repositórios digitais são para armazenamento de informações institucionais. É proibido armazenar informações da universidade em repositórios pessoais.

12. Mídias Sociais

Utilize mídias sociais de forma responsável, sem compartilhar informações confidenciais da universidade.

13. Mesa Limpa e Tela Limpa

Não deixe informações da universidade expostas em áreas comuns. Bloqueie suas estações de trabalho ao se afastar.

14. Áudio, Vídeos e Fotos

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

15. Uso de Imagem, Voz e Nome

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

16. Aplicativos de Comunicação

Use aplicativos de comunicação de forma responsável e segura

17. Monitoramento

A universidade monitora atividades para proteger seus ambientes físicos e digitais.

18. Combate ao Bullying

Participe de campanhas contra bullying e reporte incidentes imediatamente.

DIRETRIZES GERAIS

19. Contratos de Trabalho e de Prestação de Serviços

Identidades digitais de ex-alunos e ex-colaboradores são desativadas ao término do vínculo. Exclua informações institucionais de dispositivos pessoais após o término do contrato.

20. Segurança da Informação

Transmita informações com cautela e confirme a identidade do solicitante. Descarte dados de forma segura para impedir recuperação não autorizada.

PAPÉIS E RESPONSABILIDADES

TODOS

- Conhecer e seguir as diretrizes da PSI.
- Proteger os ativos da universidade.
- Reportar incidentes de segurança imediatamente.
- Participar de programas de treinamento e conscientização.

GESTORES E COORDENADORES

- Orientar suas equipes sobre o uso seguro dos ativos e informações.
- Assegurar o cumprimento da PSI em suas áreas.
- Participar da investigação de incidentes de segurança.

COLABORADORES

- Utilizar mídias sociais com responsabilidade.
- Seguir todas as diretrizes de segurança da informação.
- Reportar qualquer incidente ou suspeita de violação de segurança.

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

Para mais informações ou dúvidas sobre a Política de Segurança da Informação, entre em contato com a equipe de TI da Universidade Progressus.

Esta cartilha foi desenvolvida para ajudar você a entender e seguir as principais diretrizes da nossa Política de Segurança da Informação. Proteger nossas informações é uma responsabilidade de todos.
Contamos com a sua colaboração