Programa de Conscientização Para o Uso Seguro da Internet

Programa de Conscientização para o uso Seguro da Internet

Objetivos

Este programa tem como objetivos:

1. Educar os participantes sobre os riscos e as ameaças online;
2. Promover boas práticas de segurança na internet;
3. Ensinar a identificar e evitar armadilhas e golpes online;
4. Incentivar um comportamento ético e responsável na Internet.

Público-Alvo

Este programa tem por foco os servidores do IFSC, mas poderá ser utilizado junto aos estudantes da instituição e seus familiares.

Componentes do Programa

1. Palestras e Workshops
    a. Temas: Segurança digital, privacidade online, cyberbullying, fake news, e engenharia social.
2. Palestrante: Especialistas em segurança cibernética, psicólogos e educadores.
3. Formato: Presencial e online, com sessões interativas e espaço para perguntas e respostas.

Materiais Educativos

1. Guias e Manuais: Produção de material impresso e digital com dicas de segurança, práticas recomendadas e procedimentos de emergência.
2. Vídeos Educativos: Utilização de vídeos curtos e informativos sobre diferentes aspectos da segurança na internet.

Atividades Práticas

1. Oficinas de Segurança Digital: Sessões práticas onde os participantes aprendem a configurar privacidade em redes sociais, reconhecer e-mails fraudulentos, usar autenticação de dois fatores, etc.

Campanhas de Sensibilização

1. Redes Sociais: Utilizar plataformas institucionais para disseminar mensagens e dicas de segurança.
2. Eventos Especiais: Organizar dias temáticos, como o "Dia da Internet Segura", com atividades especiais e campanhas de conscientização.

Parcerias

1. Empresas de Tecnologia: Trabalhar com empresas de tecnologia para fornecer ferramentas e recursos adicionais.

Medição e Avaliação

1. Feedback dos Participantes: Coletar opiniões e sugestões dos participantes após cada sessão ou atividade.
2. Questionários e Pesquisas: Realizar pesquisas antes e depois do programa para medir o nível de conhecimento e conscientização.
3. Relatórios de Progresso: Criar relatórios periódicos para avaliar o impacto do programa e identificar áreas de melhoria.

Recursos Necessários

1. Equipe de Especialistas: Contratação ou parceria com profissionais de segurança cibernética, educadores e psicólogos.
2. Materiais Didáticos: Produção de guias, vídeos, jogos e outros materiais educativos.
3. Infraestrutura: Espaços para workshops e palestras, equipamentos audiovisuais e acesso à internet.

Implementação

1. Planejamento Inicial:
    a. Definir o escopo do programa.
    b. Identificar parceiros e recursos necessários.
    c. Criar um cronograma de atividades.
2. Desenvolvimento de Conteúdo:
    a. Produzir materiais educativos e desenvolver atividades interativas.
    b. Desenvolver facilitadores.

3. Lançamento do Programa:
    a. Organizar um evento de lançamento para divulgar o programa.
    b. Iniciar as atividades conforme o cronograma.
4. Monitoramento e Avaliação:
    a. Coletar feedback contínuo e ajustar o programa conforme necessário.
    b. Publicar relatórios de progresso e compartilhar resultados com stakeholders.

ANEXO

Escopo

Este programa tem por objetivo prover ações de conscientização em segurança da informação que alcancem servidores e estudantes do IFSC.

Cronograma

1. Webinar: LGPD no IFSC: Caminhos para a Conformidade e Proteção de Dados - à definir;
2. Outubro: Mês de Sensibilização para a Segurança Cibernética ;
3. Webinar: Programa de Privacidade e Segurança da Informação no IFSC - 26/11 - 10:00;
4. Dia Internacional da Segurança da Informação - 30/11;
5. Dia da Internet mais segura - 11 de fevereiro de 2025;
6. Oficina de Segurança Digital - 17 a 21 de março de 2025 - CTICs abertas onde os participantes aprenderão a configurar privacidade em redes sociais, reconhecer e-mails fraudulentos, usar autenticação de dois fatores;
7. Palestra técnica: Proteção de Acesso (Unified SASE) - Público alvo: Analistas e técnicos de TIC - 15 de abril de 2025;
8. Palestra didática: Ferramentas para Autenticação Segura - 28 de abril de 2025;
9. Palestra técnica: Gerenciamento de Identidade e Acesso (IAM) - Público alvo: Analistas e técnicos de TIC - 12 de maio de 2025;
10. Palestra didática: A importância de Sistemas Operacionais Atualizados - 02 de junho de 2025;
11. Palestra técnica: Gestão de Vulnerabilidades - Público alvo: Analistas e técnicos de TIC - 12 de agosto de 2025;
12. Palestra didática: Uso Seguro das Redes Sociais - 09 de setembro de 2025;
13. Palestra técnica: Operações de Segurança (SIEM, SOAR, EDR, XDR, NDR) - Público alvo: Analistas e técnicos de TIC - 14 de outubro de 2025;
14. Palestra didática: Golpes na Internet - 11 de novembro de 2025.