Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins

PROGRAMA DE CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

HISTÓRICO DE REVISÕES

Data	Item	Descrição
28/11/2023	1	Elaboração do programa de conscientização, educação e treinamento em segurança da informação.

1. INTRODUÇÃO

O programa de conscientização, educação e treinamento em segurança da informação é uma iniciativa do IFTO para educar e informar seus usuários ou outras partes interessadas sobre a importância da proteção de dados e segurança da informação. Trata-se de um conjunto de práticas, estratégias de ensino e ações educativas que contribuem para a mudança de comportamento de usuários em relação a segurança da informação.

Para que este programa alcance o resultado esperado é definido um plano de ação contendo atividades para apresentação de estratégias de conscientização, educação e treinamento de usuários a partir da divulgação de políticas, normas, regras e procedimentos sobre segurança da informação, dicas sobre como proteger de ameaças cibernéticas, exercícios de simulação, promoção de boas práticas de uso seguro de internet e mídias sociais, como também não cair em golpes de *phishing* e engenharia social.

1.1. Escopo

O escopo deste programa abrange a conscientização, educação e treinamento de usuários da rede IFTO em relação às políticas, diretrizes, normas, regras e procedimentos que devem ser seguidos para proteger os ativos de informação do IFTO, dados pessoais de usuários, prevenir ameaças internas e externas, aumentar a segurança de dispositivos móveis, dentro outros aspectos envolvendo privacidade e segurança da informação.

1.2. Objetivos

O objetivo deste programa é aumentar a conscientização,

educação e treinamento de usuários da rede IFTO em relação à possíveis ameaças e riscos relacionados à segurança da informação no âmbito institucional. Para que este objetivo seja alcançado são definidas os seguintes objetivos específicos:

a) reduzir riscos de incidentes de segurança da informação por meio de adoção de práticas seguras para uso de internet, software, rede cabeada e sem fio, aplicativos e mídias sociais;

b) garantir que o IFTO esteja em conformidade com as regulamentações de segurança da informação por meio do estabelecimento de políticas e normas internas complementares sobre a temática;

c) proteger os ativos digitais e informações críticas do IFTO através do uso de *softwares* de proteção de dados;

d) evitar a divulgação não autorizada de informações confidenciais ou sensíveis através de implantação de mecanismos rígidos de controle de acesso;

e) reduzir a eficácia de ataques de *phishing* e engenharia social através da atualização de sistemas de detecção e proteção de intrusão;

f) mudar o comportamento dos usuários em relação à segurança da informação a partir de ações de conscientização de usuários;

g) estabelecer um cultura de segurança da informação no IFTO a longo prazo por meio de divulgação de práticas de uso seguro dos recursos operacionais e de comunicações disponibilizados pela instituição;

h) aumentar a conscientização sobre como relatar e responder a incidentes de segurança para que os mesmos possam ser tratados de maneira eficaz e minimizar danos ao IFTO;

i) economizar recursos (humanos, tecnológicos e financeiros) e tempo que seriam gastos na recuperação de violações de segurança através da implementação de sistemas de proteção de dados; e

j) conscientização de usuários em relação a segurança da informação por meio de estratégias educativas.

1.3. **Abrangência**

O programa abrange usuários da rede IFTO: servidores, estudantes, prestadores de serviços, voluntários, estagiários, parceiros de negócios, fornecedores e outras partes interessadas que usam os recursos de TI disponibilizados pela instituição.

1.4. **Benefícios esperados**

A partir da execução do programa espera-se ter os seguintes benefícios:

a) redução de riscos e vulnerabilidades a partir da educação de usuários sobre violações de segurança, ataques cibernéticos e vazamentos de dados;

b) ter conformidade com os padrões de segurança da informação recomendados na legislação vigente;

c) proteger a imagem institucional ao demonstrar compromisso com a segurança de dados dos servidores, estudantes, voluntários, estagiários, prestadores de serviços e partes interessadas;

d) reduzir erros humanos, tais como: abertura de e-mails de phishing ou divulgação de senhas;

e) economizar dinheiro em termos de custos de recuperação, multas e ações legais;

f) implantar a cultura de segurança da informação em que todos os usuários compreendam a importância da proteção de informação e fazer da segurança da informação uma prioridade; e

g) proteger informações sensíveis e ativos de informação por meio de melhores práticas de segurança da informação.

2. **CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO**

Segundo a norma ABNT 27002 (ABNT, 2022b) convém que todos os colaboradores da organização recebam treinamento, educação e conscientização apropriados em relação a atualizações regulares das políticas, normas, regras e procedimentos organizacionais relevantes para as suas funções. Neste contexto, a conscientização sobre segurança da informação, segundo NIST 800-16, 1998 tem a intenção de alertar os indivíduos para reconhecer situações de segurança de TI e agir corretamente de forma a proteger dados e informações.

Neste contexto, a conscientização, educação e treinamento em segurança da informação referem-se à importância de garantir que as pessoas que lidam com informações confidenciais estejam cientes dos riscos de segurança cibernética e saibam como se proteger contra ameaças virtuais. Este tipo de abordagem é essencial para garantir a integridade e a privacidade dos dados, bem como também proteger a reputação e o sucesso da instituição.

Conscientização, educação e treinamento em segurança da informação ajudam a instituição a aumentar a conscientização sobre as melhores práticas de segurança da informação, além de fornecer orientação sobre como identificar e evitar possíveis ameaças à segurança das informações no contexto do IFTO. Neste sentido, este programa pretende promover uma mudança cultural entre os usuários que poderá estender-se até mesmo para fora do ambiente corporativo, perpetuando-se na rotina pessoal e familiar dos usuários.

3. **METODOLOGIA**

O programa de conscientização, educação e treinamento em segurança da informação estabelecido pelo IFTO utiliza uma metodologia forma por 6 (seis) fases conforme apresenta a figura 1. Esta abordagem é iterativa e incremental de forma a permitir a melhoria contínua da segurança da Informação no âmbito institucional.

Figura 1 - Metodologia do programa

As 6 (seis) fases da metodologia do programa de conscientização, educação e treinamento em segurança da informação apresentadas na figura 1 são: planejamento, desenvolvimento, avaliação, melhoria contínua, documentação e comunicação.

3.1. Planejamento

Esta fase realiza a avaliação do contexto interno e externo o qual a instituição está inserida para planejar as ações que serão executadas no programa. Nesta fase podem ser realizadas as seguintes atividades:

a) identificação das áreas críticas e sensíveis que requerem atenção especial, podendo incluir dados confidenciais, regulamentações especificadas, e ameaças comuns;

b) avaliação de ameaças e vulnerabilidades relacionadas a segurança da informação;

c) avaliação do nível de conhecimento e conscientização sobre segurança da informação entre os usuários;

d) identificação dos ativos de informação críticos para o IFTO;

e) definição dos objetivos do programa;

f) definição do público alvo do programa;

g) definição dos conteúdos a serem abordados nas estratégias do programa;

h) definição da meta a ser alcançada com o programa, como por exemplo

a redução de incidentes de phishing, aumento da conscientização sobre práticas seguras, entre outros;

i) definição da equipe responsável pela execução do programa; e

j) criação de cronograma de implementação das fases que compõem o programa.

3.2. Desenvolvimento

Esta fase é responsável por desenvolver e implementar o programa. Ela envolve as seguintes atividades:

a) desenvolvimento de materiais educativos, incluindo apresentações, vídeos, documentos informativos e simulados de phishing;

b) realização de cursos de capacitação de usuários de forma personalizada em todos os níveis da organização, podendo ser presenciais, virtuais, simulações de ataques ou uma combinação de ambos;

c) criação de campanhas de conscientização contínuas para manter a segurança da informação como por exemplo: e-mails informativos, posters, concursos e eventos especiais;

d) realização de testes de *phishing* simulados e outras simulações de ataques para avaliar a prontidão dos servidores em identificar ameaças e tomar ações corretivas;

e) uso de canais de comunicação eficaz para transmitir informações sobre segurança da informação de maneira clara e acessível;

f) reconhecimento e recompensa para servidores, estudantes e prestadores de serviço que demonstram um bom entendimento e práticas de segurança da informação;

g) realização de sessões educativas interativas para garantir a compreensão e retenção das informações; e

h) realização de exercícios simulados de ataques de phishing para avaliar a capacidade dos usuários em identificar e relatar tentativas de engenharia social.

3.3. Avaliação

Esta fase é responsável por avaliar a eficácia do programa. Ela envolve as seguintes atividades:

a) implementação de métricas para avaliar a eficácia do programa;

b) aplicação de avaliações para medir a compreensão dos usuários em relação às práticas de segurança aprendidas;

c) coleta de feedback dos usuários para ajustar e melhorar o programa ao longo do tempo. Isso pode incluir a atualização de conteúdo, abordagem de treinamento e simulações;

d) análise de feedback de usuários para identificar áreas de melhoria; e

e) medição do progresso do programa por meio de métricas como taxa de participação em treinamentos, incidentes de segurança relatados e mudanças de comportamento dos servidores, estudantes e prestadores de serviço;

3.4. Melhoria Contínua

Esta fase é responsável por melhorar as ações do programa continuamente. Ela envolve as seguintes atividades:

a) atualização constante do programa visando abordar novas ameaças e tecnologias;

b) ajustes no programa conforme necessário com base nos resultados e feedback recebido; e

c) adaptação do programa de acordo com as necessidades e cultura organizacional;

3.5. Documentação

Esta fase é responsável por documentar as ações do programa. Ela envolve as seguintes atividades:

a) revisão e atualização as ações de conscientização, educação e treinamento em segurança da informação; e

b) atualização do programa com as regulamentações de segurança da informação;

3.6. Comunicação

Esta fase é responsável por comunicar as ações do programa. Ela envolve as seguintes atividades:

a) incentivar a participação ativa dos funcionários para promover uma cultura de segurança da informação;

b) manutenção de uma comunicação constante sobre temas de segurança, destacando ameaças recentes, melhores práticas e atualizações de políticas; e

c) promoção da cultura de segurança da informação, onde todos os servidores, estudantes e prestadores de serviço entendam a importância da segurança cibernética e se sintam responsáveis por proteger os dados do IFTO;

4. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades para o desenvolvimento deste programa são definidos de acordo com a Instrução Normativa PR/GSI Nº 01/2020 (Brasil, 2020). Para este programa serão observadas as competências e responsabilidades apresentadas no regimento interno do IFTO.

5. **PLANO DE TRABALHO**

O plano de trabalho para conscientização, educação e treinamento em segurança da informação estabelecido neste programa utiliza a ferramenta de gestão 5W2H para definir as tarefas a serem realizadas. A tabela 1 apresenta as atividades a serem executadas nos próximos meses.

Tabela 1 - Plano de ação para programa de conscientização, educação e treinamento em segurança da informação

Questão a ser respondida	Atividade	Responsável	Previsão de Início
O que? Conscientização e treinamento de usuários sobre segurança da informação.	Apresentar o programa contendo ações de conscientização sobre segurança da informação.	GSI/ETIR	Dez/2023
Por que? Proteção das informações do IFTO	Atualizar a Política de Segurança da Informação sobre ações de conscientização em segurança da informação.	GSI/ETIR	Dez/2023
Onde? Locais em que o programa será executado	Definir área no Portal Institucional para divulgação das ações referente ao programa.	GSI/ETIR	Dez/2023
Quem? Público-Alvo (Usuários)	Definir o público alvo do programa.	GSI/ETIR	Dez/2023
Quando? 2023-2024	Definir a vigência do programa.	GSI/CSI/DTI	2023/2024
Como? Reuniões, apresentações, palestras, workshops, vídeos, cartilhas,textos, imagens	Elaborar estratégias para campanhas de conscientização de segurança da informação.	GSI/ETIR	Dez/2023
	Definições de ações educativas (exercícios simulados).	Áreas de TI	2024
	Definir métricas de desempenho do programa.	GSI/ETIR	2023/2024

	Publicar alertas e recomendações de segurança cibernética.	GSI/ETIR	2024
	Realizar avaliação contínua das ações previstas no programa.	GSI/ETIR	2024
	Redefinir a estratégia de conscientização conforme resultado da avaliação do programa.	GSI/ETIR	2024
Custo? -	Definir os recursos para o programa.	Alta Administração/ DTI	2024

5.1. Ações de conscientização, educação e treinamento em segurança da informação

A tabela 2 apresenta os temas e conteúdos a serem abordados nas ações de conscientização, educação e treinamento sobre segurança da informação.

Tabela 2 - Temas e conteúdos a serem abordados no programa

Tema	Responsável
Programa de conscientização, educação e treinamento em segurança da informação.	Comitê de Segurança da Informação/ETIR
Política de Segurança da Informação e suas normas internas complementares.	Comitê de Segurança da Informação/ETIR
Práticas sobre uso seguro de ativos institucionais. - Segurança das estações de trabalho; - Segurança em dispositivos móveis; - Vírus e códigos maliciosos; - Cópias de segurança (Backups); - Atualização de sistemas; - Mecanismos de proteção de sistemas (antivírus, antimalware e firewall); - Melhores práticas de autenticação; - identificar e comunicar se os seus ativos institucionais estão desatualizados em relação a segurança; - Verificar e relatar patches de softwares desatualizados ou quaisquer falhas em ferramentas automatizadas; - Notificar a área de TI sobre quaisquer falhas em processos e ferramentas automatizadas que estejam ocorrendo; - Perigos de se conectar e transmitir dados institucionais em redes inseguras.	GSI/ETIR

Práticas sobre uso seguro da Internet e mídias sociais - Uso de senhas seguras; - Golpes na Internet e fraudes eletrônicas (phishing); - Privacidade de informações e redes sociais; - Verificação de segurança em sites da Internet; - Recebimentos de e-mails suspeitos; - Uso de perfis falsos; - Interações com pessoas desconhecidas; - Cuidados no compartilhamento de dados; - Golpes em aplicativos de Internet; - Cuidado no uso de aplicativos; - Navegação segura; - Ataques de engenharia social; - Ataques cibernéticos; - Envio e recebimento de spams; - Fakenews. - Vazamento de dados.	GSI/ETIR
Práticas de privacidade e proteção de dados. - Proteção de dados pessoais; - Criptografia; - Navegação anônima; - VPN; - Compartilhamento de dados.	GSI/ETIR
Práticas de tratamento de dados. - Identificar e armazenar; - Arquivar e destruir informações sensíveis adequadamente; - Mesa e telas limpas; - Apagar quadros físicos e virtuais após reuniões; - Armazenar dados e ativos com segurança; Apresentar sobre as causas de exposição não intencional de dados. - Perda de dispositivos móveis; - Enviar e-mail para pessoa errada devido ao preenchimento automático de e-mail.	GSI/ETIR
Procedimentos para reconhecer e relatar incidentes de segurança. - Identificar os indicadores mais comuns de um incidente; - Relatar incidentes de segurança da informação.	GSI/ETIR
Competências e conscientização de segurança para as funções específicas. - Conscientização e prevenção de vulnerabilidades para desenvolvedores de aplicações; - Conscientização de engenharia social para funções de níveis estratégicos da organização.	GSI/ETIR

6. **ESTRATÉGIAS**

A conscientização, educação e treinamento em segurança da informação é fundamental para proteger informações sensíveis e reduzir o risco de violações de dados. Neste programa poderão ser utilizadas as

seguintes estratégias de ensino:

a) divulgação de cartilhas/folders/fascículos: divulgação de cartilhas de segurança da informação elaboradas pelo Cert.br;

b) campanhas de conscientização: atividade de ensino que tem como objetivo orientar sobre o que é segurança da informação, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema. As ações de conscientização deverão ser prestadas de forma contínua e os resultados deverão ser analisados criticamente para que este programa possa estar sempre alinhado com os objetivos do IFTO;

c) realização de treinamentos: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, como por exemplo gamificação;

d) atividades de comunicação: abrangerão ações voltadas para o acesso à informação de maneira imediata pelos usuários através de um ou mais canais de comunicação oficiais do IFTO, a saber: correio eletrônico, rede social, portal institucional, entre outros;

e) palestras de conscientização, educação e treinamento: eventos sobre privacidade e segurança da informação em que os usuários possam participar e aprender ou conhecer mais sobre os temas abordados sobre segurança da informação;

g) envio por e-mail: mensagens e informativos de incidentes alertando os usuários;

h) simulações de phishing: simulações de ataques de phishing para ensinar os usuários a reconhecer e relatar e-mails e mensagens suspeitas. Essas simulações podem ajudar a identificar áreas de fraqueza na conscientização;

i) programas de recompensas: incentivar os usuários a relatar atividades suspeitas ou vulnerabilidades de segurança oferecendo recompensas, como brindes, certificados ou até mesmo incentivos financeiros;

j) recursos de auto aprendizado: vídeos, infográficos e documentos escritos, que os usuários possam acessar a qualquer momento para obter informações sobre privacidade e segurança; e

k) testes de conscientização: testes regulares para medir o nível de compreensão e identificar áreas de fraqueza.

7. MATRIZ RACI

A matriz RACI apresentada na tabela 3 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: *responsible, accountable, consulted e informed.*

a) ***responsible (responsável):*** pessoa, função ou unidade organizacional

responsável pela execução de uma atividade no âmbito de um processo;

b) ***accountable (responsabilizado):*** dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; Cada atividade só pode possuir um *Accountable*;

c) ***consulted (consultado):*** pessoas que deverão ser consultadas durante a execução da atividade; As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade;

d) ***informed (informado):*** pessoas que serão informadas acerca do progresso da execução da atividade.

Tabela 3 - Matriz de responsabilidades

Atividade	AA	CSI	GSI	ETIR	STI	U
Disponibilizar os recursos necessários para a realização das ações de conscientização, educação e treinamento em segurança da informação.	A/R	C	C	C	C	I
Avaliar e aprovar o programa de conscientização, educação e treinamento em segurança da informação.	A	R	C	C	C	I
Definir o público alvo para o programa de conscientização, educação e treinamento em segurança da informação.	A	C	C	R	C	I
Definir as estratégias para as campanhas de divulgação das iniciativas de segurança da informação: objetivos e metas.	A	C	C	R	C	I
Definir o formato de conscientização, educação e treinamento bem como os canais de comunicação para o programa.	A	C	C	R	C	I
Apresentar ações de segurança da informação que devem ser realizadas pelos usuários de forma a evitar incidentes de segurança da informação no âmbito do IFTO.	A	C	C	R	C	I
Propor melhorias para o programa de conscientização, educação e treinamento em segurança da informação.	A	C	C	R	C	I
Elaborar e manter o programa de conscientização, educação e treinamento em segurança da informação.	A	C	R	C	C	I
Monitorar as ações de conscientização, educação e treinamento em segurança da informação.	A	C	R	C	C	C
Propor treinamentos de usuários em segurança da informação.	A	C	C	R	C	I
Realizar treinamentos sobre segurança da informação.	A	C	C	R	C	I

Conscientizar os usuários em relação às políticas e normas internas complementares sobre segurança da informação do IFTO.	A	C	R	C	C	I
Definir conteúdos a serem abordados no programa de conscientização, educação e treinamento em segurança da informação.	A	C	C	R	C	I
Incentivar os usuários a participarem dos treinamentos sobre segurança da informação.	A	C	R	C	C	I
Participar de treinamentos de segurança da informação disponibilizados pelo IFTO.	A	C	C	C	C	R

Legenda:

AA: Alta Administração

CSI: Comitê de Segurança da Informação.

GSI: Gestor de Segurança da Informação.

ETIR: Equipe de Tratamento e Resposta à Incidentes Cibernéticos.

STI: Setor de Tecnologia da Informação (Diretoria de Tecnologia da Informação e demais setores de Tecnologia da Informação das unidades do IFTO).

U: Usuário.

8. **INDICADOR DE DESEMPENHO**

O programa deverá ser monitorado através de indicador de desempenho. Esse indicador tem o objetivo de medir a eficácia do programa, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 4 apresenta os indicadores de desempenho do programa.

Tabela 4 - Indicadores de desempenho

Meta: Diminuir o número de incidentes de segurança da informação resolvidos durante o ano.	
Indicador	Número de incidentes de segurança da informação resolvidos durante o ano.
Descrição	Número de incidentes de segurança da informação.
Objetivo	Diminuir o número de incidentes de segurança da informação envolvendo o IFTO.
Periodicidade	anual.
Fórmula	Número de ações para conscientização, educação e treinamento em segurança da Informação.
Fonte	Diretoria de Tecnologia da Informação
Meta	Reduzir o número de incidentes de segurança da informação ocorridos durante o ano.

Meta: Aumentar o número de ações de conscientização, educação e treinamento em segurança da informação.	
Indicador	Número de ações de conscientização, educação e treinamento em segurança da informação.
Descrição	Número de ações de conscientização, educação e treinamento em segurança da informação.
Objetivo	Aumentar o número de ações de conscientização, educação e treinamento em segurança da informação.
Periodicidade	anual.
Fórmula	Número de ações para conscientização, educação e treinamento em segurança da Informação.
Fonte	Diretoria de Tecnologia da Informação
Meta	Aumentar o número de ações de conscientização, educação e treinamento em segurança da informação.

9. **REFERÊNCIAS**

ABNT. NBR ISO/IEC 27001:2022. **Segurança da informação, segurança cibernética e proteção à privacidade: sistemas de gestão da segurança da informação. Requisitos.** (ABNT, 2022a). Brasil, 2022.

ABNT. NBR ISO/IEC 27002:2022. **Segurança da informação, segurança cibernética e proteção à privacidade de segurança. Controles de segurança da informação.** (ABNT, 2022b). Brasil, 2022.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Estratégia Nacional de Segurança Cibernética.** Decreto 10.222, de 5 de Fevereiro de 2020. (BRASIL, 2020).

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet.** Disponível em: https://cartilha.cert.br/fasciculos/ Acesso em: 03 mar. 2022.

NIST SPECIAL PUBLICATION 800-16. **Computer Security-Information Technology Security Training Requirements: A Role-and Performance-Based Model, version 1.0**, 1998. (NIST, 1998).

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 06/12/2023, às 17:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Kleyton Matos Moreira**, **Diretor**, em 07/12/2023, às 15:11, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br /sei/controlador_externo.php?acao=documento_conferir& id_orgao_acesso_externo=0, informando o código verificador **2197591** e o código CRC **1B7605DD**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200
portal.ifto.edu.br — reitoria@ifto.edu.br

Referência: Processo nº 23235.018095/2023-64 SEI nº 2197591