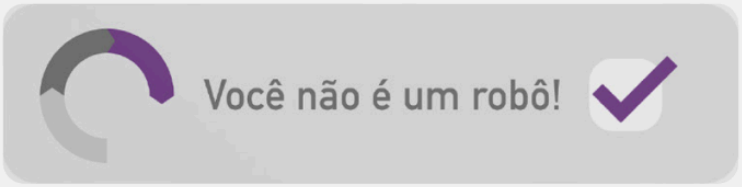
2026

Informe .SeH



PLANO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

ANDIFES CGTIC .SeH SEGURANÇA NO ELEMENTO HUMANO UFRN

Esta é a versão anual do

Plano de Conscientização em Segurança da Informação

Controle de Versões			
Versão	**Descrição**	**Autores**	**Data**
1.0	Versão inicial deste documento	UFRN - Marcos Madruga, Bruno Ferreira, Erica Miranda e Judson Alves.	06/01/2025
2.0	Versão final para uso no ano de 2025	UFRN - Marcos Madruga, Bruno Ferreira, Erica Miranda e Judson Alves.	30/05/2025
2.1	Revisão para 2026	UFRN - Bruno Ferreira e Judson Borges	30/12/2025

Sumário

1. Apresentação

Com o crescente número de ameaças cibernéticas e a importância da proteção de dados nas organizações, é essencial que todos os colaboradores estejam cientes dos riscos e das melhores práticas para manter um ambiente digital seguro. Dessa forma, foi desenvolvido um projeto nomeado de **Projeto Segurança no Elemento Humano (SEH)**.

As atividades do SEH foram realizadas de modo colaborativo por instituições participantes do Colégio de Gestores de Tecnologia da Informação e Comunicação (CGTIC) das Instituições Federais de Ensino Federal Superior (IFES) da Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior (ANDIFES).

Como uma das últimas etapas deste Projeto, este documento constitui o **Plano de Conscientização em Segurança da Informação** para o ano de 2026. Este Plano visa apresentar os conteúdos e atividades produzidos por temática, e orientar a sua aplicação à comunidade institucional, além de oferecer formas de avaliar se os principais objetivos da campanha foram atingidos: i) maior número de pessoas conscientes das questões relacionadas à segurança da informação; e ii) ambiente digital mais seguro.

2. Cronograma

Os temas abordados nessa iniciativa de conscientização em segurança da informação, e o mês em que as atividades serão realizadas, são apresentados na Figura 1.

JAN	FEV	MAR	ABR	MAI	JUN
Autenticação	Segurança Aplicada a Redes Sociais	Segurança em Redes	Vazamento de Dados	Phishing e outros Golpes	Códigos Maliciosos
JUL	**AGO**	**SET**	**OUT**	**NOV**	**DEZ**
Boatos	Comércio via Internet	Segurança em Celulares e Tablets	Segurança no Trabalho Remoto	Cópia de Segurança	Segurança na Era da Inteligência Artificial

Figura 1. Temas a serem abordados.

Vale destacar que os temas propostos são uma recomendação do SEH, mas cada instituição tem liberdade para trabalhar outros temas, caso deseje. O SEH tem

em seu cerne outros temas em fase de construção, que serão disponibilizados na página do Projeto.

3. Organização dos arquivos

Os materiais elaborados estão organizados em arquivos e estes em pastas, que obedeceram a seguinte orientação:

```
[Tema específico]
   [Conteúdos adicionais]
     [Semana<número da semana>]
        [Áudios]
        [E-mail]
        [Redes Sociais]
        [Vídeos]
```

Exemplo:

```
[Autenticação]
   [Conteúdos adicionais]
     [Semana1]
        [Áudios]
        [E-mail]
        [Redes Sociais]
        [Vídeos]
     [Semana2]
        [Áudios]
        [E-mail]
        [Redes Sociais]
        [Vídeos]
     (...)
```

A pasta/diretório `[Conteúdos adicionais]` foi usada para armazenar materiais elaborados para o referido tema (tema específico), como a newsletter e, quando houver, outras mídias, que não foram incluídas na proposta inicial do plano de conscientização.

4. Temas da campanha

As subseções a seguir apresentam os doze temas a serem abordados ao longo do ano, contemplando os materiais recomendados e as ações sugeridas pelas instituições vinculadas ao CGTIC.

Os respectivos arquivos encontram-se disponíveis no endereço eletrônico https://materiais.seh.ufrn.br, organizados em arquivos compactados por tema, com estruturas de pastas padronizadas, conforme definidas neste documento.

4.1 Atividades para o mês de janeiro: Autenticação

Descrição / objetivo: explicar como é realizado o processo de segurança para verificar a veracidade e autenticidade de uma pessoa ou objeto. O objetivo é assegurar que seja autêntica a tentativa de acesso a serviços e sistemas, evitando assim fraudes de quem ou o que não deveria ter acesso ao recurso disponibilizado. Essa autenticação pode ser realizada de diferentes formas como, por exemplo: login e senha, token ou verificação de alguma informação, que comprove a identidade da pessoa ou objeto.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 1.

Quadro 1. Cronograma de atividades para janeiro.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	O processo de autenticação	• Enviar o **texto1** e a **imagem1** para o e-mail dos usuários da comunidade; • Publicar os **banner1**, **banner2** e **texto2** nas redes sociais; • Veicular o **audio1** na rádio (se dispuser); • Anunciar o **video1** na TV (se dispuser).
Semana 2	Boas práticas de autenticação	• Enviar o **texto3** e a **imagem2** para o e-mail dos usuários da comunidade; • Publicar os **banner3**, **banner4**, **texto4** e **vídeo3** nas redes sociais; • Anunciar o **banner3** após o *login* no sistema de informação institucional; • Anunciar o **video2** na TV (se dispuser).
Semana 3	Uso indevido das credenciais	• Enviar o **texto5** e a **imagem3** para o e-mail dos usuários da comunidade; • Publicar os **banner5**, **banner6** e **texto6** nas redes sociais.
Semana 4	Criando senhas robustas	• Enviar o **texto7** e a **imagem4** para o e-mail dos usuários da comunidade; • Publicar os **banner7**, **banner8**, **texto8** e

		vídeo4 nas redes sociais; • Enviar a **newslette**r por e-mail dos usuários da comunidade.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

texto1: [Autenticação] > [Semana1] > [E-mail] > AUT_PROCESSO2_TEXTOEMAIL

imagem1: [Autenticação] > [Semana1] > [E-mail] > AUT_PROCESSO_EMAIL.png

banner1: [Autenticação] > [Semana1] > [Redes Sociais] > AUT_PROCESSO1_STORIE.png

banner2: [Autenticação] > [Semana1] > [Redes Sociais] > AUT_PROCESSO2_STORIE.png

texto2: [Autenticação] > [Semana1] > [Redes Sociais] > AUT_PROCESSO2_LEGENDAREDESSOCIAIS

audio1: [Autenticação] > [Semana1] > [Audios] > AUT_DICAS_USOSEGURODESENHAS_AUDIO.MP3

video1: [Autenticação] > [Semana1] > [vídeos]> AUT_DICAS_USOSEGURODESENHAS.mp4

texto3: [Autenticação] > [Semana2] > [E-mail] > AUT_BOAS_EMAIL.txt

imagem2: [Autenticação] > [Semana2] > [E-mail] > AUT_BOAS_EMAIL.png

banner3: [Autenticação] > [Semana1] > [Redes Sociais] > AUT_BOAS_FEED.png

banner4: [Autenticação] > [Semana1] > [Redes Sociais] > AUT_BOAS_STORIE2.png

texto4: [Autenticação] > [Semana1] > [Redes Sociais] > AUT_BOAS_LEGENDAREDESSOCIAIS.txt

video2: [Autenticação] > [Semana2] > [vídeos]>AUT_2FATORES_VIDEO.mp4

video3: [Autenticação] > [Semana2] > [vídeos] > AUT_VARIADAS_VIDEOVERTICAL.mp4

texto5: [Campanha de conscientização em SI][Temas] > [Autenticação] > [Semana3] > [E-mail] > AUT_USO_TEXTOEMAIL.txt

imagem3: [Campanha de conscientização em SI][Temas] > [Autenticação] > [Semana3] > [E-mail] > AUT_USO_EMAIL.png

banner5: [Autenticação] > [Semana3] > [Redes Sociais] > AUT_USO_FEED.png

banner6: [Autenticação] > [Semana3] > [Redes Sociais] > AUT_USO_STORIE.png

texto6: [Autenticação] > [Semana3] > [Redes Sociais] > AUT_USO_LEGENDAREDESSOCIAIS.txt

texto7: [Autenticação] > [Semana4] > [E-mail] > AUT_SENHAS_EMAIL.txt

imagem4: [Autenticação] > [Semana4] > [E-mail] > AUT_SENHAS_EMAIL.png

banner7: [Campanha de conscientização em SI] > [[Temas] > [Autenticação] > [Semana4] > [Redes Sociais] > AUT_SENHAS_FEED.png

banner8: [Campanha de conscientização em SI] > [[Temas] > [Autenticação] > [Semana4] > [Redes Sociais] > AUT_SENHAS_FEED2.png

texto8: [Campanha de conscientização em SI] > [[Temas] > [Autenticação] > [Semana4] > [Redes Sociais] > AUT_SENHAS_LEGENDAREDESSOCIAIS.txt

video4: [Autenticação] > [Semana4] > [vídeos] > AUT_SEGURAS_VIDEOVERTICAL.mp4

newsletter: [Autenticação] > [Conteúdos adicionais] > AUT_NEWSLETTER copiar.png

4.2. Atividades para o mês de fevereiro: Segurança Aplicada a Redes Sociais

Descrição / objetivo: As redes sociais conectam pessoas e facilitam o compartilhamento de informações, mas também expõem usuários a riscos como roubo de dados, golpes e exposição indevida de informações pessoais. A segurança aplicada a redes sociais busca conscientizar e capacitar os usuários para adotar práticas seguras e minimizar vulnerabilidades ao usar essas plataformas. Dessa forma, são objetivos dessa campanha auxiliar no reconhecimento de ameaças, conscientizar sobre a necessidade de haver um controle de exposição e da responsabilidade digital

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 2.

Quadro 2. Cronograma de atividades para fevereiro.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Privacidade nas redes sociais	● Enviar por e-mail a **imagem1** e o **texto1**; ● Publicar nos stories das redes sociais o **carrossel1**; ● Publicar nas redes sociais o **vídeo1**; ● Publicar no Youtube o **vídeo2**.
Semana 2	Como evitar exposição excessiva de informações	● Veicular na rádio comunitária o **audio1**; ● Enviar por e-mail a **imagem2** e o **texto2**; ● Publicar no feed das redes sociais o **carrossel2**; ● Publicar nas redes sociais o **vídeo3**.
Semana 3	Reconhecimento de golpes e fraudes em redes sociais	● Enviar por e-mail a **imagem3** e o **texto3**; ● Publicar no stories das redes sociais o **carrossel3**; ● Publicar no Youtube o **vídeo4**.
Semana 4	Cuidados com perfis falsos	● Veicular na rádio comunitária o **audio2**; ● Enviar por e-mail a **imagem4** e

		o **texto4**; ● Publicar no feed das redes sociais o **carrossel4**; ● Publicar no Youtube o **vídeo5**.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1: [Segurança Aplicada a Redes Sociais] > [Semana1] > [E-mail] > E-mail 01 Configurações de Privacidade em Redes Sociais.jpg

texto1: [Segurança Aplicada a Redes Sociais] > [Semana1] > [E-mail] > E-mail 01 Configurações de Privacidade em Redes Sociais.docx

carrossel1: [Segurança Aplicada a Redes Sociais] > [Semana1] > [Redes sociais] > [Stories] > 01-01 Configurações de Privacidade em Redes Sociais.png… a 01-10 Configurações de Privacidade em Redes Sociais.png

vídeo1: [Segurança Aplicada a Redes Sociais] > [Semana1] > [Vídeos] > Video 01 Como Proteger sua Privacidade nas Redes Sociais.mp4

vídeo2: [Segurança Aplicada a Redes Sociais] > [Semana1] > [Vídeos] > Video 01_LIBRAS.mp4

audio1: [Segurança Aplicada a Redes Sociais] > [Semana2] > [Áudio] > Segurança nas redes - SPOT 03.wav

imagem2: [Segurança Aplicada a Redes Sociais] > [Semana2] > [E-mail] > E-mail 02 Como Evitar Exposição Excessiva de Informações.jpg

texto2: [Segurança Aplicada a Redes Sociais] > [Semana2] > [E-mail] > E-mail 02 Como Evitar Exposição Excessiva de Informações.docx

carrossel2: [Segurança Aplicada a Redes Sociais] > [Semana2] > [Redes sociais] > [Feed] > 01-01 Como Evitar Exposição Excessiva de Informações.png… a 01-10 Como Evitar Exposição Excessiva de Informações.png

vídeo3: [Segurança Aplicada a Redes Sociais] > [Semana2] > [Vídeos] > SEH Reconheça notícias falsas.mp4

imagem3: [Segurança Aplicada a Redes Sociais] > [Semana3] > [E-mail] > E-mail 03 Reconhecimento de Golpes e Fraudes em Redes Sociais.jpg

texto3: [Segurança Aplicada a Redes Sociais] > [Semana3] > [E-mail] > E-mail 03 Reconhecimento de Golpes e Fraudes em Redes Sociais.docx

carrossel3: [Segurança Aplicada a Redes Sociais] > [Semana3] > [Redes sociais] > [Stories] > 03 Reconhecimento de Golpes e Fraudes em Redes Sociais (1).png… a 03 Reconhecimento de Golpes e Fraudes em Redes Sociais (10).png

vídeo4: [Segurança Aplicada a Redes Sociais] > [Semana3] > [Vídeos] > Video 03 Reconhecimento de Golpes e Fraudes em Redes Sociais.mp4

audio2: [Segurança Aplicada a Redes Sociais] > [Semana4] > [Áudio] > Segurança nas redes - SPOT 05.wav

imagem4: [Segurança Aplicada a Redes Sociais] > [Semana4] > [E-mail] > E-mail 04 Cuidados com Perfis Falsos.jpg

texto4: [Segurança Aplicada a Redes Sociais] > [Semana4] > [E-mail] > E-mail 04 Cuidados com Perfis Falsos.docx

carrossel4: [Segurança Aplicada a Redes Sociais] > [Semana4] > [Redes sociais] > [Feed] > 04 Cuidados com Perfis Falsos (1).png… a 04 Cuidados com Perfis Falsos (10).png

vídeo5: [Segurança Aplicada a Redes Sociais] > [Semana4] > [Vídeos] > Video 05_LIBRAS.mp4

4.3. Atividades para o mês de março: Segurança em Redes

Descrição / objetivo: explicar como é realizado o processo de segurança para proteger as redes de computadores contra acessos não autorizados, interrupções e ataques cibernéticos. Os objetivos são promover boas práticas, incentivar a prevenção para os ataques mais comuns e fomentar uma cultura de segurança.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 3.

Quadro 3. Cronograma de atividades para março.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Cuidados com seu roteador Wi-Fi e demais redes sem fio	● Publicar a **imagem1** nas redes sociais. ● Publicar a **imagem2** nas redes sociais ● Publicar a **imagem3** nas redes sociais ● Publicar a **imagem4** nas redes sociais ● Publicar a **imagem5** nas redes sociais
Semana 2	Cuidados com redes Wi-fi desconhecidas	● Publicar o **audio1** na rádio universitária; ● Publicar os **vídeo1** e **video2** nas redes sociais e/ou TV.
Semana 3	Controle Parental	● Enviar o **email** para o e-mail os usuários da comunidade; ● Publicar o **podcast** no Youtube da Universidade.
Semana 4	Todos os assuntos	● Enviar a **newsletter** para o e-mail dos usuários da comunidade.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1: `[Segurança em Redes] > [Semana1] > [Redes Sociais] > Storie 1080x 1920 (wifi e redes sem fio).png`

imagem2: `[Segurança em Redes] > [Semana1] > [Redes Sociais] > Feed 4 1080x1080 (wifi e redes sem fio).png`

imagem3: `[Segurança em Redes] > [Semana1] > [Redes Sociais] > Feed 3 1080x1080 (Seus roteadores Wi-Fi).png`

imagem4: `[Segurança em Redes] > [Semana1] > [Redes Sociais] > Feed 4 1080x566 (wifi e redes sem fio).png`

imagem5: `[Segurança em Redes] > [Semana1] > [Redes Sociais] > Feed 3 1080x566 (Seus roteadores Wi-Fi).png`

audio1: [Segurança em Redes] > [Semana2] > [Audios] > SPOT Segurança em Redes - UFOB - Versão1.mp3

vídeo1: [Segurança em Redes] > [Semana2] > [Vídeos] > Projeto SEH - Video 1.mp4

vídeo2: [Segurança em Redes] > [Semana2] > [Vídeos] > Projeto SEH - Video 2.mp4

email: [Segurança em Redes] > [Semana3] > [E-mail] > CONTROLE_PARENTAL_EMAIL.txt e …> CONTROLE_PARENTAL_EMAIL.png

podcast: [Segurança em Redes] > [Semana3] > [Videos] > PODCAST - Controle Parental.mp4

newsletter: [Segurança em Redes] > [Conteúdos adicionais] > CONTROLE_PARENTAL_NEWSLETTER.png

4.4. Atividades para o mês de abril: Vazamento de Dados

Descrição / objetivo: visa conscientizar a comunidade acadêmica sobre a importância de proteger informações pessoais e institucionais, adotando práticas seguras no uso de dispositivos e redes digitais. Serão abordados os riscos associados ao vazamento de dados, especialmente no contexto acadêmico e profissional, e os cuidados necessários para prevenir incidentes de segurança. O material procura destacar orientações sobre o uso de senhas fortes e variadas, a adoção da verificação em dois fatores (2FA), a importância de não clicar em links desconhecidos e de compartilhar informações de forma consciente e responsável. O objetivo é promover uma cultura de segurança digital, onde cada pessoa entenda seu papel na proteção dos dados e na prevenção de ameaças cibernéticas.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 4.

Quadro 4. Cronograma de atividades para abril.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	O que é um vazamento de dados e por que se preocupar?	● Publicar nas redes sociais a **imagem1** e o **texto1**; ● Enviar a **imagem2** e o **texto2** para os e-mails.
Semana 2	Proteção de dados pessoais	● Veicular o **audio1** para a rádio institucional; ● Publicar nas redes sociais a **imagem3** e o **texto3**.
Semana 3	Segurança de senhas	● Publicar o **video1** no Youtube; ● Anunciar o **audio2** para a rádio institucional; ● Publicar nas redes sociais a **imagem4** e o **texto4**.
Semana 4	Verificação em dois fatores e cuidados com links	● Publicar o **video2** no Youtube; ● Publicar o **video3** nas redes sociais; ● Enviar por e-mail a **newsletter**.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1 : `[Vazamento de Dados] > [Semana1] > [Redes Sociais] > Semana 1 .png`

texto1 : `[Vazamento de Dados] > [Semana1] > [Redes Sociais] > VAZ_SEM1_LEGENDAREDESSOCIAIS.docx`

imagem2 : `[Vazamento de Dados] > [Semana1] > [E-mail] > Semana 1 .png`

texto2 : `[Vazamento de Dados] > [Semana2] > [E-mail] > VAZ_SEM1_TEXTOEMAIL.docx`

audio1 : `[Vazamento de Dados] > [Semana2] > [Audios] > VAZ_SEM2_AUDIO.mp3`

imagem3 : `[Vazamento de Dados] > [Semana2] > [Redes Sociais] > Semana 2.png`

texto3 : `[Vazamento de Dados] > [Semana2] > [Redes Sociais] > VAZ_SEM2_LEGENDAREDESSOCIAIS.docx`

audio2: [Vazamento de Dados] > [Semana3] > [Audios] > VAZ_SEM3_AUDIO.mp3

imagem4: [Vazamento de Dados] > [Semana3] > [Redes Sociais] > Semana 3.png

texto4: [Vazamento de Dados] > [Semana3] > [Redes Sociais] > VAZ_SEM3_LEGENDAREDESSOCIAIS.docx

video1: [Campanha de conscientização em SI] > [Temas] > Vazamento de Dados] > [Semana3] > [Vídeos] > VAZ_SEM3_VIDEOHORIZONTAL.mp4

video2: [Vazamento de Dados] > [Semana4] > [Vídeos] > VAZ_SEM4_VIDEOHORIZONTAL.mp4

video3: [Vazamento de Dados] > [Semana4] > [Vídeos] > VAZ_SEM4_VIDEOVERTICAL.mp4

newsletter: [Vazamento de Dados] > [Conteúdos adicionais] > VAZ_TEXTO_NEWSLETTER.docx

4.5. Atividades para o mês de maio: Phishing e Outros Golpes

Descrição / objetivo: phishing e outros golpes digitais são estratégias usadas por cibercriminosos para enganar pessoas e obter acesso a informações sensíveis, como senhas, dados bancários e documentos confidenciais. A conscientização sobre essas práticas é essencial para prevenir prejuízos financeiros, vazamento de dados e outros danos. Assim, o objetivo é educar e conscientizar usuários sobre os métodos mais comuns usados por cibercriminosos e ensinar estratégias eficazes para reconhecer, evitar e responder a esses ataques.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 5.

Quadro 5. Cronograma de atividades para maio.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Proteção contra phishing e fraudes	● Publicar nas redes sociais os **stories1** e **stories2**; ● Publicar nas redes sociais o **carrossel1** e o **texto1**;

		● Enviar e-mails com a **imagem1** e o **texto2**; ● Veicular na rádio institucional o **audio01**.
Semana 2	Segurança financeira digital	● Publicar nas redes sociais os **stories3** e **stories4**; ● Publicar nas redes sociais o **carrossel2** e o **texto3**; ● Enviar e-mails com a **imagem2** e o **texto4**.
Semana 3	Segurança em apps	● Publicar nas redes sociais o **stories5**; ● Enviar e-mails com a **imagem3** e o **texto5**; ● Postar o v**ideo1** no Youtube.
Semana 4	Dicas de segurança	● Publicar nas redes sociais os **stories6** e **stories7**; ● Enviar e-mail com o **texto6** e a **newsletter**.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

stories1: `[Phishing e Outros Golpes] > [Semana1] > [Redes Sociais] > Stories 01 - Motivos para não clicar em tudo que receber (Stories).png`

stories2: `[Phishing e Outros Golpes] > [Semana1] > [Redes Sociais] > Stories 02 - Motivos para não clicar em tudo que receber (Stories).png`

carrossel1: `[Phishing e Outros Golpes] > [Semana1] > [Redes Sociais] > [Carrossel-01] > Feed 01… a Feed 05…`

texto1: `[Phishing e Outros Golpes] > [Semana1] > [Redes Sociais] > Rede Social - Semana 1`

imagem1: `[Phishing e Outros Golpes] > [Semana1] > [E-mail] > imagem-02.png`

texto2: `[Phishing e Outros Golpes] > [Semana1] > [E-mail] > Semana 1 - E-Mail`

stories3: `[Phishing e Outros Golpes] > [Semana2] > [Redes Sociais] > Stories01 - Como identificar boletos falsos.png`

stories4: [Phishing e Outros Golpes] > [Semana2] > [Redes Sociais] > Stories02 - Como identificar boletos falsos.png

carrossel2: [Phishing e Outros Golpes] > [Semana2] > [Redes Sociais] > [Carrossel-01] > Feed-01… a Feed-07…

texto3: [Phishing e Outros Golpes] > [Semana2] > [Redes Sociais] > Semana 2 - Redes Sociais

imagem2: [Phishing e Outros Golpes] > [Semana2] > [E-mail] > Imagem-01 - Dicas de uso do PIX.png

texto4: [Phishing e Outros Golpes] > [Semana2] > [E-mail] > Semana 2 - E-Mail

stories5: [Phishing e Outros Golpes] > [Semana3] > [Redes Sociais] > Stories 01 - Permissões de aplicativos (Stories).png

imagem3: [Phishing e Outros Golpes] > [Semana3] > [E-mail] > Imagem-01 - Como com aplicativos falsos.png

texto5: [Phishing e Outros Golpes] > [Semana3] > [E-mail] > E-Mail - Semana 03

vídeo1: [Phishing e Outros Golpes] > [Semana3] > [Vídeos] > video-01.mp4

stories6: [Phishing e Outros Golpes] > [Semana4] > [Redes Sociais] > Stories 01 - Permissões de aplicativos (Stories).png

stories7: [Phishing e Outros Golpes] > [Semana4] > [Redes Sociais] > Stories 02 - Permissões de aplicativos (Stories).png

texto6: [Phishing e Outros Golpes] > [Semana4] > [E-mail] > E-Mail - Semana 03

texto6: [Phishing e Outros Golpes] > [Semana4] > [E-mail] > Semana 04 - E-Mail

newsletter: `[Phishing e Outros Golpes] > [Semana4] > [E-mail] > Newsletter.png`

4.6. Atividades para o mês de junho: Códigos Maliciosos

Descrição / objetivo: códigos maliciosos são ameaças provenientes de programas desenvolvidos para causar danos, roubo de informações ou interrupção de sistemas. Nesse contexto, serão abordadas diferentes formas de malware, incluindo vírus, worms, ransomware, trojans e spyware, além de práticas para reconhecer comportamentos suspeitos e minimizar riscos. Os objetivos dessa campanha são orientar como identificar sinais de infecção e ataques cibernéticos, demonstrar a relevância do papel de cada indivíduo na proteção coletiva contra esse tipo de ataque, e reforçar a importância de políticas de segurança robustas no ambiente corporativo e no uso pessoal.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 6.

Quadro 6. Cronograma de atividades para junho.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Por que não devemos clicar em tudo que recebemos?	● Enviar por e-mail a **imagem1** e o **texto1**; ● Publicar no feed das redes sociais a **imagem2** e **texto2**.
Semana 2	Importância de se manter atualizados programas e aplicativos	● Enviar por e-mail a **imagem3** e o **texto3**; ● Publicar no feed das redes sociais a **imagem4** e o **texto4**.
Semana 3	Perda de dados e importância do backup	● Veicular na rádio comunitária o **audio1**; ● Enviar por e-mail a **imagem5** e o **texto5**; ● Publicar no feed das redes sociais a **imagem6** e o **texto6**.
Semana 4	Importância de se usar senhas seguras	● Veicular na rádio comunitária o **audio2**; ● Publicar nos stories das redes sociais a **imagem7**; ● Enviar por e-mail a **newsletter**.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1: [Códigos Maliciosos] > [Semana1] > [E-mail] > SEMANA1_IMG_EMAIL.png

texto1: [Códigos Maliciosos] > [Semana1] > [E-mail] > SEMANA1_TEXTOEMAIL.docx

imagem2: [Códigos Maliciosos] > [Semana1] > [Redes sociais] > SEMANA1_FEED_IMG1.png e … > SEMANA1_FEED_IMG2.png

texto2: [Códigos Maliciosos] > [Semana1] > [Redes sociais] > SEMANA1_LEGENDA_REDESOCIAL.docx

imagem3: [Códigos Maliciosos] > [Semana2] > [E-mail] > SEMANA2_IMG_EMAIL.png

texto3: [Códigos Maliciosos] > [Semana2] > [E-mail] > SEMANA2_TEXTOEMAIL.docx

imagem4: [Códigos Maliciosos] > [Semana2] > [Redes sociais] > SEMANA2_FEED_IMG1.png e … > SEMANA2_FEED_IMG2.png

texto4: [Códigos Maliciosos] > [Semana2] > [Redes sociais] > SEMANA2_LEGENDA_REDESOCIAL.docx

audio1: [Códigos Maliciosos] > [Semana3] > [Áudio] > backup audio.MP3

imagem5: [Códigos Maliciosos] > [Semana3] > [E-mail] > SEMANA3_IMG_EMAIL.png

texto5: [Códigos Maliciosos] > [Semana3] > [E-mail] > SEMANA3_TEXTOEMAIL.docx

imagem6: [Códigos Maliciosos] > [Semana3] > [Redes sociais] > SEMANA3_FEED_IMG1.png e … > SEMANA3_FEED_IMG2.png

texto6: [Códigos Maliciosos] > [Semana3] > [Redes sociais] > SEMANA3_LEGENDA_REDESOCIAL.docx

audio2: [Códigos Maliciosos] > [Semana4] > [Áudio] > autenticação forte audio.MP3

newsletter: `[Códigos Maliciosos] > [Semana4] > [Conteúdos adicionais] > newsletter.png`

imagem7: `[Códigos Maliciosos] > [Semana4] > [Redes sociais] > SEMANA4_STORY_IMG1.png e … > SEMANA4_STORY_IMG2.png`

4.7. Atividades para o mês de julho: Boatos.

Descrição / objetivo: Este tema aborda os perigos da circulação de boatos e informações não verificadas no ambiente corporativo. A disseminação de conteúdos falsos pode gerar confusão, prejudicar a imagem da instituição e até facilitar golpes. O objetivo é incentivar os colaboradores a sempre checarem a veracidade das informações antes de repassá-las. É fundamental confiar apenas em fontes oficiais e canais internos. Agir com responsabilidade fortalece a cultura de segurança da informação.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 7.

Quadro 7. Cronograma de atividades para julho.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Definição e formas de identificar um boato	● Enviar por e-mail a **imagem1** e o conteúdo do **texto1**; ● Publicar no feed das redes sociais: **imagem2**, **imagem3**, **imagem4**, **imagem5** e **texto2**; ● Publicar no feed das redes sociais: **vídeo1**.
Semana 2	Importância de verificar a veracidade das informação	● Enviar por e-mail a **imagem6** e o conteúdo do **texto3**; ● Publicar no feed das redes sociais: **imagem7**, **imagem8** e **texto4**; ● Publicar no stories das redes: **imagem9**, **imagem10** e **texto4**; ● Veicular na rádio comunitária o **audio1**.
Semana 3	Perigos e consequências de compartilhar boatos	● Enviar por e-mail a **imagem11** e o conteúdo do **texto5**; ● Publicar no feed das redes sociais: **imagem12, imagem13** e **texto6**. ● Publicar no stories das redes:

		imagem14 e **imagem15**.
Semana 4	Como evitar os boatos	• Enviar por e-mail a **imagem16** e o conteúdo do **texto7**; • Publicar no stories das redes sociais: **imagem17, imagem18, imagem19, imagem20, imagem21, imagem22** e **texto8**; • Publicar no reels das redes sociais: **video2**; • Enviar a **newsletter** com o resumo da campanha no mês para o e-mail dos usuários da comunidade.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1: `[Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana1] > [E-mail] > Capa_Email_Semana1.png`

texto1: `[Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana1] > [E-mail] > Capa_Email_Semana1.docx`

imagem2: `[Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana1] > [Redes sociais] > Feed_Boatos_Semana1.png`

imagem3: `[Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana1] > [Redes sociais] > Feed2_Boatos_Semana1.png`

imagem4: `[Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana1] > [Redes sociais] > Feed3_Boatos_Semana1.png`

imagem5: `[Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana1] > [Redes sociais] > Feed4_Boatos_Semana1.png`

texto2: `[Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana1] > [Redes sociais] > Legenda_FEED_Semana1.docx`

video1: `[Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana1] > [Vídeos] > Boatos_VídeoFeed_Semana1.mp4`

texto2: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana1] > Legenda_FEED_Semana1.docx

imagem6: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana2] > [E-mail] > Capa_Email_Semana2.png

texto3: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana2] > [E-mail] > Capa_Email_Semana2.docx

imagem7: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana2] > [Redes sociais] > Feed_Boatos_Semana2.png

imagem8: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana2] > [Redes sociais] > Feed2_Boatos_Semana2.png

texto2: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana2] > [Redes sociais] > Legenda_FEED.docx

imagem9: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana2] > [Redes sociais] > Storie_Semana2.png

imagem10: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana2] > [Redes sociais] > Storie2_Semana2.png

audio1: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana2] > [Audios] > Áudio_Semana2.wav

imagem11: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana3] > [E-mail] > Capa_Email_Semana3.png

texto5: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana3] > [E-mail] > Capa_Email_Semana3.docx

imagem12: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana3] > [Redes sociais] > Feed_Semana3.png

imagem13: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana3] > [Redes sociais] > Feed2_Semana3.png

texto6: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana3] > [Redes sociais] > Legenda_Semana3.docx

imagem14: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana3] > [Redes sociais] > Storie_Semana3.png

imagem15: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana3] > [Redes sociais] > Storie2_Semana3.png

imagem16: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [E-mail] > Capa_Email_Semana4.png

texto7: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [E-mail] > Capa_Email_Semana4.docx

imagem17: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [Redes sociais] > Storie_Semana4.png

imagem18: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [Redes sociais] > Storie1_Semana4.png

imagem19: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [Redes sociais] > Storie2_Semana4.png

imagem20: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [Redes sociais] > Storie3_Semana4.png

imagem21: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [Redes sociais] > Storie4_Semana4.png

imagem22: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [Redes sociais] > Storie5_Semana4.png

texto8: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [Redes sociais] > Legenda_Semana4.docx

video1: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Semana4] > [Vídeos] > CompartilharBoatos_VideoReels_Semana4.mp4

newsletter: [Campanha de conscientização em SI] > [Temas] > [Boatos] > [Conteúdos adicionais] > BOATOS_NEWSLETTER copiar.png

4.8. Atividades para o mês de agosto: Comércio via Internet.

Descrição / objetivo: O comércio eletrônico faz parte da rotina de muitas pessoas, mas também traz riscos como fraudes, sites falsos e roubo de dados. Este tema visa conscientizar sobre os cuidados necessários ao realizar compras online. O objetivo é promover práticas seguras, como verificar a confiabilidade dos sites, evitar ofertas enganosas e proteger os dados de pagamento. Ao adotar essas medidas, o colaborador reduz riscos pessoais e protege os ativos digitais da empresa.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 8.

Quadro 8. Cronograma de atividades para agosto.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Compras online	● Enviar por e-mail a **imagem1** e o conteúdo do **texto1**; ● Publicar no feed das redes sociais: **imagem2**, **imagem3**, **imagem4**, **imagem5** e **texto2**; ● Publicar no reels das redes sociais: **vídeo1**.
Semana 2	Uso de cartão virtual nas compras online	● Enviar por e-mail a **imagem6** e o conteúdo do **texto3**; ● Publicar no story das redes sociais: **imagem7** e **texto4**; ● Veicular na rádio comunitária o **audio1**.
Semana 3	Atenção às ofertas suspeitas	● Enviar por e-mail a **imagem8** e o conteúdo do **texto5**; ● Publicar no feed das redes sociais: **imagem9** e **texto6**; ● Veicular na rádio comunitária o **audio2**; ● Publicar no reels das redes sociais: **vídeo2**.
Semana 4	E-mails suspeitos e vítimas de golpe	● Enviar por e-mail a **imagem10** e o conteúdo do **texto7**; ● Publicar no feed das redes sociais: **imagem11** e **texto8**; ● Publicar no story das redes sociais: **imagem12** e **texto9**; ● Publicar no reels das redes sociais: **vídeo3**. ● Enviar a **newsletter** com o

		resumo da campanha no mês para o e-mail dos usuários da comunidade.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana1] > [E-mail] > 1FRAUDE_COMERCIO__ELETRONICO_EMAIL_SEMANA1.png

texto1: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana1] > [E-mail] > TEXTO_FRAUDE__EMAIL_SEMANA1

imagem2: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana1] > [Redes sociais] > [feed] > COMERCIO_ELETRONICO_01_FEED.png

imagem3: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana1] > [Redes sociais] > [feed] > COMERCIO_ELETRONICO_05_FEED.png

imagem4: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana1] > [Redes sociais] > [feed] > COMERCIO_ELETRONICO_06_FEED.png

imagem5: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana1] > [Redes sociais] > [feed] > COMERCIO_ELETRONICO_07_FEED.png

texto2: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana1] > [Redes sociais] > [feed] > TEXTO CARD 1.txt

video1: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana1] > [Vídeos] > CompraOnline_VideoReels_Semana1.mp4

audio1: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana2] > [Áudios] > ÁUDIO_COMERCIOVIAINTERNET_SEMANA2.mp3

imagem6: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana2] > [E-mail] > 1FRAUDE_COMERCIO__ELETRONICO_EMAIL_SEMANA1.png

texto3: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana2] > [E-mail] > TEXTO CARD 2

imagem7: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana2] > Redes sociais] > [story] > FRAUDE_COMERCIO__ELETRONICO_EMAIL-02.png

texto4: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana2] > [Redes sociais] > Redes sociais] > [story] > TEXTO CARD 2.txt

imagem8: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana3] > [E-mail] > FRAUDE_COMERCIO__ELETRONICO_EMAIL-03.png

texto5: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana3] > [E-mail] > TEXTO CARD 3

imagem9: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana3] > [Redes sociais] > [feed] > COMERCIO_ELETRONICO_03_FEED.png

texto6: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana3] > [Redes sociais] > Redes sociais] > [feed] > TEXTO CARD 3.txt

audio2: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana3] > [Áudios] > ÁUDIO_COMERCIOVIAINTERNET_SEMANA3.mp3

video2: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana3] > [Vídeos] > Golpe_VideoReels_Semana3.mp4

imagem10: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana4] > [E-mail] > FRAUDE_COMERCIO__ELETRONICO_EMAIL-04.png

texto7: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana4] > [E-mail] > TEXTO CARD 4

imagem11: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana4] > [Redes sociais] > [feed] > COMERCIO_ELETRONICO_04_FEED.png

texto8: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana4] > [Redes sociais] > [Redes sociais] > [feed] > TEXTO CARD 4.txt

imagem12: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana4] > [Redes sociais] > [story] > COMERCIO_ELETRONICO_04_STORIE.png

texto9: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana4] > [Redes sociais] > [Redes sociais] > [story] > TEXTO CARD 4.txt

video3: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Semana4] > [Vídeos] > VitimadeGolpe_VideoFeed_Semana4.mp4

newsletter: [Campanha de conscientização em SI] > [Temas] > [Comércio via Internet] > [Conteúdos adicionais] > COMERCIOVIAINTERNET_NEWSLETTER copiar.png

4.9. Atividades para o mês de setembro: Segurança em Celulares e Tablets.

Descrição / objetivo: Celulares e tablets são ferramentas essenciais, mas também alvos comuns de ameaças digitais. Este tema busca reforçar a importância de proteger esses dispositivos com práticas simples, como senhas fortes, atualizações constantes e uso consciente de aplicativos. O objetivo é garantir a integridade das informações acessadas por meio desses equipamentos. Ao seguir essas orientações, o colaborador contribui para um ambiente digital mais seguro e confiável.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 9.

Quadro 9. Cronograma de atividades para setembro.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Cuidado com Aplicativos Falsos	● Enviar por e-mail a **imagem1** e o conteúdo do **texto1**; ● Publicar no feed das redes sociais: **imagem2**, **imagem3** e **texto2**; ● Veicular na rádio comunitária o **audio1**.
Semana 2	Atualização de Sistema Operacional e Aplicativos Localização Remota do Celular	● Enviar por e-mail a **imagem4** e o conteúdo do **texto3**; ● Publicar no feed das redes sociais: **imagem5**, **imagem6** e **texto4**; ● Publicar no reels das redes sociais: **vídeo1**.
Semana 3	Identificação do IMEI Importância do Bloqueio de Tela	● Enviar por e-mail a **imagem7** e o conteúdo do **texto5**; ● Publicar no story das redes sociais: **imagem8**, **imagem9** e **texto6**; ● Veicular na rádio comunitária o **audio2**. ● Publicar no reels das redes sociais: **vídeo2**.
Semana 4	Realização de Backups Regulares Evite Compartilhar Seus Dispositivos	● Enviar por e-mail a **imagem10** e o conteúdo do **texto7**; ● Publicar no feed das redes sociais: **imagem11, imagem 12** e **texto8**; ● Publicar no reels das redes sociais: **vídeo3**. ● Enviar a **newsletter** com o resumo da campanha no mês para o e-mail dos usuários da comunidade.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1: `[Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana1] > [E-mail] > SCT_CUIDADOCOMAPLICATIVOSFALSOS_EMAIL.png`

texto1: `[Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana1] > [E-mail] > SCT_CUIDADOCOMAPLICATIVOSFALSOS_EMAIL.docx`

imagem2: [Campanha de conscientização em SI] > [Segurança em Celulares e Tablets] > [Semana1] > [Redes sociais] > SCT_PERMISSOESDEAPLICATIVOS_FEED_SEMANA1 copiar.png

imagem3: [Campanha de conscientização em SI] > [Segurança em Celulares e Tablets] > [Semana1] > [Redes sociais] > SCT_CUIDADOCOMAPLICATIVOSFALSOS_FEED_1_1080X1080.png

texto2: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana1] > [Redes sociais] > LEGENDA_SCT_CUIDADOCOMAPLICATIVOSFALSOS_FEED_1

audio1: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana1] > [Áudios] > SCT_CUIDADOCOMAPLICATIVOSFALSOS_AUDIO.mp3

imagem4: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana2] > [E-mail] > SCT_ATUALIZACAODOSISTEMAOPERACIONALEAPLICATIVOS_EMAIL.png

texto3: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana2] > [E-mail] > SCT_ATUALIZACAODOSISTEMAOPERACIONALEAPLICATIVOS_EMAIL.docx

imagem5: [Campanha de conscientização em SI] > [Segurança em Celulares e Tablets] > [Semana2] > [Redes sociais] > SCT_ATUALIZACAODESISTEMAOPERACIONALEAPLICATIVOS_FEED_1_1080X1080.png

imagem6: [Campanha de conscientização em SI] > [Segurança em Celulares e Tablets] > [Semana2] > [Redes sociais] > SCT_LOCALIZACAOREMOTADOCELULAR_FEED_2_1080X1080.png

texto4: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana2] > [Redes sociais] > LEGENDA_SCT_CUIDADOCOMAPLICATIVOSFALSOS_FEED_1

video1: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana2] > [Vídeos] > SCT_LOCALIZACAOREMOTADOCELULAR_VIDEO.mp4

imagem7: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana3] > [E-mail] > SCT_IDENTIFICACAODOEMEI_EMAIL.png

texto5: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana3] > [E-mail] > SCT_IDENTIFICACAODOEMEI_EMAIL.docx

imagem8: [Campanha de conscientização em SI] > [Segurança em Celulares e Tablets] > [Semana3] > [Redes sociais] > SCT_BLOQUEIODETELA_STORIES copiar.png

imagem9: [Campanha de conscientização em SI] > [Segurança em Celulares e Tablets] > [Semana3] > [Redes sociais] > SCT_IMPORTANCIABLOQUEIODETELA_FEED_2_1080X1080.png

texto6: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana3] > [Redes sociais] > LEGENDA_SCT_IMPORTANCIADOBLOQUEIODETELA_FEED_2

audio2: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana3] > [Áudios] > SCT_IMPORTANCIADOBLOQUEIODETELA_AUDIO.mp3

video1: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana3] > [Vídeos] > SCT_IDENTIFICACAODOIMEI_VIDEO.mp4

imagem10: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana4] > [E-mail] > SCT_REALIZACAODEBACKUPSREGULARES_EMAIL.png

texto7: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana4] > [E-mail] > SCT_REALIZACAODEBACKUPSREGULARES_EMAIL.docx

imagem11: [Campanha de conscientização em SI] > [Segurança em Celulares e Tablets] > [Semana4] > [Redes sociais] > SCT_EVITECOMPARTILHARSEUSDISPOSITIVOS_FEED copiar.png

imagem12: [Campanha de conscientização em SI] > [Segurança em Celulares e Tablets] > [Semana4] > [Redes sociais] > SCT_EVITECOMPARTILHARSEUSDISPOSITIVOS_FEED_2_1080x1080.png

texto8: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana4] > [Redes sociais] > LEGENDA_SCT_EVITECOMPARTILHARSEUSDISPOSITIVOS_FEED_2

video3: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Semana4] > [Vídeos] > SCT_REALIZACAODEBACKUPSREGULARES_VIDEO.mp4

newsletter: [Campanha de conscientização em SI] > [Temas] > [Segurança em Celulares e Tablets] > [Conteúdos adicionais] > SCT_NEWSLETTER_1080x1920.png

4.10. Atividades para o mês de outubro: Segurança no Trabalho Remoto.

Descrição / objetivo: O trabalho remoto exige cuidados adicionais com a segurança da informação, já que o ambiente fora da empresa pode ser mais vulnerável. Este tema tem como objetivo orientar sobre práticas seguras, como uso de VPN, senhas fortes e proteção física dos dispositivos. A adoção dessas medidas reduz riscos de vazamentos, acessos indevidos e incidentes de segurança. Cada colaborador é responsável por manter a segurança mesmo fora do escritório.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 10.

Quadro 10. Cronograma de atividades para outubro.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Sistemas e aplicativos atualizados	● Enviar por e-mail a **imagem1** e o conteúdo do **texto1**; ● Publicar no story das redes sociais: **imagem2**, **imagem3** e **imagem4**; ● Publicar no reels das redes sociais: **vídeo1**.
Semana 2	Phishing e engenharia social	● Enviar por e-mail a **imagem5** e o conteúdo do **texto2**; ● Publicar no feed das redes sociais: **imagem6** e **texto3**; ● Veicular na rádio comunitária o

		audio2.
Semana 3	Conexão segura e informações corporativas	● Enviar por e-mail a **imagem7** e o conteúdo do **texto4**; ● Publicar no story das redes sociais: **imagem8** e **imagem9**; ● Publicar no reels das redes sociais: **vídeo2**.
Semana 4	Segurança de dispositivos e dados confidenciais	● Enviar por e-mail a **imagem10** e o conteúdo do **texto5**; ● Veicular na rádio comunitária o **audio2**; ● Publicar no reels das redes sociais: **vídeo3;** ● Enviar a **newsletter** com o resumo da campanha no mês para o e-mail dos usuários da comunidade.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1: `[Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana1] > [E-mail] > capa_EMAIL_S1-novo.png`

texto1: `[Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana1] > [E-mail] > texto_email.docx`

imagem2: `[Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana1] > [Redes sociais] > seguranca_storie.png`

imagem3: `[Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana1] > [Redes sociais] > seguranca_storie1.png`

imagem4: `[Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana1] > [Redes sociais] > seguranca_storie2.png`

video1: `[Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana1] > [Vídeo] > video_SEH_s1.mp4`

imagem5: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana2] > [E-mail] > capa_EMAIL_S2.png

texto2: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana2] > [E-mail] > E-mail S2.docx

imagem6: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana2] > [Redes sociais] > protecao_feed.png

texto3: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana2] > [Redes sociais] > Descrição Feed S2.docx

audio1: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana2] > [Áudios] > Spot 2.mp3

imagem7: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana3] > [E-mail] > capa_EMAIL_S3.png

texto4: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana3] > [E-mail] > E-mail S3.docx

imagem8: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana3] > [Redes sociais] > Story 1 - S3.png

imagem9: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana3] > [Redes sociais] > Story 2 - S3.png

video2: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana3] > [Vídeo] > video_infocorporativa_s3.mp4

imagem10: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana4] > [E-mail] > capa_EMAIL_S4.png

texto5: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana4] > [E-mail] > texto_email_S4 .docx

audio1: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana4] > [Áudios] > Spot 4.mp3

video2: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Semana4] > [Vídeo] > protecao_videoreels_s4.mp4

newsletter: [Campanha de conscientização em SI] > [Temas] > [Segurança no Trabalho Remoto] > [Conteúdos adicionais] > seg_NEWSLETTER.png

4.11. Atividades para o mês de novembro: Cópia de Segurança.

Descrição / objetivo: A realização de backups é uma prática essencial para a proteção das informações corporativas e pessoais. Dados podem ser perdidos por falhas técnicas, erros humanos ou ataques cibernéticos. O objetivo deste tema é conscientizar sobre a importância de manter cópias seguras, atualizadas e acessíveis dos dados críticos. Ter um plano de backup confiável garante a continuidade das operações. A prevenção é sempre mais eficaz que a recuperação emergencial.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 11.

Quadro 11. Cronograma de atividades para novembro.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Definição de backup	● Enviar por e-mail a **imagem1** e o conteúdo do **texto1**; ● Publicar no feed das redes sociais: **imagem2**, **imagem3**, **imagem4**, **imagem5** e **imagem6** ● Veicular na rádio comunitária o **audio1**. ● Publicar no reels das redes sociais: **vídeo1**.

Semana 2	Métodos de backup	● Enviar por e-mail a **imagem7** e o conteúdo do **texto2**; ● Publicar no feed das redes sociais: **imagem8** e **texto3**; ● Veicular na rádio comunitária o **audio2**. ● Publicar no reels das redes sociais: **vídeo2**.
Semana 3	Recuperação de dados após incidentes	● Enviar por e-mail a **imagem9** e o conteúdo do **texto4**; ● Publicar no feed das redes sociais: **imagem10** e **texto5**; ● Veicular na rádio comunitária o **audio3**. ● Publicar no reels das redes sociais: **vídeo3**.
Semana 4	Perguntas Frequentes sobre Backups	● Publicar no feed das redes sociais: **imagem11** e **texto6**; ● Veicular na rádio comunitária o **audio4**. ● Publicar no reels das redes sociais: **vídeo4**. ● Enviar a **newsletter** com o resumo da campanha no mês para o e-mail dos usuários da comunidade.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1: `[Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana1] > [E-mail] > email_semana1_backup.png`

texto1: `[Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana1] > [E-mail] > E-mail Semana 01.pdf`

imagem2: `[Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana1] > [Redes sociais] > PROTEGERSEUSDADOS_SEMANA1.jpg`

imagem3: `[Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana1] > [Redes sociais] > PROTEGERSEUSDADOS1_SEMANA1.jpg`

imagem4: `[Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana1] > [Redes sociais] > PROTEGERSEUSDADOS2_SEMANA1.jpg`

imagem5: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana1] > [Redes sociais] > PROTEGERSEUSDADOS3_SEMANA1.jpg

imagem6: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana1] > [Redes sociais] > PROTEGERSEUSDADOS4_SEMANA1.jpg

audio1: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana1] > [Áudios] > SPOT_SEMANA1.mp3

video1: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana1] > [Vídeos] > COPIADESEGURANCA_VIDEO_SEMANA1.mp4

imagem7: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana2] > [E-mail] > email_semana2_backup.png

texto2: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana2] > [E-mail] > TEXTOEMAIL_semana2_backup.pdf

imagem8: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana2] > [Redes sociais] > ESCOLHACOPIA_FEED_SEMANA2.png

texto3: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana2] > [Redes sociais] > Texto Feed Semana 02.docx

audio2: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana2] > [Áudios] > SPOT_SEMANA2.mp3

video2: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana2] > [Vídeos] > BACKUP_VIDEO_SEMANA2.mp4

imagem9: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana3] > [E-mail] > email_semana3_backup.png

texto4: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana3] > [E-mail] > email - semana 3.docx

imagem10: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana3] > [Redes sociais] > DIVERSIFIQUEBACHUP_FEED_SEMANA3.png

texto5: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana3] > [Redes sociais] > Texto Feed Semana 03.docx

audio3: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana3] > [Áudios] > SPOT_SEMANA3.mp3

video3: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana3] > [Vídeos] > COPIADESEGURANCA_VIDEO_SEMANA3.mp4

imagem11: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana4] > [Redes sociais] > backup_feed_semana4.png

texto6: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana4] > [Redes sociais] > Texto Feed Semana 04.docx

audio4: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana4] > [Áudios] > SPOT_SEMANA4.mp3

video4: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Semana4] > [Vídeos] > FREQUENCIABACKUP_VIDEO_SEMANA4.mp4

newsletter: [Campanha de conscientização em SI] > [Temas] > [Cópia de Segurança] > [Conteúdos adicionais] > COPIADESEGURANCA_NEWSLETTER.png

4.12. Atividades para o mês de dezembro: Segurança na Era da Inteligência Artificial.

Descrição / objetivo: O crescimento drástico da Inteligência Artificial transformou a produtividade em diversos setores. Contudo, na segurança digital, o impacto é profundo e ambivalente. De um lado, a IA potencializa a detecção de ameaças e a resposta a incidentes em tempo real; de outro, mune atacantes com ferramentas para gerar golpes complexos, como engenharia social avançada e códigos maliciosos que burlam sistemas tradicionais. Nesse contexto, a educação digital torna-se a primeira linha de defesa: é essencial que os usuários compreendam os novos riscos para utilizar essas inovações de forma segura e resiliente.

Cronograma: As atividades serão realizadas, conforme cronograma detalhado no Quadro 12.

Quadro 12. Cronograma de atividades para dezembro.

Período	Assunto a ser trabalhado	Mídias e Meios de divulgação
Semana 1	Inteligência Artificial no Serviço Público	● Enviar por e-mail a **imagem1** e o conteúdo do **texto1**; ● Publicar no feed das redes sociais: **imagem2** e **imagem3**; ● Publicar nas redes sociais: **vídeo1** e **video2**.
Semana 2	DeepFake	● Enviar por e-mail a **imagem4** e o conteúdo do **texto2**; ● Publicar nas redes sociais: **imagem5**, **imagem6** e **texto3**.
Semana 3	Cuidado! A IA também comete erros.	● Enviar por e-mail a **imagem7** e o conteúdo do **texto4**; ● Publicar Nas redes sociais: **imagem8** a **imagem13**.
Semana 4	Uso ético da IA	● Enviar a **newsletter** com o resumo da campanha no mês para o e-mail dos usuários da comunidade. ● Publicar nas redes sociais: **imagem14** a **imagem19**. ● Publicar nas redes sociais: **video3**.

Caminhos e nomes dos arquivos na pasta/diretório no repositório:

imagem1: `[Semana1] > [E-mail] > IA_EMAIL_SEMANA1.png`
texto1: `[Semana1] > [E-mail] > Texto E-mail - Semana 1.docx`
imagem2: `[Semana1] > [Redes sociais] > IA_FEED_SEMANA1.png`
imagem3: `[Semana1] > [Redes sociais] > IA_STORY_SEMANA1.png`

video1: [Semana1] > [Vídeos] > IA_IAECOOKIES_SEMANA1_REELS.mp4
video2: [Semana1] > [Vídeos] > IA_IAECOOKIES_SEMANA1.mp4

imagem4: [Semana2] > [E-mail] > IA_EMAIL_SEMANA2.png
texto2: [Semana2] > [E-mail] > Texto e-mail Semana2.docx
imagem5: [Semana2] > [Redes Sociais] > IA_FEED_SEMANA2.png
imagem5: [Semana2] > [Redes Sociais] > IA_STORY_SEMANA2.png
texto3: [Semana2] > [Redes Sociais] > IA_LEGENDA_SEMANA2.docx

imagem7: [Semana3] > [E-mail] > IA_EMAIL_SEMANA3.png
texto4: [Semana3] > [E-mail] > Texto E-mail - Semana 3.docx
imagem8: [Semana3] > [Redes Sociais] > IA_FEED1_SEMANA3.png
imagem9: [Semana3] > [Redes Sociais] > IA_FEED2_SEMANA3.png
imagem10: [Semana3] > [Redes Sociais] > IA_FEED3_SEMANA3.png
imagem11: [Semana3] > [Redes Sociais] > IA_STORY1_SEMANA3.png
imagem12: [Semana3] > [Redes Sociais] > IA_STORY2_SEMANA3.png
imagem13: [Semana3] > [Redes Sociais] > IA_STORY3_SEMANA3.png

newsletter: [Semana4] > [E-mail] > IA_NEWSLETTER.png
texto5: [Semana4] > [E-mail] > IA_TEXTONEWSLETTER_SEMANA4.docx
imagem14: [Semana4] > [Redes Sociais] > IA_FEED1_SEMANA4.png
imagem15: [Semana4] > [Redes Sociais] > IA_FEED2_SEMANA4.png
imagem16: [Semana4] > [Redes Sociais] > IA_FEED3_SEMANA4.png
imagem17: [Semana4] > [Redes Sociais] > IA_STORY1_SEMANA4.png
imagem18: [Semana4] > [Redes Sociais] > IA_STORY2_SEMANA4.png
imagem19: [Semana4] > [Redes Sociais] > IA_STORY3_SEMANA4.png
video3: [Semana4] > [Videos] > IA_USOETICO_SEMANA4.mp4

5. Avaliação da execução do Plano de Conscientização

A avaliação da Campanha de Conscientização em Segurança da Informação será realizada por meio da aplicação de um quiz (ver seção 5.1) e do envio de e-mails de phishing de modo controlado (ver seção 5.2). No Apêndice A, encontram-se as questões por tema a serem utilizadas no quiz. Essas atividades serão realizadas da seguinte forma:

- A aplicação do quiz deverá acontecer antes do início e no final da divulgação do material da campanha.

- O envio de e-mails com phishing antes do mês, onde esse tema será abordado.
- O envio de e-mails com phishing algum tempo após o mês onde esse tema será abordado.

Recomenda-se que os resultados da avaliação da aplicação da ferramenta de phishing sejam passados para a coordenação do SEH, para que os dados de todas as instituições sejam agrupados, e se possa obter uma dimensão nacional do resultado da campanha. Ressalta-se que os dados de cada instituição devem ser enviados no formato especificado pelo SEH de acordo com o guia de utilização da ferramenta (GoPhish).

5.1. Sobre o quiz

As questões com as informações para o quiz estão disponíveis no Apêndice A, e o modelo de formulário para o quiz construído no Google Form, no Apêndice B.

5.2. Ferramenta para envio de phishing: GoPhish

O GoPhish[1] é um framework de código aberto que permite a criação de um servidor de rede capaz de lançar campanhas de phishing simuladas, com o objetivo de testar a resiliência a ataques em uma determinada comunidade. Além do envio do phishing simulado, o GoPhish permite a avaliação dos resultados, mostrando-os em gráficos de fácil entendimento, o que torna ideal como forma de validar a efetividade de uma campanha de conscientização contra phishing e spams. O software é open source e de uso gratuito.

Um manual com recomendações mais detalhadas pode ser baixado no site do projeto: https://seh.ufrn.br/assets/files/ProjetoSEH_GoPhish_ManualDeUso.pdf .

6. Licenciamento dos materiais

Os materiais desenvolvidos no Projeto SEH estão disponíveis sob a licença Creative Commons[2] (CC BY-NC-ND). Dessa forma, fica autorizada, previamente, a redistribuição com créditos aos autores, mas é impedindo o uso comercial, remixagem e alterações.

Ressalta-se que materiais de terceiros incluídos no projeto SEH obtiveram licença prévia e foram respeitadas as condições impostas para seu uso e modificações de acordo com o licenciamento original dos autores. Por exemplo, nos

[1] Site: https://getgophish.com/
[2] Site: https://br.creativecommons.net

vídeos do NIC.br foi mantido o propósito de interesse público informado na solicitação protocolada pela coordenação do Projeto, e cumpridos os preceitos da licença de Creative Commons BY-ND 4.01 no novo material.

7. Considerações finais

Embora este plano de conscientização apresente um conjunto de doze temas principais para serem trabalhados ao longo do ano, é importante estar atento a eventos que possam ocorrer e requeiram ações de divulgação específicas, como proposto no guia.

Ainda, as informações, sugestões, reclamações ou manifestação de interesse em participar das atividades de produção ou revisão dos temas podem ser enviadas através do e-mail de contato divulgado na página do projeto.

Apêndice A - questões para o quiz

Neste Apêndice A, são apresentadas as questões, que comporão o quiz a ser aplicado no início e final da campanha de conscientização. A resposta correta é identificada com (*).

Tema: **Autenticação**

1. Qual é o processo adicional de autenticação, que melhora a segurança no acesso a sistemas cibernéticos?

a) Autenticação multifator. (*)
b) Senha robusta.
c) Senha de terceiros.
d) Botnet.

2. O uso indevido de credenciais pode ocasionar:

a) Atualização do sistema ou aplicativo.
b) Melhor reputação da instituição junto ao público das redes sociais.
c) Sérios incidentes de segurança e prejuízos pessoais e à instituição. (*)
d) Benefícios financeiros ou monetários à instituição.

Tema: Segurança Aplicada a Redes Sociais

1. Um dos cuidados recomendados no uso das redes sociais é a proteção do seu perfil. Assinale a opção CORRETA quanto à proteção de perfis de contas.

a) Acesse o site da rede social sempre usando http.
b) Procure usar a mesma senha para acessar diferentes sites.
c) Não use opções como silenciar, bloquear e denunciar, caso identifique abusos.
d) Solicite um arquivo com suas informações ou verifique o registro de atividades, caso desconfie que o seu perfil tenha sido indevidamente usado. (*)

2. Dentre os cuidados recomendados no uso das redes sociais estão o respeito à privacidade alheia e a proteção dos seus filhos. Quanto aos cuidados citados, assinale a opção INCORRETA:

a) Evite divulgar imagens em que outras pessoas apareçam, sem autorização prévia.
b) Evite falar sobre ações, atos e rotina de outras pessoas.
c) Oriente seus filhos a se relacionarem com estranhos e a fornecer informações pessoais. (*)
d) Você estará protegendo seu filho, ao respeitar o limite de idade estipulado pelos sites.

Tema: Segurança em Redes

1. Qual desses é um cuidado ao se conectar a redes Wi-Fi?

a) Não apagar as redes que você visitou.
b) Usar redes que ofereçam apenas criptografia WEP e WPA.
c) Não permitir que seus dispositivos se conectem automaticamente a redes públicas. (*)
d) Não se certificar de usar conexão segura.

2. João teve sua rede doméstica invadida por um atacante. Qual dos seguintes procedimentos configura uma possível falha que permitiu a invasão?

a) Desabilitar o gerenciamento do equipamento de rede via Internet.
b) Usar firewall e antivírus atualizados.
c) Esconder a rede, evitando que seu nome seja anunciado para outros dispositivos.
d) Manter a senha padrão de fábrica do modem/roteador. (*)

Tema: Vazamento de Dados

1. O que normalmente não acontece em casos de dados vazados?

a) Abertura de contas, dívidas e/ou aplicação de golpes.
b) Validação de dados em sistemas de golpes.
c) Melhora no desempenho de sistemas. (*)
d) Chantagear outras pessoas se passando por você.

2. Ao realizar o cadastro em um site de cursos online e gratuitos, quais dados solicitados seriam suspeitos?

a) CPF e dados bancários. (*)
b) Nome e apelido.
c) Número de telefone e e-mail.
d) Usuário e senha.

Tema: Phishing e Outros Golpes

1. O que é phishing?

a) Uma técnica de pesca esportiva.
b) Um tipo de vírus de computador.
c) Uma forma de fraude online que busca obter informações pessoais. (*)
d) Um software de segurança.

2. Qual das alternativas abaixo é um sinal de que um e-mail pode ser uma tentativa de phishing?

a) O e-mail é enviado por um amigo.
b) O e-mail contém erros de ortografia e gramática. (*)
c) O e-mail é de uma loja onde você fez compras recentemente.
d) O e-mail não contém links.

Tema: Códigos Maliciosos

1. Existem vários tipos de códigos maliciosos. Assinale a alternativa INCORRETA quanto à descrição de cada um deles.

a) Vírus: programa ou parte de uma programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo.
b) Ransomware: programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário.
c) Backdoor: programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e com o conhecimento do usuário. (*)
d) Worm: programa capaz de se propagar automaticamente pelas redes, explorando e enviando cópias de si mesmo de equipamento para equipamento.

2. Uma das formas de prevenção contra códigos maliciosos é manter seus equipamentos atualizados. Assinale a alternativa CORRETA a respeito da atualização de equipamentos.

a) Evite usar programas originais.
b) Desinstale todas as atualizações disponíveis, principalmente as de segurança.
c) Crie um disco de recuperação e tenha-o por perto no caso de emergências. (*)

d) Descarte o disco de emergência de seu antivírus, caso perceba que o comportamento do equipamento está estranho.

Tema: Boatos

1. O que é um boato?

a) Uma notícia de fonte desconhecida, atualmente conhecida como fake news. (*)
b) Uma classificação de vírus, trojan e spyware.
c) Um tipo de programa para varredura do sistema.
d) Uma notícia de fonte confiável.

2. Os boatos difundidos nas redes sociais têm características próprias. Assinale a **sequência correta** das alternativas que podem caracterizar um boato (*Fake News)*.

( ) Não possui fonte ou cita fontes desconhecidas.
( ) Não apresenta evidências e nem embasamento dos fatos noticiados.
( ) Sugere consequências trágicas, se determinada tarefa não for realizada.
( ) Possui título bombástico, resumido e com destaques em maiúsculos.

a) F-V-V-F
b) V-V-V-V (*)
c) F-F-V-V
d) V-V-V-F

Tema: Comércio via Internet

1. Ao realizar compras online, assinale a opção que corresponde aos cuidados recomendados para melhor segurança dos seus dados pessoais.

a) Ao fornecer dados sensíveis via e-mail, é desnecessário criptografar a mensagem enviada.
b) É desnecessário guardar informações da compra, como comprovantes e número do pedido.
c) Certifique-se de usar conexões seguras, observando se há o desenho de cadeado fechado mostrado na barra de endereço. (*)
d) Verificar se o endereço do site começa com http://

2. Antes de iniciar a compra online, assinale a opção que **NÃO** representa um cuidado recomendado:

a) Acessar o site/loja , digitando o endereço diretamente no navegador web.

b) Evitar clicar em links recebidos em mensagens.
c) Utilizar sempre um computador com mecanismos de segurança instalados, como antimalware, antispam e firewall pessoal.
d) É desnecessário verificar se o site/loja é confiável. (*)

Tema: Segurança em Celulares e Tablets

1. Qual dos seguintes itens **não** apresenta um risco de uso dos dispositivos móveis?

a) Vazamento de informações.
b) Instalação de aplicativos legítimos. (*)
c) Invasão de privacidade.
d) Propagação de códigos maliciosos.

2. Assinale a ação **que não deve ser feita,** em caso de perda ou furto de um dispositivo.

a) Informar à operadora e solicitar bloqueio do número.
b) Informar à empresa onde trabalha.
c) Bloquear cartões de crédito cujos números estejam nele armazenados.
d) Manter as senhas que possam estar nele armazenadas. (*)

Tema: Segurança no Trabalho Remoto

1. Como você pode proteger seus dados enquanto utiliza dispositivos pessoais (como notebooks e celulares) para trabalhar remotamente?

a) Armazenar dados sensíveis apenas em pastas locais, sem backup na nuvem.
b) Utilizar redes de Wi-Fi públicas sem nenhum cuidado adicional.
c) Configurar senhas fortes e usar criptografia de dados quando possível. (*)
d) Compartilhar os dispositivos com familiares para economizar tempo.

2. Qual é a principal razão para usar uma rede privada virtual (VPN) ao trabalhar remotamente?

a) Melhorar a qualidade da conexão de internet.
b) Garantir que os dados sejam transmitidos de forma segura, protegendo sua privacidade. (*)
c) Aumentar a velocidade de navegação na internet.
d) Facilitar o acesso a sites bloqueados pela instituição.

Tema: Cópia de Segurança

1. Qual é a principal razão para realizar cópias de segurança (backup) regularmente?

a) Para liberar espaço no dispositivo.
b) Para garantir a recuperação de dados em caso de falhas no dispositivo ou ataque cibernético. (*)
c) Para aumentar a velocidade do sistema.
d) Para melhorar a qualidade das imagens armazenadas.

2.O que deve ser evitado ao realizar backups de dados sensíveis ou confidenciais?

a) Armazenar backups em dispositivos externos criptografados.
b) Armazenar backups em locais acessíveis ao público, como redes não protegidas ou serviços de nuvem gratuitos sem criptografia. (*)
c) Usar uma senha forte para proteger os arquivos de backup.
d) Manter cópias de segurança em diferentes locais, como discos rígidos externos e nuvem.

Tema: Segurança na Era da Inteligência Artificial

1. Ao utilizar ferramentas de Inteligência Artificial generativa (como chatbots de texto), qual é a recomendação mais segura em relação aos seus dados pessoais ou profissionais?

a) Evitar inserir informações sensíveis, como senhas, dados bancários ou segredos industriais, pois esses dados podem ser usados para treinar os modelos.
b) Inserir apenas dados criptografados manualmente no chat para que a IA possa decifrá-los com segurança.
c) Compartilhar livremente qualquer dado, pois as empresas de IA garantem por lei que ninguém terá acesso ao que você escreve.
d) Usar a IA apenas de madrugada, pois o tráfego de dados é menor e os hackers estão menos ativos nesse horário.

2. O termo 'Deepfake' é frequentemente associado a riscos de segurança na IA. O que melhor define esse conceito para um usuário comum?

a) Um tipo de vírus que apaga todos os arquivos de fotos do seu celular ou computador.

b) Vídeos, áudios ou imagens criados por IA que imitam de forma realista a aparência ou a voz de pessoas reais, podendo ser usados para fraudes.
c) Um sistema de segurança avançado que impede que estranhos acessem sua câmera de vídeo.
d) Uma ferramenta de IA que serve exclusivamente para melhorar a qualidade de fotos antigas de família.

Apêndice B - modelo de formulário para o quiz construído no Google Form

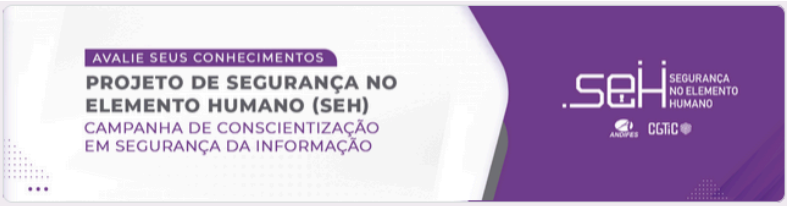
O modelo de formulário aqui apresentado foi construído no Google Form com a intenção de facilitar a criação, configuração e correção automática das questões apresentadas no Apêndice A.

A solicitação do e-mail é opcional, mas, caso não seja feita, não existe uma forma de garantir que cada usuário (e-mail) responda uma única vez o quiz através dessa ferramenta (Google Form).

Recomenda-se que as questões sejam apresentadas de forma aleatória, assim como as alternativas de cada questão.

Para definir um ranking e gamificar a participação sugere-se pedir um apelido, com fim de divulgação, e pontuar cada questão. Essa ferramenta possibilita correção automática e a geração de alguns gráficos a partir da participação dos usuários. A imagem do cabeçalho encontra-se disponível na pasta “Recursos”.

A seguir, imagens das questões embaralhadas do modelo construído:



Projeto SEH - Quiz

Este quiz tem como objetivo oferecer uma visão sobre os seus conhecimentos a respeito de alguns temas relacionados à segurança da informação. Responda e, ao final, você saberá como anda sua percepção acerca das perguntas elaboradas.

* Indica uma pergunta obrigatória

E-mail *

Seu e-mail

Informe como gostaria de ser chamado (a): *

Sua resposta

Próxima Limpar formulário

Qual é seu vínculo com instituição? *

- ◯ Aluno
- ◯ Docente
- ◯ Técnico administrativo
- ◯ Terceirizado
- ◯ Outro:

Voltar Próxima Limpar formulário

O que é phishing? * 1 ponto

- ◯ Uma técnica de pesca esportiva.
- ◯ Um tipo de vírus de computador.
- ◯ Uma forma de fraude online que busca obter informações pessoais.
- ◯ Um software de segurança.

João teve sua rede doméstica invadida por um atacante.
Qual dos seguintes procedimentos configura uma possível falha que permitiu a invasão? * 1 ponto

- ◯ Desabilitar o gerenciamento do equipamento de rede via Internet.
- ◯ Usar firewall e antivírus atualizados.
- ◯ Esconder a rede, evitando que seu nome seja anunciado para outros dispositivos.
- ◯ Manter a senha padrão de fábrica do modem/roteador.

O que normalmente não acontece em casos de dados vazados? * 1 ponto

- ◯ Abertura de contas, dívidas e/ou aplicação de golpes.
- ◯ Validar dados de sistemas de golpes.
- ◯ Melhora no desempenho de sistemas
- ◯ Chantagear outras pessoas se passando por você.

Um dos cuidados recomendados no uso das redes sociais é a proteção do seu perfil.
Assinale a opção CORRETA quanto à proteção de perfis de contas. * 1 ponto

- ◯ Acesse o site da rede social sempre usando http.
- ◯ Procure usar a mesma senha para acessar diferentes sites.
- ◯ Não use opções como silenciar, bloquear e denunciar, caso identifique abusos.
- ◯ Solicite um arquivo com suas informações ou verifique o registro de atividades, caso desconfie que o seu perfil tenha sido indevidamente usado.

Existem vários tipos de códigos maliciosos.
Assinale a alternativa INCORRETA quanto à descrição de cada um deles. * 1 ponto

- ◯ Vírus: programa ou parte de uma programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo.
- ◯ Ransomware: programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário.
- ◯ Backdoor: programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e com o conhecimento do usuário
- ◯ Worm: programa capaz de se propagar automaticamente pelas redes, explorando e enviando cópias de si mesmo de equipamento para equipamento.

O uso indevido de credenciais pode ocasionar: * 1 ponto

- ◯ Atualização do sistema ou aplicativo.
- ◯ Melhor reputação da instituição junto ao público das redes sociais.
- ◯ Sérios incidentes de segurança e prejuízos pessoais e à instituição.
- ◯ Benefícios financeiros ou monetários à instituição.

Dentre os cuidados recomendados no uso das redes sociais estão o respeito à privacidade alheia e a proteção dos seus filhos.
Quanto aos cuidados citados, assinale a opção INCORRETA: * 1 ponto

- ◯ Evite divulgar imagens em que outras pessoas apareçam, sem autorização prévia.
- ◯ Evite falar sobre ações, atos e rotina de outras pessoas.
- ◯ Oriente seus filhos a se relacionarem com estranhos e a fornecer informações pessoais.
- ◯ Você estará protegendo seu filho, ao respeitar o limite de idade estipulado pelos sites

Qual das alternativas abaixo é um sinal de que um e-mail pode ser uma tentativa de phishing? * 1 ponto

- ◯ O e-mail é enviado por um amigo.
- ◯ O e-mail contém erros de ortografia e gramática.
- ◯ O e-mail é de uma loja onde você fez compras recentemente.
- ◯ O e-mail não contém links.

Ao realizar o cadastro em um site de cursos online e gratuitos, quais dados solicitados seriam suspeitos? * 1 ponto

- ◯ CPF e dados bancários
- ◯ Nome e apelido.
- ◯ Número de telefone e e-mail.
- ◯ Usuário e senha.

Qual desses é um cuidado ao se conectar a redes Wi-Fi? * 1 ponto

- ◯ Não apagar as redes que você visitou.
- ◯ Usar redes que ofereçam apenas criptografia WEP e WPA
- ◯ Não permitir que seus dispositivos se conectem automaticamente a redes públicas.
- ◯ Não se certificar de usar conexão segura.

Uma das formas de prevenção contra códigos maliciosos é manter seus equipamentos atualizados.
Assinale a alternativa CORRETA a respeito da atualização de equipamentos. * 1 ponto

- ◯ Evite usar programas originais.
- ◯ Desinstale todas as atualizações disponíveis, principalmente as de segurança.
- ◯ Crie um disco de recuperação e tenha-o por perto no caso de emergências
- ◯ Descarte o disco de emergência de seu antivírus, caso perceba que o comportamento do equipamento está estranho.

O que é um boato? *

- ◯ Uma notícia de fonte desconhecida, atualmente conhecida como fake news.
- ◯ Uma classificação de vírus, trojan e spyware.
- ◯ Um tipo de programa para varredura do sistema.
- ◯ Uma notícia de fonte confiável.

Os boatos difundidos nas redes sociais têm características próprias. Assinale a sequência correta das alternativas que podem caracterizar um boato (Fake News). *

( ) Não possui fonte ou cita fontes desconhecidas.

( ) Não apresenta evidências e nem embasamento dos fatos noticiados.

( ) Sugere consequências trágicas, se determinada tarefa não for realizada.

( ) Possui título bombástico, resumido e com destaques em maiúsculos.

- ◯ F-V-V-F
- ◯ V-V-V-V
- ◯ F-F-V-V
- ◯ V-V-V-F

Ao realizar compras online, assinale a opção que corresponde aos cuidados recomendados para melhor segurança dos seus dados pessoais. *

- ◯ Ao fornecer dados sensíveis via e-mail, é desnecessário criptografar a mensagem enviada.
- ◯ É desnecessário guardar informações da compra, como comprovantes e número do pedido.
- ◯ Certifique-se de usar conexões seguras, observando se há o desenho de cadeado fechado mostrado na ...
- ◯ Verificar se o endereço do site começa com http://

Antes de iniciar a compra online, assinale a opção que NÃO representa um cuidado recomendado: *

- ◯ Acessar o site/loja , digitando o endereço diretamente no navegador web.
- ◯ Evitar clicar em links recebidos em mensagens.
- ◯ Utilizar sempre um computador com mecanismos de segurança instalados, como antimalware, antispa...
- ◯ É desnecessário verificar se o site/loja é confiável.

Qual dos seguintes itens NÃO apresenta um risco de uso dos dispositivos móveis? *

- ◯ Vazamento de informações.
- ◯ Instalação de aplicativos legítimos.
- ◯ Invasão de privacidade.
- ◯ Propagação de códigos maliciosos.

Assinale a ação que NÃO DEVE SER FEITA, em caso de perda ou furto de um dispositivo. *

- ◯ Informar à operadora e solicitar bloqueio do número.
- ◯ Informar à empresa onde trabalha.
- ◯ Bloquear cartões de crédito cujos números estejam nele armazenados.
- ◯ Manter as senhas que possam estar nele armazenadas.

Como você pode proteger seus dados enquanto utiliza dispositivos pessoais (como notebooks e celulares) para trabalhar remotamente? *

- ◯ Armazenar dados sensíveis apenas em pastas locais, sem backup na nuvem.
- ◯ Utilizar redes de Wi-Fi públicas sem nenhum cuidado adicional.
- ◯ Configurar senhas fortes e usar criptografia de dados quando possível.
- ◯ Compartilhar os dispositivos com familiares para economizar tempo.

Qual é a principal razão para usar uma rede privada virtual (VPN) ao trabalhar remotamente? *

- ◯ Melhorar a qualidade da conexão de internet.
- ◯ Garantir que os dados sejam transmitidos de forma segura, protegendo sua privacidade.
- ◯ Aumentar a velocidade de navegação na internet.
- ◯ Facilitar o acesso a sites bloqueados pela instituição.

Qual é a principal razão para realizar cópias de segurança (backup) regularmente? *

- ◯ Para liberar espaço no dispositivo.
- ◯ Para garantir a recuperação de dados em caso de falhas no dispositivo ou ataque cibernético.
- ◯ Para aumentar a velocidade do sistema.
- ◯ Para melhorar a qualidade das imagens armazenadas.

O que deve ser evitado ao realizar backups de dados sensíveis ou confidenciais? *

- ◯ Armazenar backups em dispositivos externos criptografados.
- ◯ Usar uma senha forte para proteger os arquivos de backup.
- ◯ Manter cópias de segurança em diferentes locais, como discos rígidos externos e nuvem.
- ◯ Armazenar backups em locais acessíveis ao público, como redes não protegidas ou serviços de nuvem ...

O que é a primeira coisa que você deve fazer se seu celular for furtado? *

- ◯ Comprar outro celular imediatamente.
- ◯ Avisar seus amigos nas redes sociais.
- ◯ Bloquear o chip e o IMEI do aparelho.
- ◯ Desinstalar seus aplicativos.

Por que é importante manter o backup automático ativado no seu celular? *

- ◯ Para liberar espaço na memória interna.
- ◯ Para restaurar os dados em caso de perda ou furto.
- ◯ Para não precisar lembrar senhas.
- ◯ Para compartilhar arquivos mais rápido.

Qual é o processo adicional de autenticação, que melhora a segurança no acesso a sistemas cibernéticos? * 1 ponto

- ◯ Autenticação multifator
- ◯ Senha de terceiros.
- ◯ Botnet.
- ◯ Senha robusta.

Voltar | Enviar | Limpar formulário

ANDIFES

CGTIC

SEH
SEGURANÇA NO
ELEMENTO
HUMANO