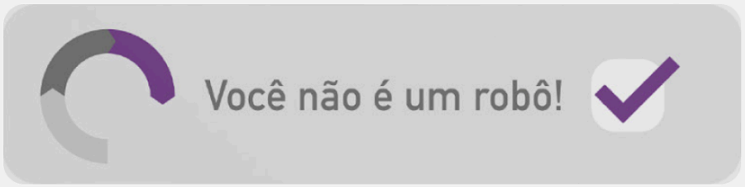
2025

Informe .seH



PLANO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

ANDIFES CGTIC .seH SEGURANÇA NO ELEMENTO HUMANO

Esta é uma versão do
Plano de Conscientização em Segurança da Informação
para o primeiro semestre de 2025.

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

[Este documento encontra-se em uma versão preliminar.]

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 primeiro semestre de 2025. 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 para o primeiro semestre

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

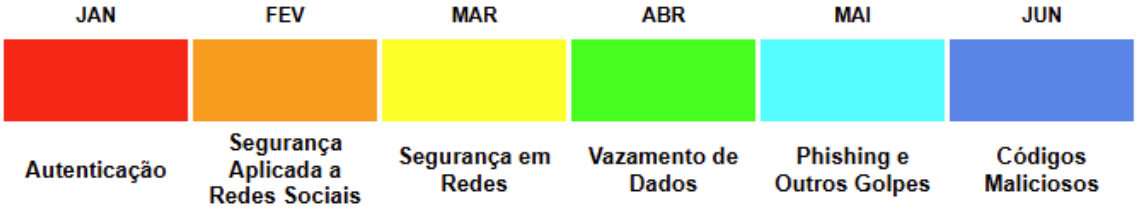


Figura 1. Temas a serem abordados.

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), mas que não foram incluídos na proposta inicial do plano de conscientização.

4. Temas da campanha

As próximas subseções apresentam os seis temas, que devem ser trabalhados ao longo deste primeiro semestre, incluindo os materiais a serem utilizados e possíveis ações a serem realizadas propostos pelas instituições participantes do CGTIC.

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 para o e-mail dos usuários da comunidade; ● Publicar a banner1 nas redes sociais; ● Veicular o audio1 na rádio (se dispor); ● Anunciar o video1 na TV (se dispor).
Semana 2	Boas práticas de autenticação	● Enviar o **texto2** para o e-mail dos usuários da comunidade; ● Publicar o **banner2** e o **vídeo3** nas redes sociais; ● Anunciar o **banner2** após o *login* no sistema de informação institucional; ● Anunciar o **video2** na TV (se dispor).
Semana 3	Uso indevido das credenciais	● Enviar o **texto3** para o e-mail dos usuários da comunidade; ● Publicar o **banner3** nas redes sociais.
Semana 4	Criando senhas robustas	● Enviar o **texto4** para o e-mail dos usuários da comunidade; ● Publicar o **banner4** e o **vídeo4** nas redes sociais; ● Enviar a **newsletter** 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 (1).txt e … > AUT_PROCESSO_EMAIL copiar.png`

banner1: [Autenticação] > [Semana1] > [Redes Sociais] > AUT_PROCESSO1_STORIE_UFRN.png, … > AUT_PROCESSO2_STORIE_UFRN.png e … > AUT_PROCESSO2_LEGENDAREDESSOCIAIS (1).txt

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

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

texto2: [Autenticação] > [Semana2] > [E-mail] > AUT_BOAS_EMAIL.txt e … > AUT_BOAS_EMAIL.txt

banner2: [Autenticação] > [Semana1] > [Redes Sociais] > AUT_BOAS_FEED.png, …> AUT_BOAS_STORIE2.png e … > AUT_BOAS_LEGENDAREDESSOCIAIS.txt

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

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

texto3: [Campanha de conscientização em SI][Temas] > [Autenticação] > [Semana3] > [E-mail] > AUT_USO_TEXTOEMAIL.txt e … > AUT_USO_EMAIL.png

banner3: [Autenticação] > [Semana3] > [Redes Sociais] > AUT_USO_FEED.png, … >AUT_USO_STORIE.png e … > AUT_USO_LEGENDAREDESSOCIAIS.txt

texto4: [Autenticação] > [Semana4] > [E-mail] > AUT_SENHAS_EMAIL.txt e … > AUT_SENHAS_EMAIL.png

banner4: [Campanha de conscientização em SI] > [[Temas] > [Autenticação] > [Semana4] > [Redes Sociais] > AUT_SENHAS_FEED.png, … > AUT_SENHAS_FEED2.png, …>AUT_SENHAS_STORIE.png, … > AUT_SENHAS_STORIE2.png e … > 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 **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 o arquivo **imagem1** nas redes sociais. ● Publicar o arquivo **imagem2** nas redes sociais ● Publicar Publicar o arquivo **imagem3** nas redes sociais ● Publicar o arquivo **imagem4** nas redes sociais ● Publicar o arquivo **imagem5** nas redes sociais
Semana 2	Cuidados com redes Wi-fi desconhecidas	● Publicar o **audio1** na rádio universitária; ● Publicar os VTs **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 **imagem1** e texto **texto1**; ● Enviar **imagem2** e **texto2** para os

		e-mails.
Semana 2	Proteção de dados pessoais	• Veicular o **audio1** para a rádio institucional; • Publicar nas redes sociais **imagem3** e texto **texto3**.
Semana 3	Segurança de senhas	• Publicar o vídeo **video1** no Youtube; • Anunciar o **audio2** para a rádio institucional; • Publicar nas redes sociais **imagem4** e texto **texto4**.
Semana 4	Verificação em dois fatores e cuidados com links	• Publicar o vídeo **video2** no Youtube; • Publicar o vídeo **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 **stories1** e **stories2**; ● Publicar nas redes sociais **carrossel1** e **texto1**; ● Enviar e-mails com **imagem1** e **texto2**; ● Veicular na rádio institucional o **audio01**.
Semana 2	Segurança financeira digital	● Publicar nas redes sociais **stories3** e **stories4**; ● Publicar nas redes sociais

		carrossel2 e **texto3**; ● Enviar e-mails com **imagem2** e **texto4**.
Semana 3	Segurança em apps	● Publicar nas redes sociais **stories5**; ● Enviar e-mails com **imagem3** e **texto5**; ● Postar v**ideo1** no Youtube.
Semana 4	Dicas de segurança	● Publicar nas redes sociais **stories6** e **stories7**; ● Enviar e-mail com **texto6** + **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 **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 **texto3**; ● Publicar no feed das redes sociais a **imagem4 e texto4**.
Semana 3	Perda de dados e importância do backup	● Veicular na rádio comunitária o **audio1**; ● Enviar por e-mail a **imagem5** e **texto5**; ● Publicar no feed das redes sociais a **imagem6** e **texto6**.
Semana 4	Importância de se usar senhas seguras	● Veicular na rádio comunitária o **audio2**; ● Publicar nos stories das redes sociais **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

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 a cada semestre.
- 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.

[1] Site: https://getgophish.com/

Um manual com recomendações mais detalhadas encontra-se em fase de elaboração.

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 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 seis temas principais para serem trabalhados ao longo do semestre, 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.

[2] Site: https://br.creativecommons.net

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.

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

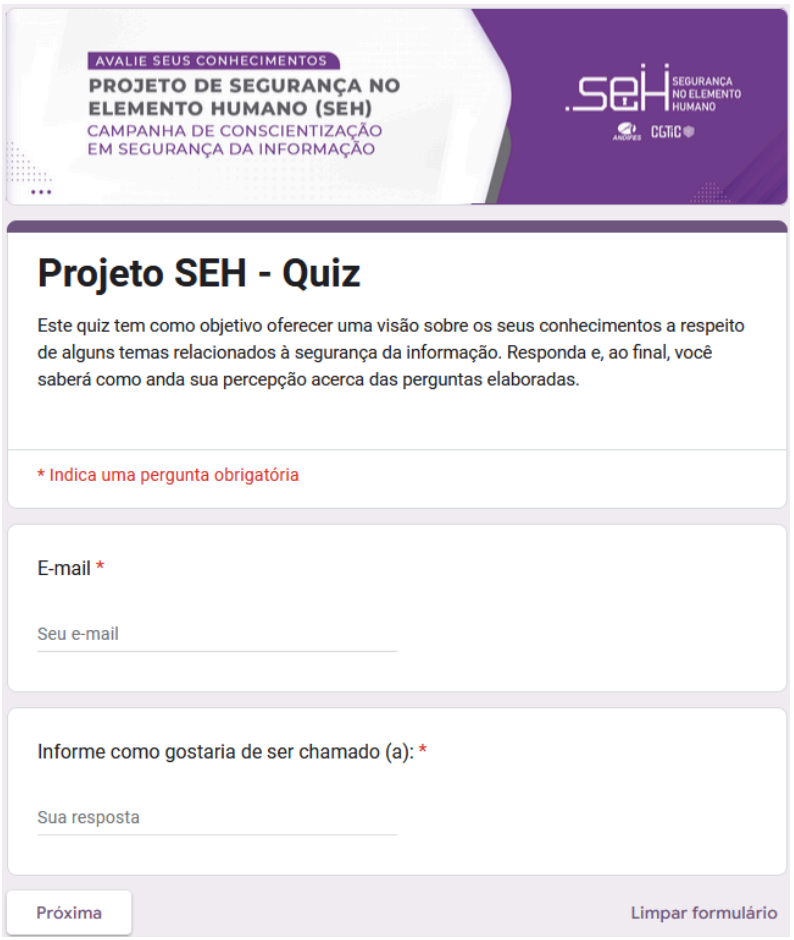
O modelo de formulário aqui apresentado foi construído no Google Form com a intenção de facilitar a criação, configuração e correção automática das questões apresentadas no Apêndice A.

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:



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.

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