Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto

Descrição gerada automaticamente

**Instituto de Gestão e Tecnologia da Informação**

**Relatório do Projeto Aplicado**

Proposta de um sistema de campanhas de *phishing* baseado em uma política de base conceitual *behaviorista*

Guilherme da Franca Batista

Orientador: Professor Maximiliano Jacomo

2022

****

**GUILHERME DA FRANCA BATISTA**

**INSTITUTO DE GESTÃO E TECNOLOGIA DA INFORMAÇÃO**RELATÓRIO DO PROJETO APLICADO

PROPOSTA DE UM SISTEMA DE CAMPANHAS DE *PHISHING* BASEADO EM UMA POLÍTICA DE BASE CONCEITUAL *BEHAVIORISTA*

Relatório de Projeto Aplicado desenvolvido para fins de conclusão do curso de MBA em Segurança Cibernética.  
  
Orientador: Professor Maximiliano Jacomo

**Guarulhos  
2022**

**Sumário**

[1. CANVAS do Projeto Aplicado 4](#_Toc101281510)

[1.1 Desafio 5](#_Toc101281511)

[1.1.1 Análise de Contexto 5](#_Toc101281512)

[1.1.2 Personas 6](#_Toc101281513)

[1.1.3 Benefícios e Justificativas 7](#_Toc101281514)

[1.1.4 Hipóteses 8](#_Toc101281515)

[1.2 Solução 9](#_Toc101281516)

[1.2.1 Objetivo SMART 9](#_Toc101281517)

[1.2.2 Premissas e Restrições 11](#_Toc101281518)

[1.2.3 Backlog de Produto 13](#_Toc101281519)

[2. Área de Experimentação 14](#_Toc101281520)

[2.1 Sprint 1 16](#_Toc101281521)

[2.1.1 Solução 16](#_Toc101281522)

[● Evidência do planejamento: 16](#_Toc101281523)

[● Evidência da execução de cada requisito: 16](#_Toc101281524)

[● Evidência dos resultados: 16](#_Toc101281525)

[2.1.2 Experiências vivenciadas 16](#_Toc101281526)

[2.2 Sprint 2 17](#_Toc101281527)

[2.2.1 Solução 17](#_Toc101281528)

[● Evidência do planejamento: 17](#_Toc101281529)

[● Evidência da execução de cada requisito: 17](#_Toc101281530)

[● Evidência dos resultados: 17](#_Toc101281531)

[2.2.2 Experiências vivenciadas 17](#_Toc101281532)

[2.3 Sprint 3 18](#_Toc101281533)

[2.3.1 Solução 18](#_Toc101281534)

[● Evidência do planejamento: 18](#_Toc101281535)

[● Evidência da execução de cada requisito: 18](#_Toc101281536)

[● Evidência dos resultados: 18](#_Toc101281537)

[2.3.2 Experiências vivenciadas 18](#_Toc101281538)

[3. Considerações Finais 19](#_Toc101281539)

[3.1 Resultados 19](#_Toc101281540)

[3.2 Contribuições 19](#_Toc101281541)

[3.3 Próximos passos 19](#_Toc101281542)

## 1. CANVAS do Projeto Aplicado

Figura conceitual, que representa todas as etapas do Projeto Aplicado.



## Desafio

### 1.1.1 Análise de Contexto

Há cerca de setenta e um anos atrás, Presper Eckert e John Mauchly, engenheiros da Universidade da Pensilvânia, entregaram ao governo americano o *Universal Automatic Computer I* (*Univac-I*) para que o Departamento de Censo dos Estados Unidos da América pudesse realizar o monitoramento do *Baby Boom*[[1]](#footnote-1). Nesta época, apesar de estas máquinas estarem sendo usadas em larga escala pelos setores civil e militar do governo americano e por outras grandes corporações, as pessoas ainda não poderiam vislumbrar o que haveria de vir em pouco tempo. No domínio da literatura, um dos criadores do gênero *cyberpunk*, William Gibson, em seu romance *Neuromancer*, conseguiu, ainda em 1984, ter um vislumbre do futuro, criando a ideia do cyberespaço que consiste um espaço virtual composto por cada computador e usuário conectados em uma rede mundial. Desde a década de 90, a evolução de hardware e software, seguindo as leis de *Moore*[[2]](#footnote-2) e os saltos qualitativos observados por Brooks[[3]](#footnote-3), foi cada vez mais rapidamente transformando o mundo, aproximando as pessoas, criação de modelos de negócio completamente novos e novos hábitos na sociedade através da evolução tecnológica das redes e dispositivos computacionais cada vez mais acessíveis e simples de serem utilizados pela população mundial. Esta nova era do mundo digital trouxe novas oportunidades e com certeza muitos desafios, como a da segurança cibernética para o contexto empresarial e pessoal.

No início dos anos 2000, a primeira grande ameaça em forma de *phishing* contra um banco foi realizada[[4]](#footnote-4) e esse tipo de atividade criminosa foi, ao longo dos anos se tornando mais comuns e ficando cada vez mais fidedignas. A infração de enganar pessoas para que estas compartilhem informações pessoais como senhos, números de cartão de crédito e XPTO não é nova. O termo foi cunhado em 1987 em um artigo e apresentação da *International HP Users Group* e supõe-se que esta prática ocorre desde a década de 60. Estes ataques não possuem apenas uma única categoria de pessoas alvo, como bancários, industriais, comerciantes ou zeladores, eles são enviados para pessoas de variados níveis sociais e culturais com o objetivo único de ganhar vantagem sobre as pessoas.

Um fato extraordinário aumentou bastante o número de ataques cibernéticos de modo geral, o avento da pandemia de *COVID-19* em dezembro de 2019. Após decretos de *lockdowns* por potências estrangeiras e políticas de confinamento em território nacional, a sociedade precisou se adaptar e digitalizar o máximo de atividades presenciais e manuais possível para que o mínimo da parcela da população precisasse deixar seus lares e assim evitar o contágio da nova variante *SARS-CoV*. Assim sendo, muitas empresas adotaram o trabalho remoto, implantando de forma rápida e muitas vezes insegura as *VPN’s* e infraestruturas necessárias para esta nova realidade e em muitas dessas ocasiões o treinamento necessário para adoção de boas práticas e mitigação das ameaças cibernéticas foram negligenciadas.

Assim sendo, neste cenário de uma sociedade cada vez mais conectada à rede mundial de computadores, negócios cuja sobrevivência está estritamente ligada a seus ativos digitais e a privacidade e segurança de pessoas empresas em constante risco de violação, o desafio deste projeto aplicado é de propor um sistema de gerenciamento de campanhas de *phishing* com uma base sólida, especificamente da psicologia comportamental ou behaviorismo, para que os colabores das organizações que possuem restrições financeiras para a contratação de serviços deste tipo ou implantação de sistemas complexos e de alto custo possam ter acesso a software livre e uma base sólida para a criação dos testes, acompanhamento dos resultados e engajamento dos envolvidos além da possibilidade de extrair *insights* e propostas com mais qualidade.

**Matriz CSD**

Aspirando a uma melhor compreensão do cenário e do problema apresentado a este projeto aplicado, seguir-se-á na apresentação do artefato proposto nesta seção, a saber, a matriz CSD, cujo acrônimo significa Certezas, Suposições e Dúvidas, uma técnica simples na qual três ângulos importantes sobre um determinado projeto são listados de modo a auxiliar na obtenção de informações necessárias que proporcionam o esclarecimento de ideias, bem como o melhor entendimento das partes envolvidas. Sua aplicabilidade se faz por meio de uma representação visual – um quadro ou tabela – em que durante a confecção inicial do projeto os envolvidos possam preencher as certezas, suposições e dúvidas presentes no projeto e inerentes ao problema no qual busca-se uma solução.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Certezas** | **Suposições** | **Dúvidas** |
| **Atores** | Colaboradores estão expostos a ameaças provindas de *phishing* a todo momento. | Realizar uma pesquisa teórica e empírica sobre a taxonomia dos diversos tipos de phishing pode ser viável. | Quais são as formas mais e menos comuns de ataques a empresas através de *phishing*? |
| **Cenário** | Todo colaborador é um potencial vetor para ataques à organização a qual prestam serviços. | Colaboradores são pessoas e, assim sendo, estão sujeitos a manipulações de caráter psicológico criadas por criminosos cibernéticos. | Como evitar que os trabalhadores sejam vítimas dos ataques ou chegar mais próximo da mitigação desse risco? |
| **Regra** | Definir um modelo conceitual behaviorista para que um sistema de campanhas de *phishing* seja implementado. | Conhecer modelos tradicionais da psicologia comportamental (Watson e Skinner) e ferramentas técnicas que viabilizem a construção do sistema. | Qual seria o melhor modelo psicológico para tomar como base e quais ferramentas são as mais indicadas para a construção do sistema? |

**Observação do tipo POEMS**

Para que o desafio deste projeto aplicado possa ser concluído, a utilização do POEMS (Pessoas, Objetos, Ambiente, Mensagem e Serviço), um *framework* que tem como objetivo principal orientar e estruturar toda a pesquisa deste trabalho acadêmico, também será utilizado, tornando mais fácil sintetizar as observações feitas por mim bem como a identificar as correlações e contrastes existentes no desafio e em todo o projeto aplicado.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Pessoas** | **Objetos** | **Ambientes** | **Mensagem** | **Serviços** |
| Quem está presente no contexto da análise? | Que objetos fazem parte do ambiente? | Quais são as características do ambiente? | Que mensagens são comunicadas? | Quais são os serviços oferecidos? |
| Alta administração da empresa;  Colaboradores da área de TI (*Blue* e *Red Team’s* se houver) | Sistemas operacionais das estações de trabalho; Servidores que mantém as aplicações da empresa. | Usuários internos acessando sistemas internos da empresa. | Logs de sistemas operacionais das estações;  Logs das aplicações corporativas | Sistemas e aplicações da empresa na internet e intranet. |
| **Registros** | |  | **Insights** | |
| Resultados obtidos após relatórios apresentados pela área de T.I. da empresa após análise inicial de vulnerabilidade.  Lições que serão aprendidas no decorrer das sprints. | |  | Por enquanto, ainda não foi possível ter insights. | |

### 1.1.2 Personas

Nesta seção apresentaremos as pessoas envolvidas diretamente no problema apresentado, definindo as características pessoais, sociais, intelectuais e profissionais, de acordo com o mapa de empatia e suas seções.

****

**Mapas de Empatia**

Os mapas de empatia pensados para este trabalho são no total de três. O primeiro deles refere-se à alta administração da organização que tomará decisões importantes na adoção ou não do sistema proposto e também são em última instância os mais impactados pelo tipo de ataque que o projeto tem objetivo por mitigar.

O segundo,

Por fim, o último mapa de empatia diz respeito a ameaça que gostaríamos de prevenir. Sua forma é sistêmica pois ela usa o e-mail como veículo de propagação, mas sua natureza é de natureza humana por conter elementos que levam os colaboradores a cair nelas.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mapa de empatia**: Alta administração | | | | | |
| **Quem** | **Fazer** | **Vê** | **Diz** | **Faz** | **Ouve** |
|  |  |  |  |  |  |
| **Pensa / Sente** | | | | | |
| **Dores** | | | **Ganhos** | | |
|  | | |  | | |

### 1.1.3 Benefícios e Justificativas

**O que significa esta seção?**

Esta seção tem o objetivo de apresentar as justificativas e os benefícios que motivam o desenvolvimento do projeto; nela apresentaremos os dados em forma de lista em duas seções respectivamente.

Como justificativa a realização deste projeto e solução do desafio/problema proposto por ele, destacamos os seguintes pontos:

1. **A**
2. **B**
3. **C**
4. **D**
5. **E**
6. **F**
7. **G**

Como benefícios em decorrência da realização deste projeto e resução do desafio/problema proposto por ele, destacamos os seguintes pontos:

1. **A**
2. **B**
3. **C**
4. **D**
5. **E**
6. **F**
7. **G**

**Blueprint**

Para proporcionar um melhor entendimento, a seguir apresentamos as interações existentes através do Blueprint que permite encontrar pontos de melhorias e oportunidades de inovação para a realização desse projeto. Posteriormente, segue-se o Canvas Proposta de valor que tem como objetivo auxiliar na criação e posicionamento dos serviços em torno do que a alta administração da Organização Tabajara deseja e precisa em relação a segurança da informação.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Blueprint** |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**CANVAS de proposta de Valor**

seguintes

### 1.1.4 Hipóteses

A partir do **conhecimento aprofundado do contexto** do desafio e **da definição das personas**, nesta seção será mostrada uma tabela contendo as hipóteses levantadas para este projeto aplicado.

**Matriz de observações para hipóteses**

|  |  |
| --- | --- |
| **Observação** | **Hipóteses** |
|  |  |
|  |  |
|  |  |
|  |  |

Diante das hipóteses expostas acima, realizou-se um brainstorm com o objetivo de priorizar as ideias em relação ao (projeto aqui). Neste contexto, as principais ideias levantadas foram: ex: 1- O serviço utiliza o TOMCAT um software open source;, 2- O teste de intrusão é necessário para apurar vulnerabilidades, 3- Realizar as tratativas em relação as vulnerabilidades encontradas, 4- Validar as tratativas realizadas em relação as vulnerabilidades encontradas, 5- Aplicar uma metodologia de melhoria contínua em relação a proteção do servidor

**Priorização de Ideias**

|  |  |
| --- | --- |
| **Cenários** | |
| **C1** | Complexidade na execução do projeto |
| **C2** | Urgência na execução do projeto |
| **C3** | Investimento necessário a execução do projeto |
| **C4** | Benefícios esperados ao final do projeto |
| **C5** | Nível de satisfação da alta administração |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Escala** | **Benefícios** | **Abrangência** | **Satisfação** | **Investimento** | **Clientes**  **(impacto)** | **Operacional**  **(dificuldade)** |
| **5** | Valor imediato para o modelo de negócio | Total | Total | Nenhum | Muito fácil | Muito fácil |
| **4** | Significativo para o modelo de negócio | Grande | Grande | Baixo | Fácil | Fácil |
| **3** | Razoável para o modelo de negócio | Razoável | Razoável | Médio | Médio | Médio |
| **2** | Pouco para o modelo de negócio | Pequena | Pequena | Alto | Grande | Grande |
| **1** | Baixo para o modelo de negócio | Baixa | Baixa | Elevado | Elevado | Elevado |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ideias** | **Comparação de Cenários** | | | | | |
|  |  | | | | | |
|  | **Cenário 1** | **Cenário 2** | **Cenário 3** | **Cenário 4** | **Cenário 5** | **Total** |
| 1 - |  |  |  |  |  |  |
| 2 - |  |  |  |  |  |  |
| 3 - |  |  |  |  |  |  |
| 4 - |  |  |  |  |  |  |
| 5 - |  |  |  |  |  |  |
| 6 - |  |  |  |  |  |  |

seguintes

## Solução

Esta seção tem o objetivo de apresentar, de maneira bem estruturada, os objetivos do projeto, definindo expectativas claras e objetivas, para maximizar as chances de alcançar os resultados esperados.

### 1.2.1 Objetivo SMART

Esta seção tem o objetivo de apresentar, de maneira bem estruturada, os objetivos do projeto, definindo expectativas claras e objetivas, para maximizar as chances de alcançar os resultados esperados.

### 1.2.2 Premissas e Restrições

**O que significa esta seção?**

Esta seção tem o objetivo de apresentar as condições necessárias para que o projeto seja desenvolvido de maneira eficiente.

**Matriz de Riscos**

Enquanto

### 1.2.3 Backlog de Produto

**O que significa esta seção?**

Esta seção tem o objetivo de apresentar, de maneira bem detalhada, o backlog de requisitos idealizados para o desenvolvimento da solução.

O Backlog de Produto deve ser sempre atualizado, de acordo com a evolução do projeto.

**Como esta seção deve ser preenchida?**

Deve-se criar uma lista de requisitos necessários para o desenvolvimento da solução, alinhando os mesmos com as disciplinas futuras a serem cursadas.

É importante que você **defina sprints de desenvolvimento da solução**, de acordo com as próximas disciplinas.

No seu planejamento, no total, devem ser consideradas as realizações de 3 sprints.

**Trello**

# 2. Área de Experimentação

**O que significa esta seção?**

Esta seção tem o objetivo de apresentar as evidências do planejamento dos requisitos selecionados do Backlog de Produto, além de mostrar a maneira como eles foram desenvolvidos e registrar os resultados alcançados.

É necessário expor a execução e a validação dos experimentos relacionados ao desenvolvimento da solução, ou seja, testar se você está no caminho certo ou se algo precisa ser modificado (pivotar).

**Quais etapas já devem estar finalizadas no momento do preenchimento desta seção? (Pré-requisitos)**

No momento do preenchimento, é esperado que você já tenha cursado a disciplina de Inovação e Design Thinking, em especial as etapas do processo de Design Thinking, além de estar se preparando para desenvolver a solução idealizada no seu Projeto Aplicado.

Você também já deve ter preenchido o primeiro capítulo deste relatório (CANVAS do Projeto Aplicado).

**Como esta seção deve ser preenchida?**

Esta seção é a área mais dinâmica do CANVAS do Projeto Aplicado. Nela você deverá inserir os experimentos necessários para desenvolver e validar cada Sprint. Ao final do experimento, você deverá preencher o item “**Solução**” da seguinte maneira:

* **Evidência do Planejamento**: comprove que os requisitos referentes à Sprint foram efetivamente planejados. Para isso, utilize o Trello e adicione, neste campo, uma cópia da tela da ferramenta com a Sprint planejada.
* **Evidência da Execução de cada Requisito**: para cada requisito planejado, adicione um artefato que comprove o cumprimento da etapa. Podem ser anexados, por exemplo, códigos, documentos, modelos, scripts, capturas de tela, entre outros. *Importante: o número de artefatos adicionados deve ser o mesmo que o número de requisitos planejados.*
* **Evidência da Solução**: os requisitos implementados contribuem para o alcance de um resultado geral, que deverá ser comprovado neste campo. Isso será feito por meio de capturas de tela, gráficos, modelos, textos, figuras, tabelas, testes, entre outros.

Para cada Sprint, cite no item “**Experiências vivenciadas**” o que não foi validado, mas forneceu insights para ajuste da rota.

**Quais ferramentas devem ser utilizadas?**

Obs.: Para realização desta seção você deverá utilizar o Trello.

## 2.1 Sprint 1

### 2.1.1 Solução

#### Evidência do planejamento:

#### Evidência da execução de cada requisito:

#### Evidência dos resultados:

### 2.1.2 Experiências vivenciadas

## 2.2 Sprint 2

### 2.2.1 Solução

#### Evidência do planejamento:

#### Evidência da execução de cada requisito:

#### Evidência dos resultados:

### 2.2.2 Experiências vivenciadas

## 2.3 Sprint 3

### 2.3.1 Solução

#### Evidência do planejamento:

#### Evidência da execução de cada requisito:

#### Evidência dos resultados:

### 2.3.2 Experiências vivenciadas

# 3. Considerações Finais

## 3.1 Resultados

Por meio de um texto detalhado, apresente os principais resultados alcançados pelo seu Projeto Aplicado.

Cite os pontos positivos e negativos, as dificuldades enfrentadas e as experiências vivenciadas durante todo o processo.

## 3.2 Contribuições

Apresente quais foram as contribuições que o seu Projeto Aplicado trouxe para que o Desafio proposto fosse solucionado.

Cite, por exemplo, as inovações, as vantagens sobre os similares, as melhorias alcançadas, entre outros.

## 3.3 Próximos passos

Descreva quais são os próximos passos que poderão contribuir com o aprimoramento da solução apresentada pelo seu Projeto Aplicado.

1. Termo que se refere a explosão demográfica entre os anos 1946 e 1964 nos EUA. [↑](#footnote-ref-1)
2. Lei/observação feita por Gordon Earle Moore em 1965 que consiste no aumento de cem por cento dos transistores dos chips, pelo mesmo custo, a cada dois anos. [↑](#footnote-ref-2)
3. Referimo-nos ao artigo *No Silver Bullet – Essence and Accident in Software Engineering* publicado por Frederick Phillips Brooks Jr em 1987 pela Universidade da Carolina do Norte. [↑](#footnote-ref-3)
4. No início dos anos 2000 sistemas de pagamento foram o grande foco de ataques de larga escala por *phishing*. Softwares, como o *Turnkey*, foram disponibilizados no mercado negro e a *Gartner* estima que cerca de 3.6 milhões de pessoas perderam 3.2 bilhões de dólares em um período de um ano. [↑](#footnote-ref-4)