igti

RELATÓRIO

PROJETO APLICADO

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

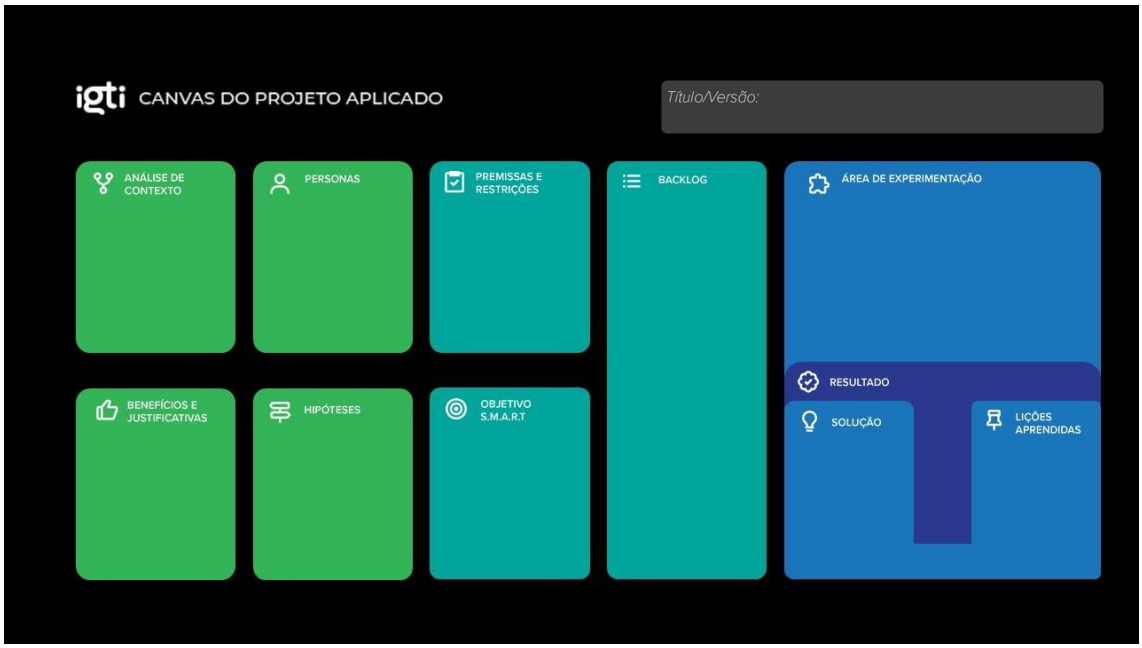
Guarulhos

2022

Sumário

1. CANVAS do Projeto Aplicado

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



1.1 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]. 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] e os saltos qualitativos observados por Brooks[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] 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

[1] Termo que se refere a explosão demográfica entre os anos 1946 e 1964 nos EUA.
[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.
[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.
[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.

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?

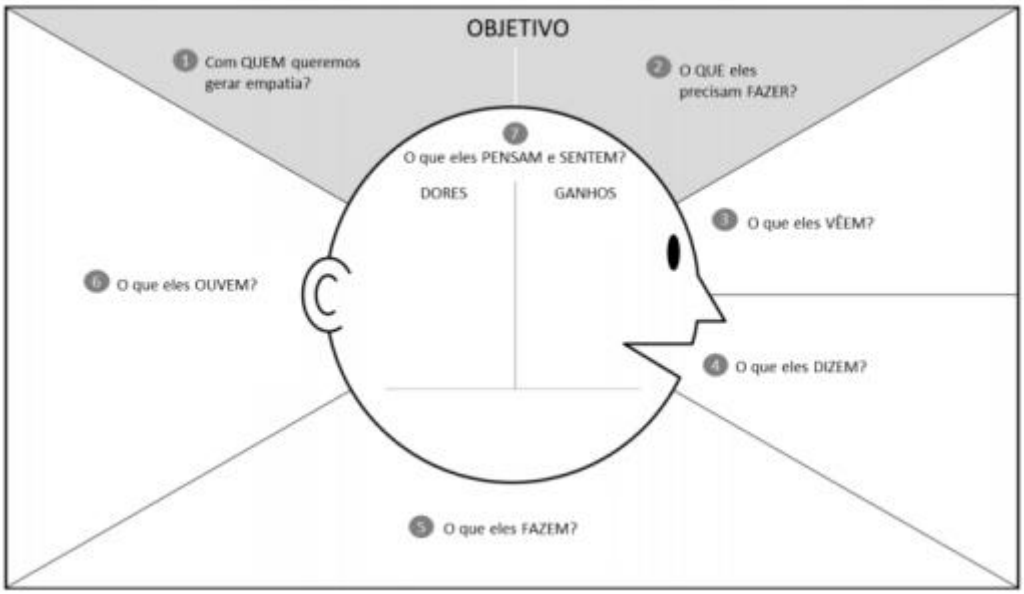
Observação do tipo POEMS

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, é o mapa de empatia relacionado à equipe de TI da empresa (segurança mais especificamente). É ela uma das mais importantes áreas, responsável por elaborar, acompanhar e conscientizar todas as outras áreas a respeito da necessidade da defesa cibernética dentro da organização.

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**
Board Executivo/Diretoria	Transmitir segurança e seriedade nos negócios aos clientes; Certificar que dados e informações essenciais para o negócio da empresa estejam protegidas.	Oportunidade de aumentar a reputação da corporação e ganho de novos clientes com uma empresa mais protegida; Perda financeira e potencial perda de clientes por quebra da reputação causada por incidentes de intrusão.	Eu preciso que os colaboradores da empresa estejam muito bem preparados para possíveis ataques de *phishing* que venham a causar impactos; Eu quero que os clientes e a sociedade captem a empresa possui uma boa política de segurança.	Administração e gerenciamento geral da empresa; Planeja as metas estratégicas e cria metas para os departamentos;	Notícias na mídia sobre roubo de dados por e-mails enviados por criminosos; Amigos e conhecidos terem seus negócios arruinados por conta de invasões;
Pensa / Sente					
Dores			**Ganhos**		
Dados da organização sequestrados por criminosos a espera de altas quantias para o resgate; Dados e informações vazados para empresas concorrentes.			Aumentar a segurança da empresa; ter colaboradores mais preparados para lidar com e-mails externos ou suspeitos; aumentar a credibilidade da empresa de maneira geral.		

Mapa de empatia: Equipe/Área de Segurança da Informação					
Quem	**Fazer**	**Vê**	**Diz**	**Faz**	**Ouve**
Analistas técnicos e funcionais de Segurança da Informação	Gerenciar sistemas e tecnologias que ajudam a garantir a proteção dos ativos digitais da empresa; Monitorar a infraestrutura e rede da organização; Responder a incidentes de segurança; Elaborar novas formas de proteger a organização contra ataques cibernéticos.	Colaboradores sem uma preparação adequada para lidar com tentativas de *phishing*, inclusive no alto escalão da organização; Empresa em constante crescimento, dados importantes sendo adquiridos e cobiçados seja pela concorrência seja por criminosos.	Precisamos garantir a segurança dos ativos digitais da empresa; Ter uma política de *phishing* com uma base conceitual mais fundamentada, não dependendo apenas da experiência ou empirismo de colabores da equipe de segurança.	Monitoram a infraestrutura e rede da organização; Elaboram estratégias para proteger a organização contra ataques cibernéticos;	Corporações sofrem ataques diariamente; Grande parte dos ataques se iniciam através de técnicas de engenharia social; A alta administração preocupada com o preparo de seus colaboradores para lidar com ataques cibernéticos.
Pensa / Sente					
Dores			**Ganhos**		
A empresa ser vítima de ataques cibernéticos; ter sistemas comprometidos e dados vazados; não ter uma empresa comprometida ou preparada para lidar com a principal porta de entrada dos ataques, i.e., o *phsihing*.			Empresa mais protegida; colaboradores de todos os departamentos colaborando para um ambiente mais seguro; tríade CIA sendo completamente entregue.		

Mapa de empatia: Ameaça					
Quem	**Fazer**	**Vê**	**Diz**	**Faz**	**Ouve**
Humana	Explorar vulnerabilidades em servidores e sistemas da organização; Proporcionar ganhos ilícitos para o praticante e perdas financeiras para a organização atacada.	Oportunidades em explorar a organização tendo como porta de entrada cada um de seus colaboradores; falha na avaliação de e-mails pelos colaboradores de todos os níveis hierárquicos da organização.	Eu quero explorar vulnerabilidades, principalmente as que envolvam engenharia social, muito mais eficazes contra pessoas; eu quero obter informações seja para vendê-las para a própria organização após o sequestro de dados ou sistemas ou para o concorrente.	Explora vulnerabilidades, também de caráter humano; aplica golpes em pessoas; coleta e sequestra dados fundamentais para a sobrevivência da organização.	Que a maioria das pessoas ainda estão despreparadas para lidar com ataques de engenharia social; muitas organizações não possuem políticas bem estabelecidas ou campanhas de *phishing* eficazes.
Pensa / Sente					
Dores			**Ganhos**		
Ser detectado ou o link com código malicioso não ser aberto pelo colaborador; ser preso por praticar crime.			Experiência ao atacar organizações; ganhos financeiros através da venda de informações e/ou sistemas.		

1.1.3 Benefícios e Justificativas

Esta seção do trabalho tem por objetivo a apresentação das justificativas e dos benefícios que motivam o desenvolvimento do projeto; nela apresentaremos os dados em forma de lista em duas seções que seguem respectivamente.

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

a) Aumento exponencial de crimes cibernéticos, principalmente após transformação digital ocorrida em tempo recorde após a pandemia da *COVID-19*.
b) Preocupação da alta administração com o preparo dos colaboradores da organização para mantê-la segura e a preservação dos recursos de T.I.
c) Organizações com pouco recurso financeiro para implementar campanhas de *phishing* e organizações com testes sem embasamento teórico.
d) Organizações cada vez mais dependentes dos ativos digitais para a continuidade do negócio.
e) Pessoas suscetíveis a ataques de engenharia social.
f) Programas de *phsihing* "para inglês ver", ou seja, e-mails de teste pouco fidedignos e sem o devido acompanhamento para melhoria contínua dos colaboradores na detecção de ameaças.
g) Programas de *phishing* sem a correta elaboração ou embasamento.

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

a) Sistema e política gratuitos, com pouca necessidade de investimento em infraestrutura para a viabilização dos mesmos.
b) Campanhas mais elaboradas, com base em teorias behavioristas, i.e., a mesma arma utilizada no ataque servirá para a defesa.
c) Mitigação de riscos envolvendo ataques de engenharia social por *e-mail*.
d) Credibilidade da organização tende a crescer e se consolidar.
e) Colaboradores mais capacitados na detecção de ameaças.
f) Alta administração percebe alto valor em uma proposta que traz ganhos qualitativos à organização sem necessariamente um alto custo envolvido na solução proposta.

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 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	Identificar ataques por e-mail	Analisar os e-mails	Validação de tentativa	Feedback sobre o teste
Ações do colaborador	Identificar um e-mail suspeito, analisá-lo e reportar a equipe de segurança da informação a possível tentativa de ataque.			
Objetivos	Mitigar ameaças e ter colaboradores mais capacitados na identificação de ameaças.			
Atividades	Criar modelo conceitual e desenvolver sistema de campanhas.			
Questões	Qual modelo psicológico será adotado na elaboração da política? Qual linguagem de programação será utilizada para construir o sistema? Existirão integrações com outros softwares?			
Barreiras	Prazos para elaboração de todo o material.			
Saídas desejáveis	Garantia da segurança da organização.			
Funcionalidades	Execução de campanhas de *phishing* para toda a organização.			
Interação	Feedback para colaboradores sobre sucesso ou falha de testes e resultados para a alta administração acompanhar o andamento e evolução do nível de detecção.			
Mensagem	Mitigação de vulnerabilidades.			
Onde ocorre	Na estação de trabalho de todos os colaboradores através do cliente de e-mail.			
Tarefas Aparentes	Escolha de modelo conceitual adequado para execução de campanha.			
Tarefas Escondidas	Acompanhamento dos testes e constante evolução na modelagem de campanhas.			
Processos de suporte	Disposição da equipe de segurança da informação em realizar constante acompanhamento das campanhas.			

CANVAS de proposta de Valor

O canvas ainda não foi desenhado. Em processo de criação.

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
Ameaças por e-mail através de engenharia social são portas de entrada perigosas para os sistemas e dados da organização.	Supõe-se que que todo o gênero humano é suscetível a ameaças que venham com gatilhos e mecanismos psicológicos próprios da nossa espécie e de nossa evolução.
Alta administração está ciente da importância da segurança de seus ativos.	Supõe-se que a alta administração tem simpatia por essa nova proposta e ajudará às demais áreas a adotarem e seguirem as orientações do time de segurança no que diz respeito ao treinamento/novo paradigma de campanhas de *phishing*.
Equipe de segurança da informação possui metodologias e ferramentas de segurança, mas ainda não possui o apoio necessário para lidar com ataques aos colabores através de engenharia social.	Supõe-se que a equipe de segurança tem preparo e background suficiente para lidar com o novo sistema e política de campanhas de *phishing*.
Colaboradores são pessoas e assim sendo são suscetíveis a ataques.	Supõe-se que que os colaboradores da organização não possuam treinamento adequado ou suficiente para conter todas ou a maioria das tentativas de ataque.

Diante das hipóteses expostas acima, realizou-se um *brainstorm* com o objetivo de priorizar as ideias em relação ao projeto proposto. Neste contexto, as principais ideias levantadas foram:

1- Levantar, analisar, compilar e propor um modelo conceitual com base no behaviorismo para o sistema de gerenciamento de campanhas proposto.
2- Analisar e empregar tecnologias de caráter *open source* para que a implantação seja possível e sem custos elevados nas organizações.
3- Aplicar uma metodologia com fortes bases para elaboração das campanhas.
4- Com o avanço das campanhas

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	4	5	3	5	4	21
2	4	3	3	4	3	17
3	5	4	2	3	4	18
4	5	3	4	5	5	22

1.2 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. De modo geral, a proposta de solução para o projeto se divide nas categorias teórica e prática. A primeira referindo-se a analise das correntes comportamentais para que, após entendimento da linha e mecanismos a serem adotados, a segunda parte, a prática possa ser iniciada. Nela, bases de dados e sistema para gerenciamento de campanhas serão desenvolvidos usando os insumos da parte inicial. Para melhor compreensão, o artefato de objetivo SMART será apresentado a seguir.

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.

S (Specific - Específico)	Tornar a organização mais segura e mitigar ameaças por meio de correio eletrônico.
M (Mensurable - Mensurável)	Satisfação dos diversos departamentos e controle centralizado do sucesso ou não dos colaboradores nos testes de simulação de intrusão por e-mails maliciosos.
A (Attainable - Antigível)	Realização de disparos de campanhas de *phishing*.
R (Relevant - Relevante)	Proteção dos ativos de T.I. e aumento da crença de garantia de continuidade dos negócios da organização.
T (Time Based - Temporal)	Aumento da eficiência na detecção de ameaças cibernéticas pelos colaboradores da organização e, por consequência, aumento da reputação da mesma perante a sociedade.

1.2.2 Premissas e Restrições

Esta seção tem o objetivo de apresentar as condições necessárias para que o projeto seja desenvolvido de maneira eficiente. Assim sendo, a matriz de riscos será apresentada a seguir.

O projeto apresenta as seguintes premissas:

a) A maior parte das tentativas de *phishing* deve ser reconhecida pelos colaboradores após certo período de campanhas.
b) O sistema, base de conhecimento e estratégias devem ser atualizadas com muita frequência para que os testes não se tornem "viciados" ou facilmente detectados. A verossimilhança com ataques de criminosos verdadeiros deve ser almejada sempre.
c) O resultado deve ser satisfatório.

O projeto apresenta as seguintes restrições:

a) Deve utilizar uma aproximação teórica confiável para concepção e desenvolvimento do projeto.
b) Deve ser *open source* e bem documentado para utilização em qualquer organização que quiser adotá-lo.
c) Deve ser realizado com o menor custo financeiro possível.

Matriz de Riscos

De acordo com as premissas e restrições do projeto, os riscos foram identificados e correlacionados entre impacto e probabilidade. O resultado pode ser encontrado logo abaixo em forma tabular.

Risco	Probabilidade	Impacto	Ação
Falso/Positivo durante a fase inicial de implementação do sistema.	Alto	Médio	Análise cuidadosa e detalhada da equipe de segurança da informação durante as etapas iniciais de desenvolvimento e implantação.
Invasão por criminoso por *phishing* antes que o projeto e seus efeitos desejados sejam alcançados.	Médio	Alto	Constante alerta, como é feito atualmente na organização, para mitigação, proteção e resposta a incidentes até que os frutos do projeto sejam alcançados.
Falha no design ou arquitetura baseada no modelo conceitual comportamental.	Baixo	Médio	Estudo detalhado durante a primeira sprint, a fase mais conceitual do trabalho para evitar a propagação de erros e falhas para as fases posteriores.

1.2.3 Backlog de Produto

Esta seção tem o objetivo de apresentar, de maneira bem detalhada, o backlog de requisitos idealizados para o desenvolvimento da solução. Aqui está sendo considerado o total de três sprints para a realização das atividades.

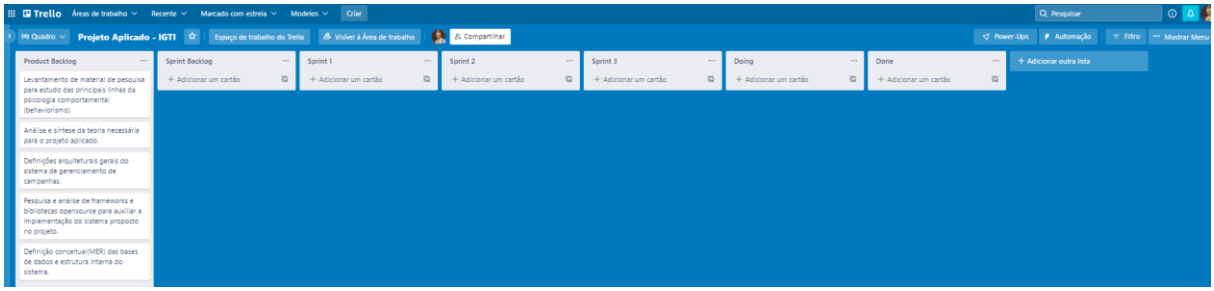
A fase inicial deste projeto tem como objetivo os ajustes necessários na primeira etapa após avaliação do orientador, como análise de contexto, matriz CSD, personas, apresentação da solução, benefícios e justificativas, hipóteses, premissas e restrições, Canvas de proposta e valor e todos os artefatos necessários para a entrega deste projeto.

A primeira sprint será a parte fundacional deste projeto. O estudo, análise e elaboração de um modelo baseado na psicologia comportamental para a elaboração do sistema de gerenciamento de campanhas de *phishing*. Pretende-se, além da elaboração deste modelo, a definição de bases de dados(modelo de entidade e relacionamento) necessárias para a construção do software, além do estudo de viabilidade para utilização de outros projetos *open source* para a construção do sistema.

A segunda sprint terá como objetivo uma parte mais técnica, do início da construção do sistema propriamente dito. Por meio de uma máquina virtual pretende-se criar as bases de dados no SGBD escolhido na primeira parte além do desenvolvimento do sistema com uma linguagem de programação que também será definida na primeira sprint.

Na terceira e última sprint será desenvolvido o restante do sistema além da parte final deste projeto, as considerações finais que consiste nos seguintes itens: resultados, contribuições e próximos passos.

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.