



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  
Jacomio

Guarulhos

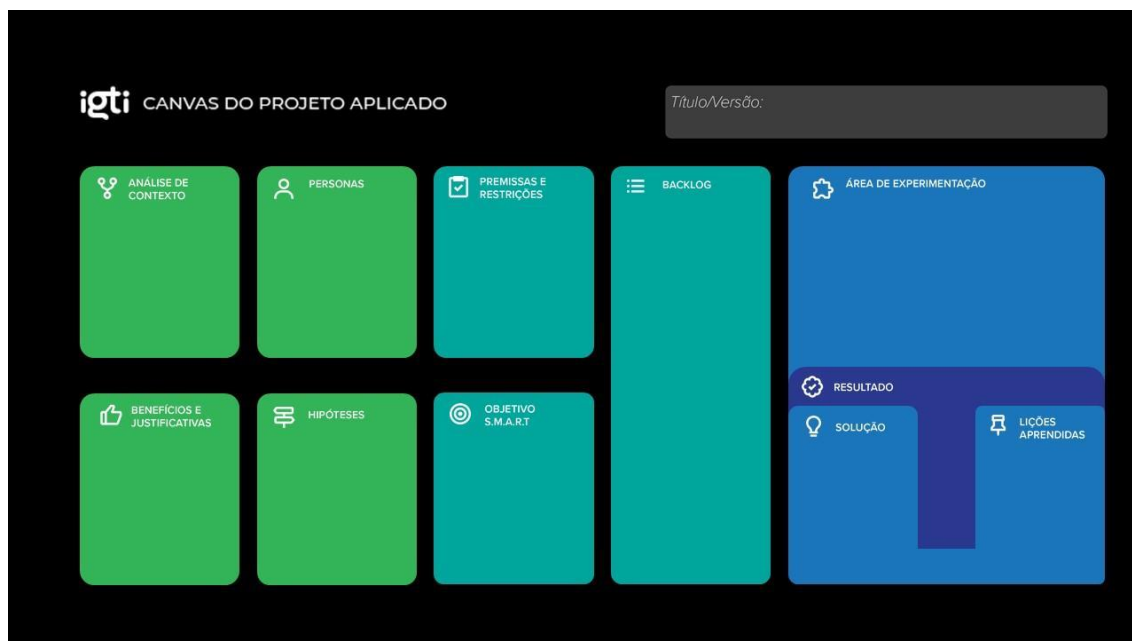
2022

# Sumário

1. CANVAS do Projeto Aplicado	4
1.1 Desafio	5
1.1.1 Análise de Contexto	5
1.1.2 Personas	9
1.1.3 Benefícios e Justificativas	12
1.1.4 Hipóteses	16
1.2 Solução	18
1.2.1 Objetivo SMART	18
1.2.2 Premissas e Restrições	19
1.2.3 Backlog de Produto	21
2. Área de Experimentação	23
2.1 Sprint 1	23
2.1.1 Solução	23
• Evidência do planejamento:	23
• Evidência da execução de cada requisito:	25
• Evidência dos resultados:	26
2.1.2 Experiências vivenciadas	31
2.2 Sprint 2	33
2.2.1 Solução	33
• Evidência do planejamento:	33
• Evidência da execução de cada requisito:	33
• Evidência dos resultados:	33
2.2.2 Experiências vivenciadas	33
2.3 Sprint 3	34
2.3.1 Solução	34
• Evidência do planejamento:	34
• Evidência da execução de cada requisito:	34
• Evidência dos resultados:	34
2.3.2 Experiências vivenciadas	34
3. Considerações Finais	35
3.1 Resultados	35
3.2 Contribuições	35
3.3 Próximos passos	35

## 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*<sup>1</sup>. 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 cyberspaço 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*<sup>2</sup> e os saltos qualitativos observados por Brooks<sup>3</sup>, 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<sup>4</sup> 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

---

<sup>1</sup> Termo que se refere a explosão demográfica entre os anos 1946 e 1964 nos EUA.

<sup>2</sup> 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.

<sup>3</sup> 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.

<sup>4</sup> 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 advento 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 colaboradores 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
<b>Atores</b>	Colaboradores estão expostos a ameaças providas de <i>phishing</i> a todo momento.	Realizar uma pesquisa teórica e empírica sobre a taxonomia dos diversos tipos de <i>phishing</i> pode ser viável.	Quais são as formas mais e menos comuns de ataques a empresas através de <i>phishing</i> ?
<b>Cenário</b>	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?
<b>Regra</b>	Definir um modelo conceitual behaviorista para que um sistema de campanhas de <i>phishing</i> 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

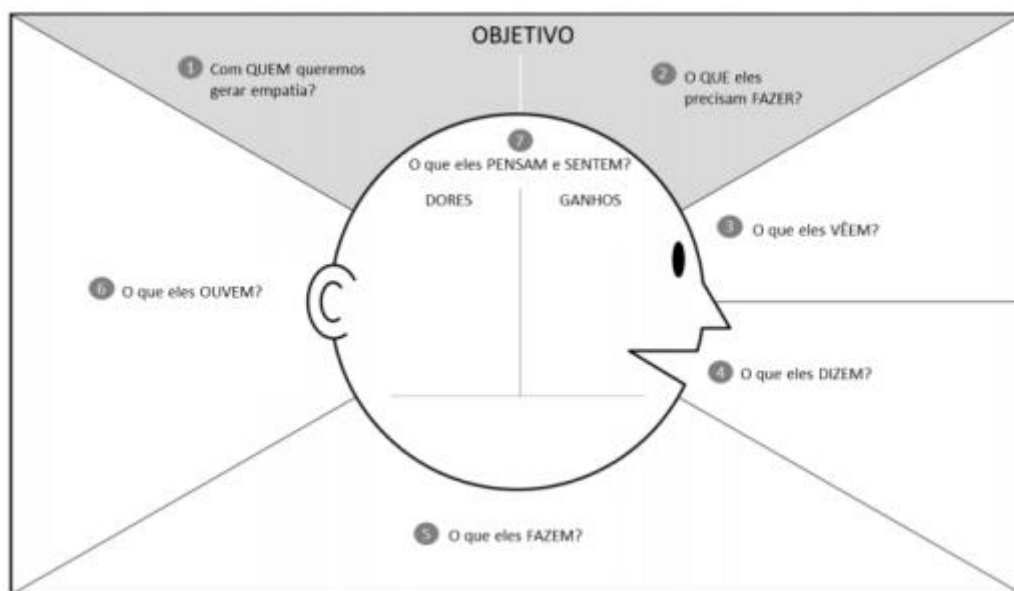
Para que o desafio deste projeto aplicado possa ser concluído, a utilização do POEMS (Pessoas, Objetos, Ambiente, Mensagem e Serviço), um *framework* que tem como objetivo principal orientar e estruturar toda a pesquisa deste trabalho acadêmico, também será utilizado, tornando mais fácil sintetizar as 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 mantêm 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 <i>phishing</i> 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 <i>phishing</i> , 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 <i>phishing</i> com uma base conceitual mais fundamentada, não dependendo apenas da experiência ou empirismo de colaboradores 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 <i>phishing</i> .			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 <i>phishing</i> 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 *phishing* “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 <i>phishing</i> 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





### 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 <i>phishing</i> .
Equipe de segurança da informação possui metodologias e ferramentas de segurança, mas ainda não possui o apoio necessário para lidar com ataques aos colaboradores 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 <i>phishing</i> .
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	
<b>C1</b>	Complexidade na execução do projeto
<b>C2</b>	Urgência na execução do projeto
<b>C3</b>	Investimento necessário a execução do projeto
<b>C4</b>	Benefícios esperados ao final do projeto
<b>C5</b>	Nível de satisfação da alta administração

Escala	Benefícios	Abrangência	Satisfação	Investimento	Clientes (impacto)	Operacional (dificuldade)
<b>5</b>	Valor imediato para o modelo de negócio	Total	Total	Nenhum	Muito fácil	Muito fácil
<b>4</b>	Significativo para o modelo de negócio	Grande	Grande	Baixo	Fácil	Fácil
<b>3</b>	Razoável para o modelo de negócio	Razoável	Razoável	Médio	Médio	Médio
<b>2</b>	Pouco para o modelo de negócio	Pequena	Pequena	Alto	Grande	Grande
<b>1</b>	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 análise 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.

<b>S</b> (Specific - Específico)	Tornar a organização mais segura e mitigar ameaças por meio de correio eletrônico.
<b>M</b> (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.
<b>A</b> (Attainable - Antecipável)	Realização de disparos de campanhas de <i>phishing</i> .
<b>R</b> (Relevant - Relevante)	Proteção dos ativos de T.I. e aumento da crença de garantia de continuidade dos negócios da organização.
<b>T</b> (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 <i>phishing</i> 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.

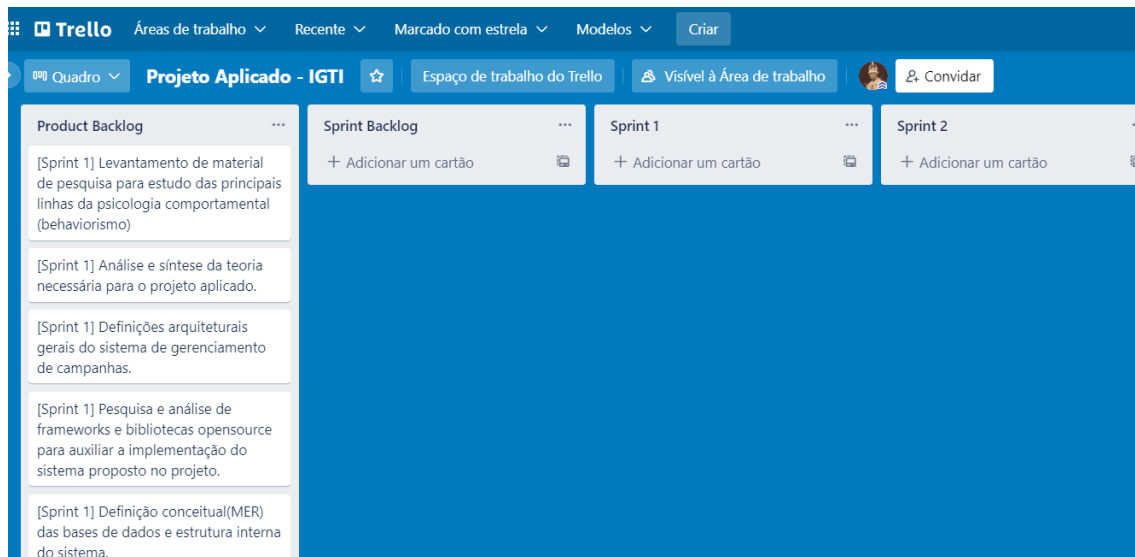
A fase inicial deste projeto tem como objetivo os ajustes necessários na primeira etapa após avaliação do orientador, como análise de contexto, matriz CSD, personas, apresentação da solução, benefícios e justificativas, hipóteses, premissas e restrições, Canvas de proposta e valor e todos os artefatos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



The screenshot shows a Trello workspace for 'Projeto Aplicado - IGTI'. The board is organized into four columns: Product Backlog, Sprint Backlog, Sprint 1, and Sprint 2. The Product Backlog column contains five cards detailing tasks for Sprint 1, such as research, theory analysis, architectural definitions, and database conceptualization. The Sprint Backlog, Sprint 1, and Sprint 2 columns are currently empty, each with a button to add a card.

**Trello Board: Projeto Aplicado - IGTI**

**Product Backlog**

- [Sprint 1] Levantamento de material de pesquisa para estudo das principais linhas da psicologia comportamental (behaviorismo)
- [Sprint 1] Análise e síntese da teoria necessária para o projeto aplicado.
- [Sprint 1] Definições arquiteturais gerais do sistema de gerenciamento de campanhas.
- [Sprint 1] Pesquisa e análise de frameworks e bibliotecas opensource para auxiliar a implementação do sistema proposto no projeto.
- [Sprint 1] Definição conceitual(MER) das bases de dados e estrutura interna do sistema.

**Sprint Backlog**

+ Adicionar um cartão

**Sprint 1**

+ Adicionar um cartão

**Sprint 2**

+ Adicionar um cartão

## 2. Área de Experimentação

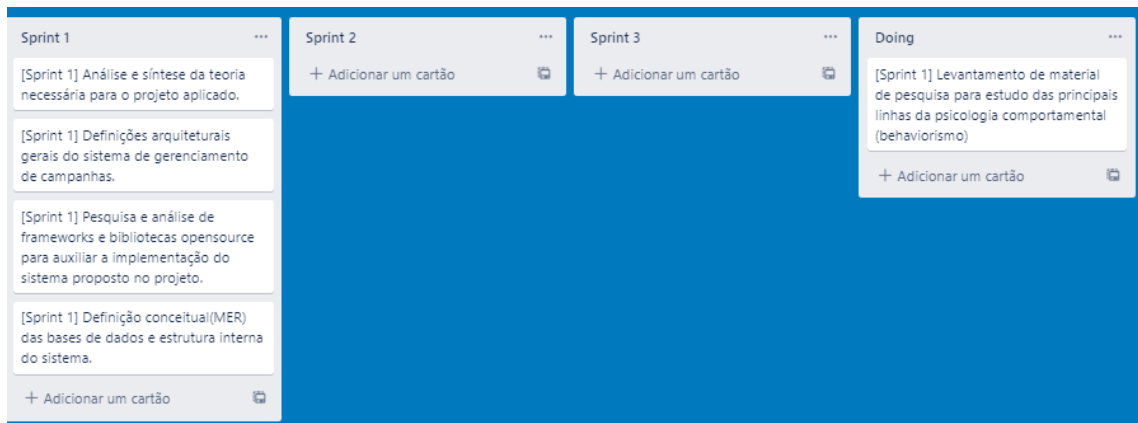
Esta seção tem o objetivo de apresentar as evidências do planejamento dos requisitos selecionados do Backlog de Produto, além de mostrar a maneira como eles foram desenvolvidos e registrar os resultados alcançados.

### 2.1 Sprint 1

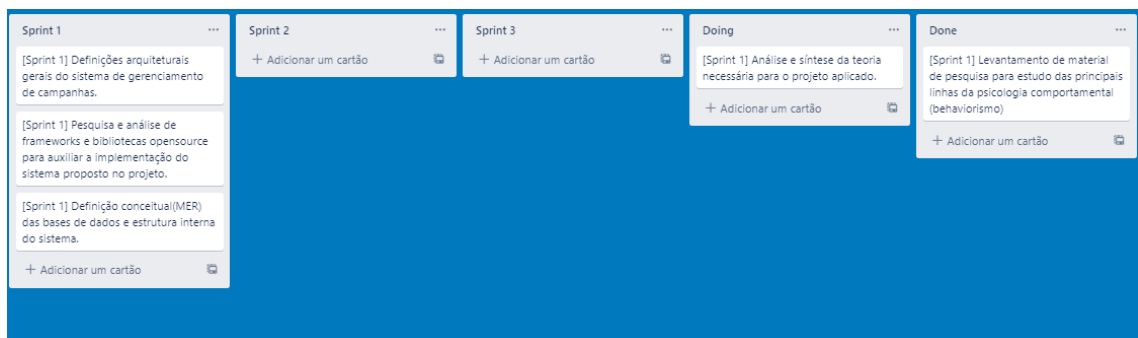
#### 2.1.1 Solução

- Evidência do planejamento:

Para o item 1 da primeira sprint, a saber, “Levantamento de material de pesquisa para estudo das principais linhas da psicologia comportamental(behaviorismo), o planejamento via *Trello* encontra-se abaixo:

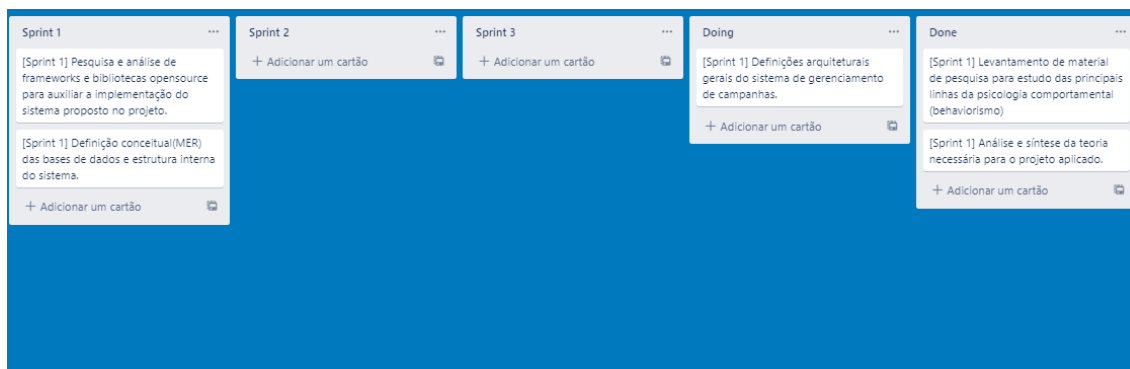


Para o item 2 da primeira sprint, a saber, “Análise e síntese da teoria necessária para o projeto aplicado”, o planejamento via *Trello* encontra-se abaixo:

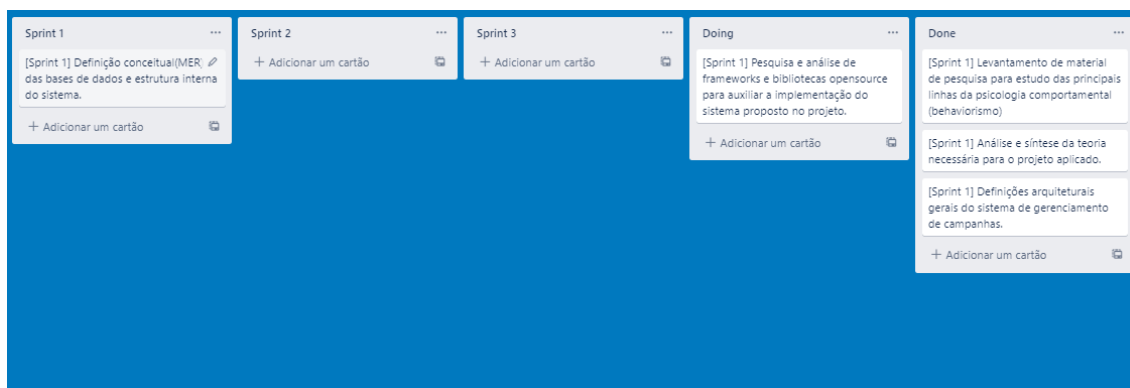




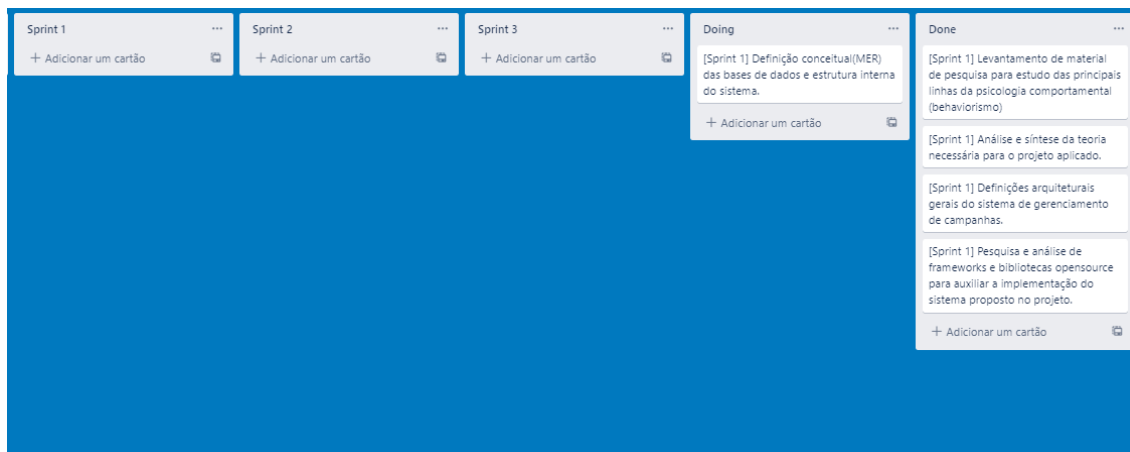
Para o item 3 da primeira sprint, a saber, “Definições arquiteturais gerais do sistema de gerenciamento de campanhas”, o planejamento via *Trello* encontra-se abaixo:



Para o item 4 da primeira sprint, a saber, “Pesquisa e análise de frameworks e bibliotecas *opensource* para auxiliar a implementação do sistema proposto no projeto”, o planejamento via *Trello* encontra-se abaixo:



Para o item 5 da primeira sprint, a saber, “Pesquisa e análise de frameworks e bibliotecas *opensource* para auxiliar a implementação do sistema proposto no projeto”, o planejamento via *Trello* encontra-se abaixo:



Para que os itens possam ser facilmente correlatos nas seções posteriores, eles serão identificados de acordo com a tabela que segue abaixo:

Código	Descrição
A (Item 1)	Levantamento de material de pesquisa para estudo das principais linhas da psicologia comportamental (behaviorismo).
B (Item 2)	Análise e síntese da teoria necessária para o projeto aplicado.
C (Item 3)	Definições arquiteturais gerais do sistema de gerenciamento de campanhas.
D (Item 4)	Pesquisa e análise de frameworks e bibliotecas open source para auxiliar a implementação do sistema proposto no projeto.
E (Item 5)	Definição conceitual (MER) das bases de dados e estrutura interna do sistema.

- Evidência da execução de cada requisito:

#### A (Item 1)

Para o item inicial desta lista, aquele que será a base fundadora e funcional para o sistema de gerenciamento de *phishing* com base na psicologia behaviorista, adotou-se a metodologia de revisão bibliográfica para aquisição de conhecimento mais profundo sobre a psicologia comportamental.

Desse modo, para dar estrutura a esse estudo, adotou-se a seguinte estratégia para obter o conhecimento fundamental necessário para o projeto: levantamento e aquisição de bibliografias sobre história da psicologia e sobre história da psicologia comportamental, levantamento e aquisição de obras mais especializadas sobre os dois maiores expoentes dessa linha de estudo, Watson e Skinner, além da leitura de outros artigos encontrados na internet.

Em suma, as obras utilizadas para estudo do tema proposto serão listadas abaixo utilizando a ordenação alfabética autoral:

#### LIVROS AQUI

Além desse levantamento inicial, durante a aula inaugural da disciplina, tivemos a oportunidade de apresentar as ideias para o professor orientador e receber feedback instantâneo para que o projeto pudesse ser realizado da melhor forma possível. Assim sendo, após a apresentação da ideia deste projeto, o professor Maximiliano citou um outro grande psicólogo que ajudaria na pesquisa teórica sobre o tema, Abraham Maslow, que criou uma teoria da necessidade humana que vai em encontro às teorias behavioristas mais consolidadas na academia. Desse modo,

utilizamos também o conhecimento proposto por Maslow para ajudar a esclarecer e entender melhor o comportamento humano com o objetivo de propor um melhor sistema de gerenciamento de phishing behaviorista. As obras estudadas para entender um pouco melhor a teoria de Maslow estão listadas abaixo:

#### LIVROS AQUI

#### B (Item 2)

O objetivo deste item, “Análise e síntese da teoria necessária para o projeto aplicado” é o de consolidar a base teórica fundamental para formular a política de *phishing* e também para arquitetar a estrutura interna do sistema de gerenciamento proposto. Este item, junto com o primeiro (A - Item 1: levantamento de materiais de pesquisa), terão seus resultados apresentados de forma detalhada na próxima seção (Evidência dos resultados).

#### C (Item 3)

#### D (Item 4)

#### E (Item 5)

- Evidência dos resultados:

Como resultado desta primeira iteração do projeto, os resultados serão evidenciados da seguinte maneira nesta seção: Os itens A e B terão como resultado a metodologia consolidada em forma de texto, o item C será evidenciado através de dois diagramas, o de componentes e o de implantação, o item D xpto, e o item E terá como output final o diagrama de entidade relacional que será utilizado na próxima iteração (sprint 2) para o desenvolvimento do sistema em si.

#### Itens 1 e 2(A e B)

Conforme explicado no parágrafo introdutório, apresentar-se-á em uma única seção os resultados obtidos na realização dos itens A e B da sprint 1. Para que o texto fique organizado, este será dividido em três pontos, o primeiro será uma breve apresentação da teoria por trás do projeto, o segundo será a apresentação de uma política estruturada com base na teoria apresentada anteriormente e, por fim, a teoria aplicada a proposta do sistema de gerenciamento de phishing.

#### Behaviorismo: de Watson à Skinner

A teoria adotada neste projeto nasceu no século XIX, período em que a psicologia se consolidava como ciência e muitos de seus representantes procuravam

retirar as amarras metafísicas e adotavam com cada vez mais vigor o método científico já consolidado em outras ciências da natureza.

Dito isso, o behaviorismo, anglicismo para a palavra original na língua inglesa *behaviorism*, i.e., comportamentalismo, é a linha psicológica que tem como objetivo o estudo do comportamento. Diferente de outras doutrinas e linhas de pesquisa com bastante carga subjetiva, a linha de estudos iniciada por John B. Watson acredita que a psicologia humana pode ser estudada objetivamente por meio da observação das ações dos espécimes humanos, observando o comportamento.

John Broadus Watson, iniciador deste movimento em 1913 com o seu artigo *Psychology as the Behaviorist Views it*<sup>5</sup>, utiliza as teorias de Vladimir Mikhailovich Bechtereve e Ivan Petrovich Pavlov (estudos sobre o mecanismo de condicionamento animal) para propor a universalização desta teoria ao gênero humano, criando assim seu principal conceito, o de condicionamento reflexo. Watson explica que o mecanismo de estímulo e resposta, como mostrar um fragmento de carne a um cachorro(estímulo) e observar a salivação(resposta), poderia sofrer engenharia ao acrescentar um novo estímulo neutro associado ao estímulo original. Dessa forma, ao mostrar uma pequena porção de carne a um cachorro e ao mesmo tempo acrescentar um novo estímulo, como o tocar de uma campainha, o estímulo original expande seus efeitos ao novo estímulo condicionado. Dessa forma, após algum tempo de treino e repetição, o estímulo da campainha por si só traria o efeito da salivação ao cão sem que o cheiro ou a visão da fração de carne fossem apresentados. Evidentemente, os humanos também estão sujeitos a esse tipo de mecanismo e alteração/expansão de estímulos para se chegar num mesmo efeito. Essa teoria, hoje chamada de behaviorismo clássico, tem algumas limitações como considerar fundamentalmente estímulos organolépticos e ainda ter uma base metafísica, como considerar que os seres vivos nascem com determinados reflexos, i.e., uma espécie de inatismo. No entanto, em 1945, um outro pensador deu mais base a essa teoria e é a que utilizaremos como base no projeto.

No primeiro dos três grandes artigos escritos por Burrhus Frederic Skinner<sup>6</sup>, intitulado *The Operational Analysis of Psychological Terms*, o autor inicia uma nova interpretação do behaviorismo. Na teoria tradicional, o estudo do comportamento dos seres vivos era resumido ao comportamento e reflexo, como vimos anteriormente. O mecanismo clássico pode ser traduzido nas seguintes fórmulas:

I - Estrutura pré-existente na psique animal e humana

**Estímulo incondicionado => resposta incondicionada**

II - Adição do elemento neutro em conjunto com o estímulo incondicionado

<sup>5</sup> Artigo publicado na revista *Psychological Review*. Pode ser lido atrav[es deste link? <https://www.ufrgs.br/psicoeduc/chasqueweb/edu01011/behaviorist-watson.pdf>

<sup>6</sup> Os artigos que xpto são: ABC, 123, OIA

**Estímulo incondicionado + estímulo neutro => resposta incondicionada**

III - Transformação do estímulo neutro em estímulo condicionado substituindo o incondicionado

**Estímulo condicionado => resposta incondicionada**

Na nova interpretação, Skinner nos traz o conceito de condicionamento operante que traz, além dos elementos “inatos” do behaviorismo clássico, os pensamentos e emoções. Os comportamentos que podemos observar não são somente estimulados por forças biológicas/genéticas. O comportamento em si possui um mecanismo de reforço para que possa se repetir e isso acontece devido às consequências deste.

Todo indivíduo busca sobreviver, se autorrealizar e outras ações que cada qual sente necessidade. Então, à medida que determinado comportamento ajude o indivíduo a suprir sua necessidade, este entrará numa espécie de coleção comportamental de onde será consultado e reutilizado na mesma ou numa necessidade semelhante. No vocabulário de Skinner, o mecanismo de repetição é o operante. Além disso, diferente do caráter determinístico defendido por Watson, os comportamentos para Skinner seguem um padrão probabilístico. A depender do reforço positivo (sucesso no alcance do objetivo) ou negativo (punição por determinado comportamento), a probabilidade de o comportamento voltar a acontecer é alterada; se seguir pelo reforço positivo a probabilidade aumenta, caso siga pelo reforço negativo, diminui. Isso não significa que o comportamento será recorrente ou extinto necessariamente.

Para formalizar o mecanismo skinneriano do behaviorismo radical, apresenta-se a seguinte fórmula:

**(I)  $S(d/\delta)$  - (II) R -> (III) C**

(I) S: Estímulo. Pode ser um estímulo do tipo  $d$  (discriminativo) ou do tipo  $\delta$  (delta). O primeiro se refere a um estímulo, que na sua presença aumenta a probabilidade de o comportamento ocorrer. O segundo se refere a um estímulo que na sua presença infere que o estímulo consequente reforçador não estará presente.

(II) Resposta ou forma. É a reação a determinado estímulo. Na passagem do estímulo para a resposta podemos observar que se utiliza o traço (-) ao invés da flecha (->), justamente para indicar que esta transição é probabilística, não determinística.

(III) Consequência que pode vir na forma de reforço positivo ou negativo.

Por fim, para finalizar a contribuição de Skinner na parte conceitual deste projeto, uma outra categorização importante para o sistema será apresentada, as classes de estímulos. Anteriormente, na primeira fase do behaviorismo, considerava-se apenas uma classe, a proximidade física, também chamada de generalização (como

a porção de carne sendo aproximada do cão para causar a salivação). Mas, após o avanço desta ciência, construiu-se uma nova categoria, conhecida como funcional.

Esta segunda categoria é um pouco mais complexa e abarca todos os níveis da vida. Ela é dividida em três itens. O primeiro deles é a filogênese, que abarca as características genéticas que são transmitidas de geração em geração, os chamados comportamentos padrões ou genéticos, como o medo “inato” herdado através das mais diferentes fobias. Entre outros, alguns destes são exemplos dessa subcategoria: início da vida, aptidão e sucesso reprodutivo, reflexos condicionados inatos, aptidão. O segundo item é a ontogênese, que são aprendizados individuais do organismo com seu meio. É a seleção comportamental por consequência, é o condicionamento operante skinneriano por definição; um comportamento que teve sucesso tende a ser selecionado ou reforçado e tem maior probabilidade de ocorrer numa circunstância similar, i.e., a lei do feito. O último item é a cultura, presente apenas no gênero humano. Esta subcategoria se traduz naquilo que traz benefícios para o grupo e contribui para solução de problemas coletivos, o mais profundo e complexo item da categoria funcional.

Por fim, para citar Abraham Harold Maslow, autor citado pelo orientador deste projeto, utilizamos sua famosa hierarquia de necessidades para ajudar no entendimento dos estímulos que poderiam gerar determinados comportamentos nos seres humanos. Este conhecimento está traduzido de forma didática na conhecida pirâmide de Maslow, que busca dar forma a esta hierarquia de necessidades humanas. Com cinco níveis, esta figura geométrica busca dar profundidade e hierarquizar as necessidades. Para que uma necessidade seja despertada, a necessidade anterior necessita ser satisfeita. Iniciando da base da pirâmide, temos as necessidades fisiológicas, que são constituídas da respiração, comida, água, sexo, sono e excreção. O próximo nível é o da segurança, composta por segurança corporal, do ofício, dos recursos, da moralidade, família, saúde e propriedade. Logo acima, encontramos o nível do relacionamento, que contém a amizade, família e intimidade sexual. O penúltimo nível da pirâmide guarda a estima, que é formada pela autoestima, confiança, conquista, respeito aos outros e dos outros. Por fim, no topo da pirâmide está a realização pessoal, onde podemos encontrar a moralidade, criatividade, espontaneidade, solução de problemas, ausência de preconceitos e aceitação dos fatos.

Para realizar uma síntese de Maslow com Skinner, observamos que a hierarquia de necessidades do primeiro se relacionam diretamente com a categoria de comportamentos funcionais do segundo. A subcategoria filogenética está para a base da pirâmide como a última categoria cultural está para o topo do poliedro. As três categorias no meio da figura geométrica se relacionam com a categoria ontogenética. Desse modo, a estruturação da política e, por consequência o modelo de entidade relacional podem ser melhor estruturados para guardar as informações necessárias para a proposta deste projeto.

## Política de campanhas baseada no comportamentalismo

A política de campanhas pensada para os analistas de segurança e funcionais que elaboram os testes e educação dos colaboradores da organização é, em seu primeiro modelo, simples, mas dá estrutura ao caos que encontramos nas organizações contemporâneas que muitas vezes realizam testes ineficazes e não promovem a conscientização necessária de seus funcionários, objetivo final das campanhas para que dados e sistemas não sejam comprometidos por meio de engenharia social.

De início, propõe-se a criação de um calendário segmentado para a realização das diversas campanhas que devem ocorrer com regularidade ao longo do ano fiscal. O tempo é sem dúvida algo intrínseco à espécie humana; desde a regulação do funcionamento interna do corpo até as convenções sociais e culturais como horário do almoço ou jantar, chá ou período despendido no trabalho. Utilizar-se deste recurso, da regularidade, traz ordem ao caos algumas vezes chamado de aleatoriedade ou testes surpresa. A fim de dar essa estrutura, propõe-se a divisão por *quarter* do ano fiscal ou qualquer outra divisão que segmente o ano em 4 partes. Cada uma destas partes será composta por um nível de regularidade de campanhas. Por exemplo, o primeiro trimestre terá nível 1 de campanhas, i.e., *phishings* serão enviados a cada duas semanas. O segundo trimestre terá nível 2, i.e., *phishings* serão enviados a cada 1,5 semanas inclusive aos finais de semana. E assim por diante, até o último semestre, o mais severo de todos de acordo com esta lógica. Evidentemente, outras variáveis devem ser acrescentadas nesse sistema de divisão do tempo, como o tipo de categoria que será explorado para verificar a recorrência de pessoas que clicam nos links dos testes.

A seguir, propõe-se a estruturação dos *phishings* por categorias. No entanto, antes de seguir com a proposta, faz-se necessário realizar a analogia ou junção da teoria vista no tópico anterior com a proposta desta política. O mecanismo de phishing é bem semelhante à estrutura estudada pelos psicólogos comportamentais. Assim como elucidamos a fórmula para formalização de Skinner,

$$S(d/\delta) - R \rightarrow C$$

podemos facilmente substituir as variáveis por

**E-mail malicioso - clique em link -> dano**

afinal, os criminosos responsáveis por este tipo de ataque não estão apenas técnicos altamente especializados na engenharia de malwares, vírus ou outros artefatos capazes de causar danos à organização ou seus membros, estas pessoas conhecem a natureza humana, ao menos num nível básico, e utilizam esse tipo de vulnerabilidade para obter acesso a dados confidenciais e prejudicar seus alvos. Dito isso, prosseguindo com a proposta da divisão dos testes por categorias, Skinner e Maslow podem ajudar



os analistas responsáveis pela elaboração dos testes no seguinte sentido. Para que os funcionários da organização possam ser conscientizados de maneira mais completa, a maior gama possível de simulações deve ser aplicada. Assim sendo, a categorização proposta é a seguinte:

Categoria 1: Classe funcional filogenética

De acordo com o que foi visto na teoria behaviorista e na

Categoria 2: Classe funcional ontogenética

Categoria 3: Classe funcional cultural

CONCLUSAO - FUNCAO PEDAGOGICA

**Política de campanhas comportamentalista e gênese do sistema de gerenciamento**

A política proposta no tópico anterior também xpto123

Item 3 - C

Xpto abc

Item 4 - D

Xpto abc

Item 5 - E

Xpto abc

### 2.1.2 Experiências vivenciadas

Após reuniões realizadas junto a Alta Administração e a equipe de TI, apurou-se que as necessidades em relação à proteção do servidor WWW, giram em torno dos principais pilares que sustentam a segurança da informação, que são: disponibilidade, integridade e confidencialidade. Este fato, torna-se maduro a partir dos conceitos apresentados na disciplina fundamento em segurança que apontam a importância em relação a garantia dos pilares que sustentam a segurança da informação junto a ativos e recursos de TI utilizados pelas organizações em modo geral. Outro fator que chamou a atenção foi a possibilidade de melhoria dos mecanismos de proteção aos ativos de TI, por meio da adoção das boas práticas apresentadas nas normas ISO 27001, 27002 e NIST que buscam colocar em conformidade todos os aspectos relacionados à segurança da informação. Quanto a escolha do modelo do teste a ser realizado, bem como as ferramentas a serem utilizadas durante toda a execução do teste de intrusão a disciplina Ethical Hacker apresentou os conceitos necessários que foram importantes para o melhor entendimento das diferenças entre os modelos existentes que podem ser utilizados em um teste de intrusão, incluindo as fases necessárias a serem cumpridas durante a



execução do teste e o sistema operacional Kali Linux como uma solução completa para realizar todas as fases de um teste de intrusão e fornecer as informações necessárias à resolução do desafio/problema apresentado pela alta administração da Organização Tabajara. Durante o processo de reconhecimento do alvo, detectamos que ele possui várias informações que poderão servir de subsídios para realizar uma análise de possíveis vulnerabilidades que possam posteriormente ser exploradas para ganho de acesso. Abaixo print contendo a informação do sistema contido no servidor WWW

## 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.