UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS CASTANHAL
FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

LUCAS GABRIEL MIRANDA RIBEIRO

PROJETO DE UMA FERRAMENTAS BASEADA EM CRIPTOGRAFIA VISUAL PARA COMBATER ATAQUES DE PHISHING

Castanhal – PA
2021

LUCAS GABRIEL MIRANDA RIBEIRO

PROJETO DE UMA FERRAMENTAS BASEADA EM CRIPTOGRAFIA VISUAL PARA COMBATER ATAQUES DE PHISHING

Trabalho de Conclusão de Curso apresentado à Universidade Federal do Pará - Campus Castanhal, como requisito parcial para obtenção do Grau de Bacharel em Sistemas de Informação.

Orientador: Profº. Drº. Roberto Samarone dos Santos Araújo
Coorientador: Profº. Drº. Tássio Costa de Carvalho

Castanhal – PA
2021

LUCAS GABRIEL MIRANDA RIBEIRO

PROJETO DE UMA FERRAMENTAS BASEADA EM CRIPTOGRAFIA VISUAL PARA COMBATER ATAQUES DE PHISHING

Trabalho de Conclusão de Curso apresentado à Universidade Federal do Pará - Campus Castanhal, como requisito parcial para obtenção do Grau de Bacharel em Sistemas de Informação.

Aprovado em: ___/___/_____

BANCA EXAMINADORA:

_____

Profº. Drº. Roberto Samarone dos Santos Araújo - Orientador
Universidade Federal do Pará – Campus Belém (ICEN)

_____

Profº. Drº. Tássio Costa de Carvalho – Coorientador
Universidade Federal do Pará – Campus Castanhal (FACOMP)

_____

Profº. Drº. José Jailton Henrique Ferreira Junior – Examinador
Universidade Federal do Pará – Campus Castanhal (FACOMP)

Castanhal – PA
2021

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter dado forças para a conclusão deste trabalho, agradeço também a minha mãe por sempre ter esforçado para ver o meu melhor e por ser meu alicerce e motivo pra eu querer melhorar cada vez mais.

Aos meus amigos Adirley Gaia, Luciano Teran, Raonner Bruno e Tobias Sanos por sempre estarem presentes e dispostos a ajudar em todos os momentos e pelas noites em claro estudando para provas e seminários e também ao Joab Mateus pela parceria de sempre.

Também não posso deixar de agradecer ao meu orientador Professor Roberto Samarone, pela paciência e dedicação a este trabalho, sem ele nada disso seria possível.

RESUMO

Crimes praticados através dos meios digitais tem se tornado cada vez mais frequentes, ao decorrer do tempo criminosos tem desenvolvido diversas técnicas com o objetivo de contornar as soluções implementadas por empresas e usuários comuns para obterem algum tipo de benefício. Um ataque que tem sido amplamente utilizado é o chamado Phishing, onde o atacante tem por objetivo ludibriar uma vítima fazendo-a fornecer dados sensíveis geralmente através de páginas web falsas que normalmente são cópias de um serviço legítimo. Este trabalho propõe um projeto de ferramenta usando a criptografia visual para combater este tipo de crime, onde ao longo desta pesquisa serão apresentadas as principais técnicas e ferramentas utilizadas por estes atacantes, conceitos relacionados a criptografia visual e por fim os aspectos relativos ao funcionamento do projeto que visa mitigar estes ataques.

Palavras Chaves: Phishing, Criptografia Visual, Engenharia Social.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

APWG - Anti-Phishing Working Group

ASCII - American Standard Code for Information Interchange

CAPTCHA - Completely Automated Public Turing Test To Tell Computers And Humans Apart

CERT.BR - Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil

CPF - Cadastro de Pessoa Física

DES - Data Encryption Standard

DNS - Domain Name System

ES - Engenharia Social

ID - Identity

IEC - International Electrotechnical Commission

IP - Internet Protocol

ISO - International Organization of Standardization

NTDIC - Novas Tecnologias Digitais Da Informação E Comunicação

OSINT - Open Source Intelligence

OTP - One-Time Password

PIL - Python Imaging Library

QR - Quick Response

RGB - Red, Green, Blue

RSA - Rivest-Shamir-Adleman

SaaS - Software as a service

SMS - Short Message Service

SMTP - Simple Mail Transfer Protocol

URL - Uniform Resource Locator

VOIP - Voice Over Internet Protocol

SUMÁRIO

CAPÍTULO I

INTRODUÇÃO

1.1. MOTIVAÇÃO E JUSTIFICATIVA

Diante a consolidação da Internet e todas as facilidades e vantagens que esta trouxe, diversas instituições, tais como: lojas e bancos, observaram a oportunidade de migrarem seus serviços objetivando o crescimento do negócio, automatização de serviços e maior lucro. No entanto, assim como nos meios físicos, o mundo digital também pode apresentar sérios problemas principalmente quando se trata da segurança.

Percebendo a grande quantidade de empresas que passaram a operar também no meio digital criminosos passaram a desenvolver as mais diversas técnicas a fim de obter retornos financeiros e prejudicar empresas, as técnicas incluem criação de aplicativos maliciosos, golpes que utilizam nomes de empresas conhecidas, desenvolvimento de páginas falsas para roubo de dados e muitas outras. Na grande maioria dos casos o propósito é o mesmo: roubo de dados do usuário.

De acordo com o relatório da NORTON (2019) 117,6 milhões de pessoas em 16 países foram vítimas de roubo de dados, dentre essas 10.1 milhões somente no Brasil, o que pode ser agravado pelo aumento no uso de dispositivos portáteis no Brasil que segundo MEIRELLES (2020) chegam a 342 milhões, ou seja, 1,6 dispositivo portátil por habitante.

Dados publicados pelo relatório da KASPERSKY (2019) apontam que 35% dos brasileiros não sabem como proteger sua privacidade online, abrindo uma porta de entrada para que criminosos digitais obtenham sucesso e motivação para continuar com roubos e extorsões.

Em vista disso, crescem também os crimes digitais do tipo *phishing,* segundo a *KASPERSKY* (2014), o phishing é um ataque caracterizado por tentar ludibriar o usuário a inserir dados pessoais dentro de um site fraudulento. Segundo a empresa, o Brasil é líder mundial em ataques desse tipo, sendo que no ano de 2017 28,30% dos internautas brasileiros já tinham sido afetados no por esse tipo de ataque.

Segundo DHILLON e BACKHOUS (2000), as organizações precisam desenvolver ações de estrutura para evitar atitudes fraudulentas que são danosas e

destoam as informações que são providas aos seus usuários. E, ao analisar os dados apresentados, é indubitável a necessidade de implementar novas tecnologias digitais da informação e comunicação (NTDICs) que proporcionem segurança e integridade dos dados de pessoas físicas e jurídicas, para que permaneçam protegidos e intactos.

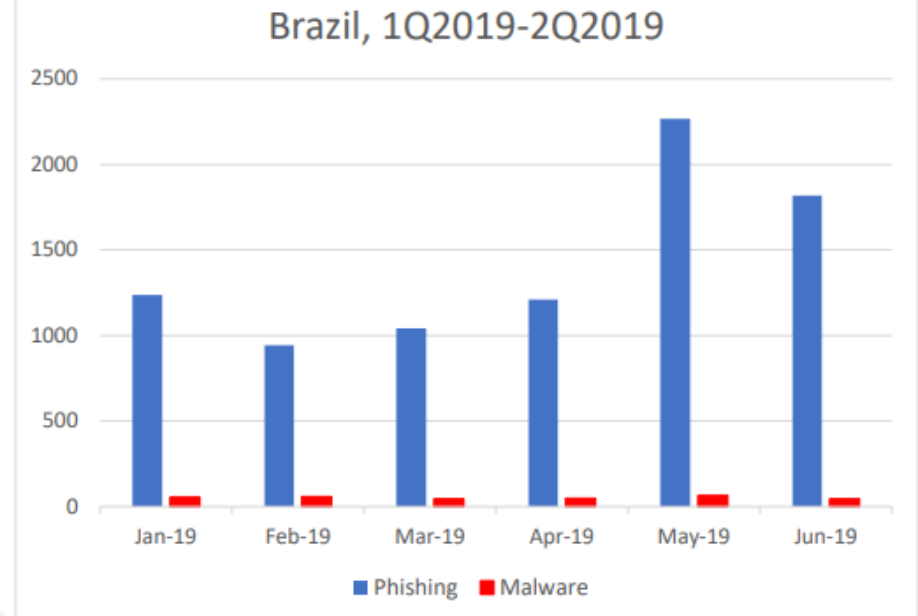
A segurança das aplicações utilizadas cotidianamente, tais como sistemas bancários, redes sociais, sistemas internos usados por empresas, tem sido o foco de muitas pesquisas. Em busca da melhora destas, diversos pesquisadores têm desenvolvido técnicas e ferramentas que auxiliam tanto usuários comuns quanto empresas a se prevenirem das ameaças que essas aplicações enfrentam.

Contudo, de acordo com SERAFIM *et al.* (2017) a disponibilidade de novas ferramentas e técnicas na área ainda não são suficientes diante do crescimento exponencial dessas aplicações e o conhecimento técnico por si só dos profissionais não faz com que uma empresa esteja segura contra ataques cibernéticos.

Dentre as principais ameaças, uma categoria de ataque que tem sido largamente utilizado é o phishing, nos quais criminosos roubam e usufruem de dados sensíveis de suas vítimas. Segundo ASSOLINI (2018) *apud* COSSETTI (2018) o Brasil é campeão em ataques de *phishing*, em nível global. Há dois ou três anos o Brasil lidera o ranking, o especialista aponta que a grande maioria dos ataques de *phishing* no Brasil são feitos por brasileiros, sem que haja intervenção de criminosos de outros países o que faz com que o Brasil se mantenha na liderança local e global ficando na frente de países como Rússia e China.

De acordo com dados da Axur empresa localizada no Brasil membro do Anti-Phishing Working Group (APWG), no segundo trimestre de 2019 foram detectados 5.297 casos de phishing, um aumento de 64% em relação aos 3.220 que foram observados no primeiro trimestre, os maiores alvos desses ataques, como mostra a Figura 1.

Figura 1. Relatório dos ataques de phishing nos dois primeiros trimestres de 2019



Fonte. *APWG, Phishing Activity Trends Reports, (2019*)

A empresa também analisou sobre quais serviços foram mais afetados por *phishing*. No primeiro trimestre de 2019 o setor de SaaS (*Software as a service*) e *Webmail* foram os mais atacados no Brasil, contudo no segundo trimestre casos de *phishing* direcionados ao comércio eletrônico, bancos e instituições financeiras foram os mais frequentes, como é possível observar na figura 2.

Figura 2. Relatório dos ataques de phishing por tipo de serviço nos dois primeiros trimestres de 2019

Fonte. *APWG, Phishing Activity Trends Reports, (2019*)

Dados publicado pela NORTON (2017), demonstram que o Brasil foi considerado o segundo país com maior prejuízo devido a ataques cibernéticos, incluindo o *phishing*, estima-se que o rombo financeiro alcançou em torno de US$ 22 bilhões, abrangendo usuários e empresas.

Dada a gravidade deste cenário, este trabalho visa combater uma técnica amplamente usada por criminosos chamada de *phishing* na qual um criminoso induz a vítima a inserir informações confidenciais em páginas fraudulentas, que na grande maioria das vezes são réplicas de páginas originais. Para a mitigação deste ataque será apresentada uma proposta que utiliza a técnica de criptografia visual somada ao uso da câmera dos dispositivos utilizados por usuários.

1.2 OBJETIVOS

Os objetivos do presente trabalho são listados a seguir:

1.2.1 OBJETIVO GERAL

Percebendo um dos grandes problemas da segurança da informação conhecido como *phishing* que usa o elo mais fraco da segurança, o fator humano, este trabalho visa propor um conceito para identificar e mitigar ataques de *phishing* através do uso da técnica de criptografia visual. Para isso, o trabalho tem como base as ideias de PIETZ (2014).

1.2.2 OBJETIVOS ESPECÍFICOS

- Estudar alguns dos principais de mecanismos de identificação de phishing;
- Estudar técnicas de criptografia visual;
- Projetar uma ferramenta baseada em Criptografia Visual como solução no Combate a Ataques de Phishing.

1.3 ESTRUTURA DO TRABALHO

Este TCC é dividido em 5 Capítulos. No qual cada capítulo aborda os seguintes conteúdos:

- **CAPÍTULO 2:** Este capítulo apresenta quatro trabalhos correlatos à proposta apresentada.
- **CAPÍTULO 3:** Este capítulo aborda os conceitos relativos à engenharia social e phishing que serviram como base para este trabalho. Além disso, ele apresenta as principais técnicas usadas por atacantes, também é abordada a técnica de Criptografia Visual, apresentando aspectos relativos ao funcionamento deste método
- **CAPÍTULO 4:** Este capítulo apresenta a proposta de solução, demonstrando o funcionamento e detalhando as técnicas e ferramentas.
- **CAPÍTULO 5:** Este capítulo apresenta as considerações finais e os trabalhos futuros.

CAPÍTULO 2

TRABALHOS CORRELATOS

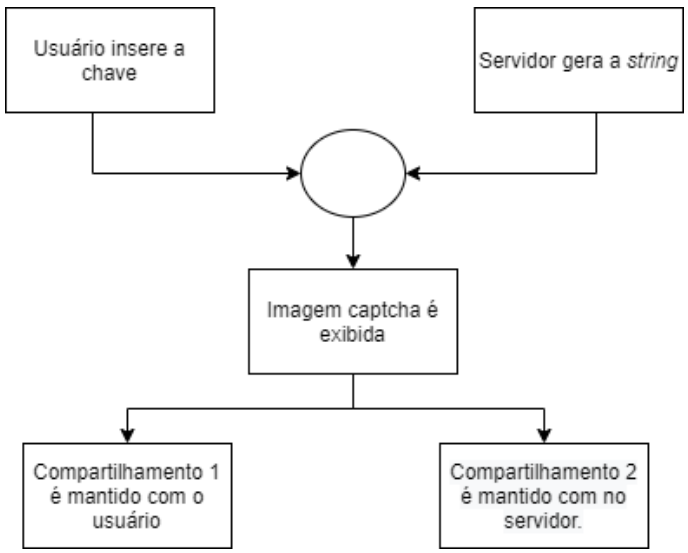
Nesta seção serão apresentados quatro trabalhos correlatos à proposta apresentada, onde serão analisados o funcionamento da proposta, as técnicas utilizadas e os objetivos.

2.1 JAMES E PHILIP

Na proposta “A Novel Anti Phishing Framework Based On Visual Cryptography” JAMES E PHILIP (2012) utilizaram a criptografia visual aplicada a imagens *captcha* (Completely Automated Public Turing test to tell Computers and Humans Apart) para propor uma solução de combate ao phishing. A proposta é dividida em duas fases: registro e login.

Na fase de registro o usuário cria uma senha que pode ser composta por letras e números para prover mais segurança, esta senha é concatenada a uma *string* que é gerada aleatoriamente pelo servidor para então uma imagem *captcha* ser gerada com base nessas informações. A imagem *captcha* é então criptografada visualmente e dividida em duas parcelas, onde são encaminhadas para o usuário uma parcela do *captcha* criptografado e também o *captcha* original, e a outra parcela fica armazenada no servidor pronta para ser usada durante o processo de login. A Figura 3 resume a fase de registro.

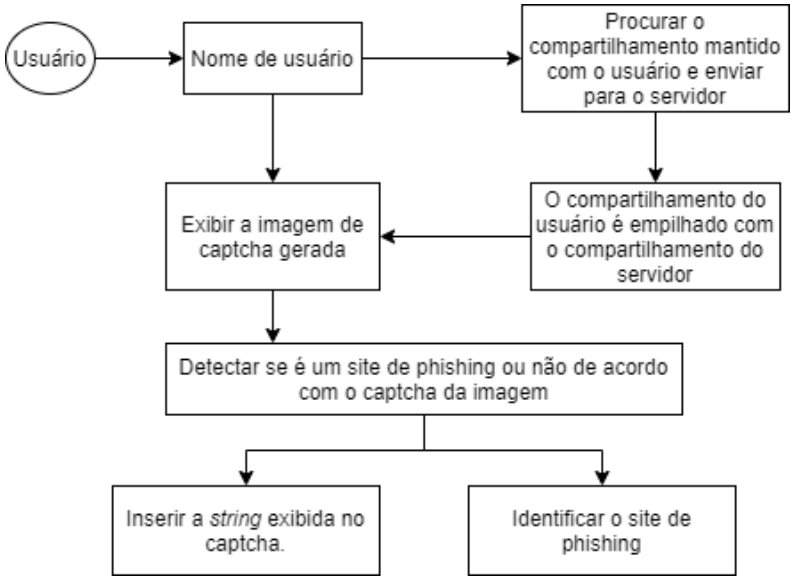
Figura 3. Fase de registro



Fonte. Traduzido de James e Philip, (2012)

A segunda fase do processo consiste no login, ao acessar o site o usuário primeiro insere uma chave que será o seu ID (podendo ser um nome de usuário de acordo com a proposta) e após isso realiza o upload de sua parcela, o servidor então realiza a sobreposição das duas imagens e exibe o *captcha* para o usuário onde este tem que identificar se este *captcha* corresponde ao que foi gerado no momento do registro para que possa identificar se a página é falsa ou não. A Figura 4 resume a fase de login.

Figura 4. Fase de login



Fonte. Traduzido de James e Philip, (2012)

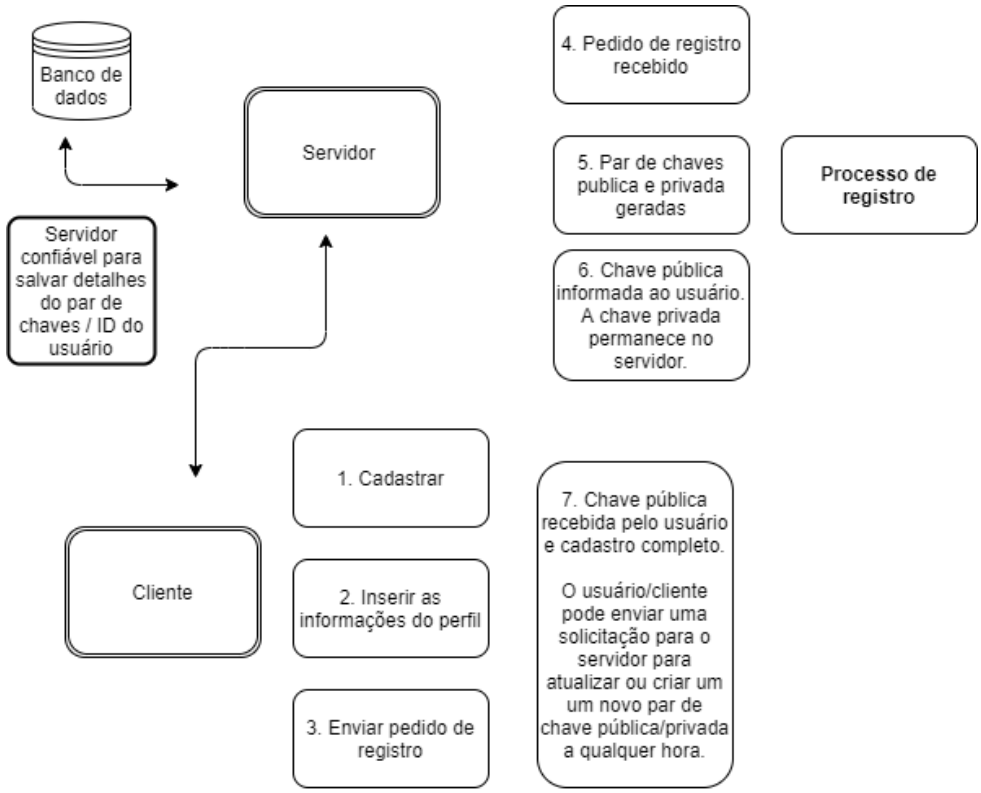
O fato de o sistema gerar um *captcha* com base em uma informação repassada pelo usuário concatenado a uma chave gerada pelo servidor é uma vantagem da proposta pois impediria ataques automatizados ou até mesmo em um possível ataque ao banco de dados da aplicação o roubo dos mesmos, já que estão criptografados visualmente. Por outro lado, a necessidade de o usuário armazenar uma parcela em seu dispositivo a deixa suscetível a roubos e outros problemas como caso a parcela seja excluída acidentalmente, outra questão é que o usuário tem que memorizar o conteúdo do *captcha* criado no cadastro.

2.2 SAOJI

Na proposta apresentada por KHATRI *et. al* (2015), "*Phishing Detection System Using Visual Cryptography*" além do esquema de criptografia visual também é utilizado o esquema de criptografia com chaves assimétricas[1]. A proposta é dividida em duas fases, a de cadastro e de login.

Na fase de cadastro o usuário insere informações básicas como: nome, e-mail, senha no sistema proposto para dar início ao processo. O servidor recebe esses dados juntamente com a solicitação de registro e gera um par de chaves assimétricas: uma pública e outra privada, armazena este par em um banco de dados e encaminha a chave pública para o usuário. A partir disso o processo de registro está concluído.

Figura 5. Fase de registro



Fonte. Traduzido de Khatri et. al, (2015)

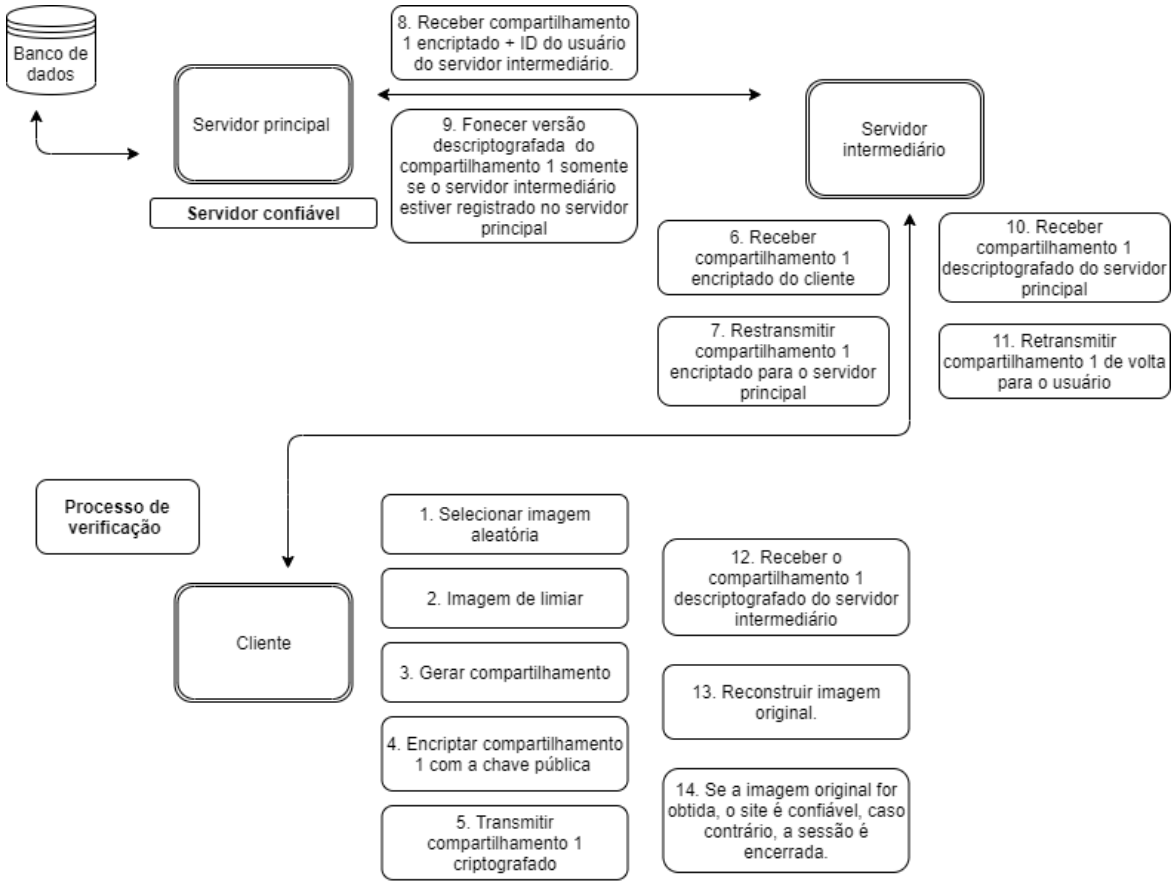
A segunda parte consiste na fase de login. Nessa parte o usuário seleciona uma imagem aleatória de seu dispositivo e encaminha para o servidor no qual a mesma será limpa, ou seja, transformada em escala de cinzas para então ser criptografada visualmente e dividida em duas parcelas, após isso a parcela 1 é criptografada com a chave pública do usuário e encaminhada para um servidor

[1] Chaves assimétricas: Conceito da criptografia para descrever a chave pública e privada que são usadas para cifrar mensagens e verificar a identidade de um usuário, onde a chave pública é usada para cifrar um conteúdo enquanto que a privada permite que esse conteúdo seja decifrado.

intermediário onde será verificada a identidade do usuário e autenticidade da operação.

Após o processo de criptografia e identificação do usuário o servidor intermediário encaminha a parcela 1 criptografada para o servidor principal onde será descriptografada usando a chave privada que ficou armazenada previamente, encaminhada de volta para este servidor intermediário, onde será realizada a sobreposição das duas parcelas. Caso a imagem original que foi enviada pelo usuário seja formada o mesmo saberá que o site é autêntico.

Figura 6. Fase de login



Fonte. Traduzido de Khatri et. al, (2015)

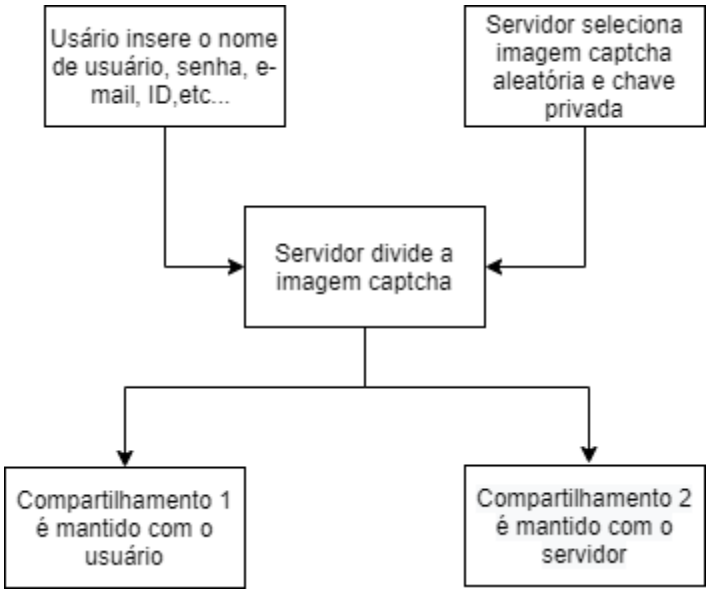
Uma vantagem a ser observada está no uso de um servidor intermediário para validar a identidade do usuário o que impediria um ataque direto ao servidor principal. Entretanto, a necessidade de o usuário sempre ter que escolher uma imagem de seu dispositivo para ser criptografada pode ser custoso.

2.3 CHAUDHARI

Na proposta "*Phishing Attack Prevention Using Visual Cryptography"* desenvolvida por CHAUDHARI *et. al* (2019) é apresentada a união da criptografia visual ao uso de uma chave gerada com base no sistema de cores RGB (*Red, green, blue*).

Como as propostas anteriores, este método também é dividido em duas fases, na fase de registro. O usuário insere informações de e-mail, nome de usuário e senha no site, após a inserção das informações, o servidor escolhe uma imagem aleatoriamente que está armazenada em sua base de dados para gerar um *captcha*. Esse *captcha* é analisado por um algoritmo que gera uma chave privada única com base nas cores RGB da imagem para então ser dividida em duas parcelas usando a criptografia visual. A parcela 1 ficará com o usuário e a parcela 2 ficará no servidor. Então são encaminhados para o usuário sua parcela do compartilhamento[2], a imagem original descriptografada e sua chave gerada com base na combinação de cores.

Figura 7. Fase de registro



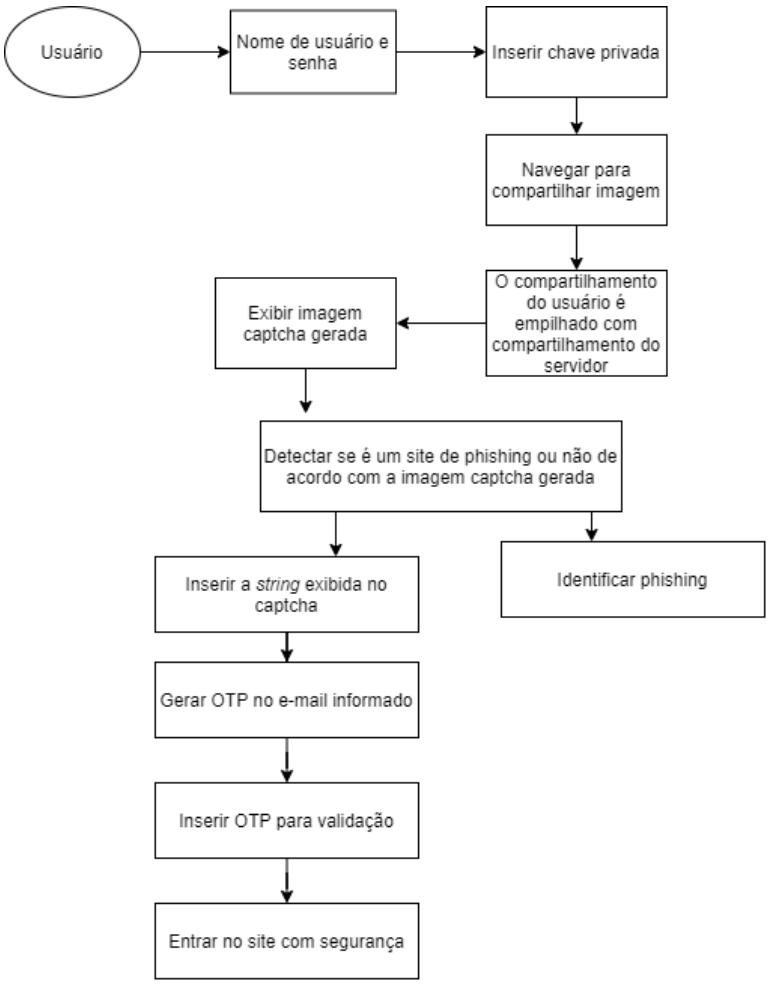
Fonte. Traduzido de Chaudhari *et. al*, (2019)

Na fase de login o site solicita o nome e a senha do usuário, solicita a chave gerada pela combinação de cores e o compartilhamento que ficou com o usuário. Após a validação das informações o sistema realiza a sobreposição e o *captcha* é gerado. A partir disso é possível identificar se o *captcha* corresponde ao que foi criado no momento do registro. Caso seja, o usuário insere o conteúdo daquele *captcha*, clica

[2] Compartilhamentos: São as imagens geradas após o processo criptografia visual de um segredo.

em confirmar, para então uma OTP (*One-time password*)[3] ser gerada e encaminhada para o e-mail cadastrado, o usuário coleta essa OTP e insere no campo solicitado e então a fase de login é concluída.

Figura 8. Fase de login



Fonte. Chaudhari *et. al*, (2019)

A pesquisa apresentada por CHAUDHARI (2019) possui técnicas adicionais de segurança para um sistema. Além do uso da criptografia visual, a proposta usa uma chave privada gerada pelo servidor com base no RGB de uma imagem no momento do cadastro e solicita que essa chave seja usada no login. O sistema também usa OTP para que o usuário acesse o sistema. Contudo, o fato de o usuário ter que inserir

[3] *One-time password:* É uma senha gerada que só tem validade para ser usada uma vez, podendo estar presente em sistemas de logins ou transações bancárias.

a senha primeiro antes de verificar a autenticidade do site poderá ocasionar no roubo de sua senha.

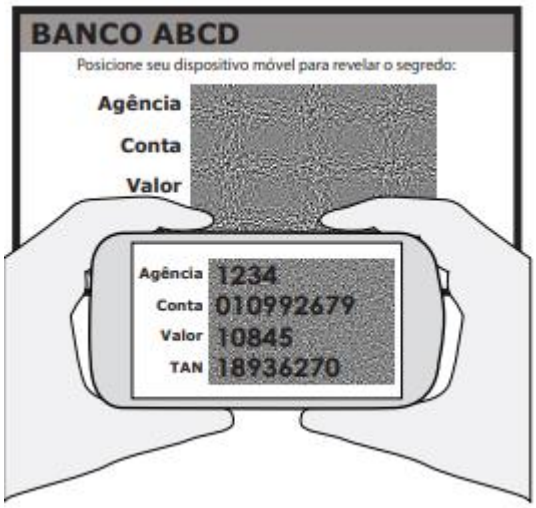
2.4 PIETZ

No trabalho “Criptografia Visual: Métodos de Alinhamento Automático de Parcelas Utilizando Dispositivos Móveis” de PIETZ (2014) foi desenvolvida uma proposta visando a grande variedade e quantidade de dispositivos móveis que possuem câmera. A proposta tem por objetivo utilizar a câmera dos dispositivos para visualizar o conteúdo de um segredo em uma parcela presente em outro meio.

O foco do trabalho gira em torno do uso da criptografia visual para autenticações bancárias e também na autenticação de produtos para que possa ser verificado se um produto é legítimo, usando métodos de alinhamento automático.

Em um caso de uso criado pelo autor é dado um exemplo de como o sistema

Figura 9. Resultado da sobreposição utilizando dispositivo móvel



Fonte. Pietz (2014)

poderia ser usado em um cenário de autenticação bancária. Um banco poderia gerar duas parcelas, de modo em que uma fosse encaminhada para o dispositivo no usuário, podendo ser através de um aplicativo da instituição, e a outra fosse exibida em um monitor, ao utilizar o sistema de alinhamento o usuário teria iria realizar a sobreposição das duas parcelas e revelar o conteúdo do segredo como mostra a figura 9.

Em outro caso de uso, o autor apresenta a fragilidade dos métodos para a verificação da autenticidade de um produto, demonstrando que não raro empresas têm utilizado códigos QR (*Quick Response*) impressos em produtos para que o

consumidor possa verificar se aquele produto é autêntico ou não. Porém, o autor relata que atualmente é muito fácil para qualquer pessoa criar seu próprio código QR através de diversos sites que estão disponíveis na web o que consequentemente facilita o trabalho de falsificadores para que criem versões inautênticas de produtos.

Para exemplificar, um criminoso de posse de um produto original, para ter acesso aos detalhes de autenticação, poderia copiar o site da empresa e criar o uma versão fraudulenta que faça o usuário acreditar que está se trata de um site verdadeiro de um produto supostamente original.

A proposta traz vantagens nas quais possibilita que as parcelas sejam alinhadas de maneira automática, visto que pode ser difícil alinhar pixel a pixel de maneira manual, outro ponto interessante é a distribuição das parcelas em tempo real, todavia enquanto que as propostas anteriores utilizam somente um dispositivo durante o processo, esta necessita de um recurso adicional para a autenticação, neste caso o celular.

De forma a sumarizar as propostas anteriores, a seguir é apresentada uma tabela contendo o objetivo de cada proposta.

Tabela 1. Diferença entre os correlatos e a proposta apresentada

	James e Philip	**Saoji**	**Chaudhari**	**Pietz**	**Proposta**
Objetivo	Mitigação de phishing	Mitigação de phishing	Mitigação de phishing	Alinhamento automático de parcelas	Mitigação de phishing
Modo de sobreposição das parcelas	Automático, mas somente após o usuário realizar o upload de sua parcela manualmente.	Automático, mas somente após o usuário realizar o upload de uma imagem escolhida manualmente.	Automático, mas somente após o usuário realizar o upload de sua parcela manualmente.	Automático	Manual, através da câmera do dispositivo.
Plataforma	Computador	Computador	Computador	Celular	Computador e celular

Necessário escolher a imagem para ser criptografada	Sim	Sim	Sim	Não	Não

Fonte. Autoria própria, (2020)

CAPÍTULO 3

FUNDAMENTAÇÃO TEÓRICA

Neste capítulo será abordada as temáticas que serviram como base para o desenvolvimento deste trabalho. As seções 3.1 e 3.2 apresentam uma breve abordagem sobre os ataques de engenharia social e as principais técnicas utilizadas pelos atacantes para ludibriar as vítimas, Na Seção 3.3 é abordado sobre o ataque de phishing. Em seguida, na Seção 3.4, são apresentadas principais técnica de phishing usadas por atacantes. Posteriormente, na Seção 3.5, é realizada uma breve introdução sobre as ferramentas usadas por estes atacantes. Sa Seção 3.6 é realizada uma abordagem geral sobre criptografia. Por fim, na Seção 3.7, são apresentadas as principais características da criptografia visual, bem como descrição do funcionamento de algumas técnicas utilizadas.

3.1 ENGENHARIA SOCIAL

Frente ao crescimento da tecnologia e do papel de grande importância que esta vem tomando na sociedade sendo usada para os mais diversos fins, empresas perceberam a necessidade da informatização de seus sistemas visando se manterem competitivas no mercado e também almejando uma melhor gerência da informação.

Dado o valor da informação, diversas instituições têm investido na aquisição de sistemas mais modernos e seguros visando uma melhor gerência desse ativo. Porém, segundo SILVA (2013) há um menosprezo da importância do fator humano dentro desse sistema o que deixa a organização suscetível ao ataque de Engenharia Social (ES).

A Engenharia Social, ao contrário do que se pensa, não se trata de um ataque onde o criminoso possui conhecimentos técnicos avançados em computação. Para a realização dos ataques só é preciso a habilidade social para persuadir um indivíduo a tomar decisões que beneficiem o atacante. De acordo com MITNICK (2004), no âmbito da Segurança da Informação a ES é a habilidade de manipular pessoas para obter informações necessárias a fim de conseguir acessar um sistema ou obter informações privadas.

O uso dessa técnica tem se mostrado um grande obstáculo para a Segurança da Informação, visto que uma instituição pode adquirir os melhores e mais eficazes hardwares e softwares para corrigir falhas e proteger informações. No entanto, por mais rigorosa que seja a política de segurança da informação dessa instituição certamente ainda irão existir pessoas para gerir esses recursos; pessoas que são suscetíveis a fatores sociais e psicológicos se tornando uma rota de invasão para os Engenheiros Sociais.

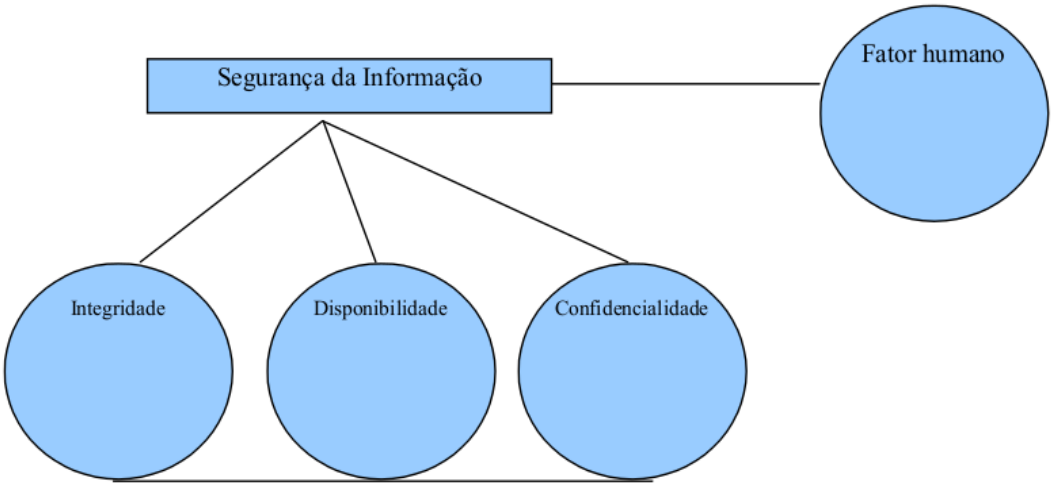
> “Os humanos são, em geral, o ponto mais suscetível de qualquer esquema de segurança. Um trabalhador que seja malicioso, descuidado ou desavisado acerca da política de informação de uma organização pode comprometer até a melhor segurança”. (COMER, 2015)

Segundo ALVES (2010) um dos maiores problemas da segurança da informação está relacionado ao ser humano e sua ignorância, NASSARO (2012) adverte que as organizações devem sempre estar atentas a funcionários descontentes, que por algum motivo, podem usar informações sigilosas da organização a fim de prejudicar a mesma.

Atualmente, muito se tem discutido sobre a inclusão do fator humano como um dos pilares da segurança da informação visto que os pilares abordados pela ISO/IEC 17799:2000 - padrão internacional específico para segurança da informação - são os de: Confidencialidade, Integridade e Disponibilidade. Nesse sentido, o fator humano, ainda que considerado na Segurança da Informação não é levado como um pilar, como é possível observar na Figura 10.

De acordo com SILVA e COSTA (2009) se faz necessária a implantação desse fator como um dos pilares, pois embora ele seja fundamental para gerenciar os outros

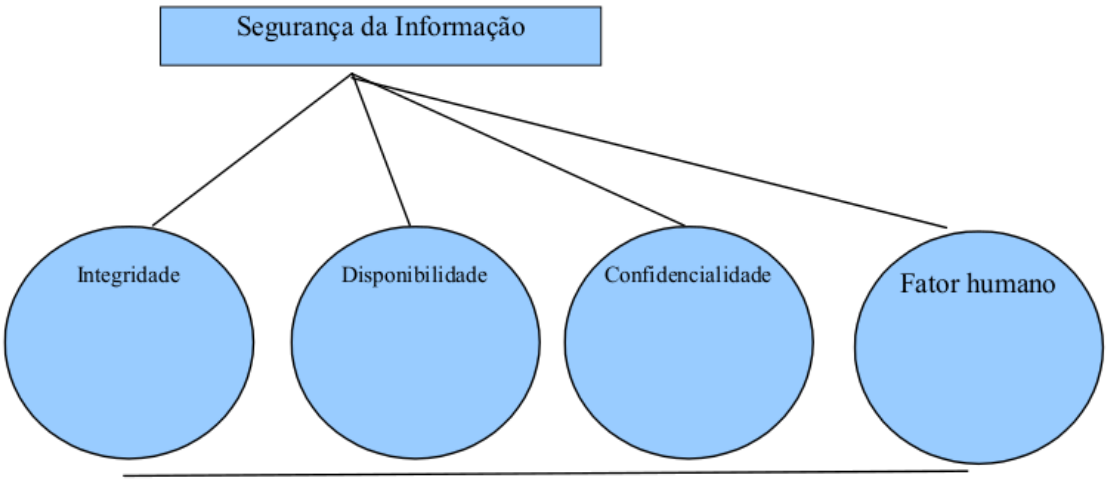
Figura 10. Atual modelo da Segurança da Informação baseada em três pilares



Fonte. Silva e Costa, (2009)

pilares, o aspecto humano ainda é constantemente menosprezado e essa desvalorização contribui para que todo o sistema tenha prejuízos significativos.

Figura 11. Proposta para a inserção do fator humano como pilar para a Segurança da Informação



Fonte. Silva e Costa, (2009)

As figuras 10 e 11 expõem respectivamente os pilares atuais da Segurança da Informação e esses mesmos pilares somados ao fator humano, denotando que assim como a Integridade, Disponibilidade e a Confidencialidade que atuam através de fatores técnicos dentro de um sistema, com uso de softwares e hardwares, o fator humano precisa ser tratado de igual maneira e não somente como um fator secundário.

3.2 AS PRINCIPAIS TÉCNICAS DE PERSUASÃO EMPREGADAS POR ENGENHEIROS SOCIAIS

Para emplacarem ataques bem sucedidos os Engenheiros Sociais fazem uso de diversas técnicas, que vão desde vasculhamento de lixos até a manipulação psicológica da vítima. Segundo PEREIRA e MARTINS (2014) os ataques podem ter dois aspectos: o físico, que pode ser caracterizado como o local de trabalho, o uso de telefone, busca de informações em lixos da empresa ou vítima, ou mesmo através de meios on-line e o aspecto psicológico que envolve a persuasão da vítima para a obtenção de vantagens.

No livro "*Influence: The Psychology of Persuasion*", CIALDINI (2006) descreve as principais técnicas de manipulação psicológica que são utilizadas pelos Engenheiros Sociais: Reciprocidade; Compromisso/Consistência; Prova Social; Simpatia; Autoridade e Escassez.

3.2.1 Reciprocidade

A reciprocidade diz que deve-se retribuir algo que foi dado por outra pessoa, naturalmente o ser humano se sente obrigado a retribuir algo que lhe é dado.

> "Se um homem nos envia um presente de aniversário devemos lembrar do aniversário dele com um presente, se um casal nos convida para a sua festa, devemos ter certeza de convidá-los para a nossa. Em virtude da regra de reciprocidade nós obrigatoriamente temos que retribuir esses favores, presentes, convites." (CIALDINI, 2006, p.23)

Geralmente essa "troca de favores" pode acabar resultando em trocas desiguais de informações ou favores causando prejuízos para a vítima. Segundo CIALDINI (2006) a pessoa paga mais do que é devido para aliviar o sentimento o sentimento de culpa.

3.2.2 Compromisso e Consistência

O princípio do compromisso e da consistência são condições do ser humano que são passivas para um ataque de engenharia social. Esse princípio diz que uma vez tomada uma decisão, a pessoa tem o compromisso de agir de maneira mais consistente possível de acordo com a decisão tomada. Assim como outras técnicas de persuasão esta está profundamente dentro do ser humano, influenciando suas ações de forma silenciosa.

> "É simplesmente nosso desejo quase obsessivo ser (e parecer) consistente com o que já fizemos. Depois de fazer uma escolha ou tomar uma posição, encontraremos pressões pessoais e interpessoais para se comportar de forma consistente com esse compromisso. Essas pressões nos levarão a responder de maneira a justificar nossa decisão anterior. "(CIALDINI, 2006, p. 53)

3.2.3 Prova Social

As pessoas tendem a seguir os passos ou atitudes de outras pessoas, geralmente pessoas parecidas com elas, isso faz com que esse princípio seja bastante eficaz para um ES. Normalmente isso acontece quando um indivíduo está inseguro quanto a maneira que ele deve se comportar dentro um ambiente ou diante de alguma situação e, perante esse estado de incerteza, é comum olhar para o comportamento de outras pessoas para descobrir como se comportar, supondo que essas pessoas ao redor possuem mais conhecimento sobre a situação.

> “A tendência é ver uma ação como mais apropriada quando outras pessoas a praticam, normalmente funciona muito bem. Como regra, cometeremos menos erros agindo de acordo com as evidências sociais do que contrárias a elas. Normalmente, quando um grande número de pessoas está fazendo alguma coisa, é a coisa certa a fazer. Esta característica do princípio da prova social prova é simultaneamente sua força maior influência e sua maior fraqueza.” (CIALDINI, 2006, p. 98-99)

Assim, como os outros princípios de influência, a prova social fornece um caminho vantajoso para determinar como um indivíduo deve se comportar, contudo como uma faca de dois gumes, torna-o vulnerável para ataques de ES, CIALDINI (2006).

3.2.4 Simpatia

É provável que esse princípio seja o mais fácil para se aplicar, contudo não deixa de ser uma grande ferramenta na mão de um ES. É comum as pessoas se sentirem mais à vontade com pessoas com quem elas se identificam, a beleza, as semelhanças, a familiaridade, os elogios e exaltações são alguns dos fatores usados para causar simpatia e com os quais são capazes de seduzir vítimas em potencial. As pessoas tendem a dizer mais “sins” para pedidos de pessoas de quem conhecem e gostam CIALDINI (2006).

> “Aparentemente, temos uma reação automaticamente positiva a elogios que podemos ser vítimas de alguém que os usa de uma maneira óbvia para tentar ganhar nosso favor.” (CIALDINI, 2006, p. 146)

3.2.5 Autoridade

Naturalmente o ser humano tem a tendência de acatar ordens de pessoas que aparentemente exibem um determinado grau de autoridade, geralmente as pessoas deduzem essa autoridade pelo modo que uma pessoa está vestida seja um jaleco, farda que conote um cargo de autoridade, terno, pelo veículo, ou condição financeira.

Segundo CIALDINI (2001) o ser humano tende a responder afirmativamente, aos pedidos ou as ordens de uma figura autoritária por medo de repreensão ou pela esperança de uma recompensa.

> "[...] porque suas posições falam de superior acesso à informação e ao poder, faz muito sentido cumprir com os desejos das autoridades devidamente constituídas." (CIALDINI, 2006, p. 174)

3.2.6 Escassez

Segundo o princípio da escassez o ser humano tem uma forte tendência a ficar mais interessado em coisas que estão menos disponíveis. Essa característica está relacionada a uma ação instintiva que praticamente todas as pessoas possuem, a de querer coisas que são mais raras ou incomuns.

> "Com o princípio da escassez as oportunidades nos parecem mais valiosas quando a disponibilidade delas é limitada… A ideia de perda em potencial desempenha um grande papel na tomada de decisão humana.
>
> De fato, as pessoas parecem estar mais motivadas pelo pensamento de perder algo do que pelo pensamento de ganhar algo de igual valor." (CIALDINI, 2006, p. 177)

Um evidente exemplo é o ouro, é um elemento que assim como o ferro, está presente na natureza. A grande diferença é que o ferro é um elemento encontrado em abundância, fazendo com seu valor de mercado seja bastante baixo enquanto que o ouro que também é um metal encontrado na natureza tem o valor de mercado consideravelmente mais alto que o do ferro, além de ser um elemento cobiçado por muitas pessoas, diferente do ferro. A questão é: o que faz o ouro ser tão cobiçado? A escassez.

3.3 O ATAQUE DE PHISHING

O *phishing* é uma técnica de ataque onde criminosos tentam ludibriar vítimas a fim de roubar dados pessoais, geralmente são de cunho financeiro, como: dados de cartões de crédito, *tokens* usados para autenticação de transações bancárias, logins utilizados em sites de instituições financeiras, entre outros. A estratégia consiste em criar um site fraudulento que apresente todos os elementos de um site legítimo, contendo logotipos, textos e elementos que são extremamente parecidos com o do site original.

Existem diversas formas do *phishing* chegar até a vítima, mensagens de texto, redes sociais, *pop-ups* nos navegadores de internet, e-mails; no qual um atacante

disponibiliza um link para a vítima que irá direcioná-la para uma página falsa, onde comumente a mesma encontrará um formulário solicitando informações pessoais que normalmente são dados de cartões de crédito, senhas, números de documentos que serão enviados ao atacante.

Segundo o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (Cert.br), para atrair a atenção das vítimas são explorados os mais diversos tópicos e temas geralmente são campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento. O Cert.br resume os exemplos de tópicos e temas de mensagens de phishing como apresentado na Tabela 2.

Tabela 2. Exemplos de tópicos e temas de mensagens de phishing

Tópico	Tema da mensagem
Álbuns de fotos e vídeos	pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão traição, nudez ou pornografia, serviço de acompanhantes
Antivírus	atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades
Associações assistenciais	AACD Teleton, Click Fome, Criança Esperança
Avisos judiciais	intimação para participação em audiência comunicado de protesto, ordem de despejo
Cartões de crédito	programa de fidelidade, promoção
Cartões virtuais	UOL, *Voxcards*, Yahoo! Cartões, O Carteiro, *Emotioncard*
Comércio eletrônico	cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em *site* de compras coletivas
Companhias aéreas	promoção, programa de milhagem
Eleições	título eleitoral cancelado, convocação para mesário
Empregos	cadastro e atualização de currículos, processo seletivo em aberto

Imposto de renda	nova versão ou correção de programa consulta de restituição, problema nos dados da declaração
Internet Banking	unificação de bancos e contas, suspensão de acesso atualização de cadastro e de cartão de senhas lançamento ou atualização de módulo de segurança comprovante de transferência e depósito, cadastramento de computador
Multas e infrações de trânsito	aviso de recebimento, recurso, transferência de pontos
Prêmios	loteria, instituição financeira
Promoções	vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita
Redes sociais	notificação pendente, convite para participação aviso sobre foto marcada, permissão para divulgação de foto
Serviços de *e-mail*	recadastramento, caixa postal lotada, atualização de banco de dados
Serviços de proteção de crédito	regularização de débitos, restrições ou pendência financeira
Serviços de telefonia	recebimento de mensagem, pendência de débito bloqueio de serviços, detalhamento de fatura, créditos gratuitos

Fonte. Cert.br, (2017)

3.4 TIPOS DE PHISHING

Existem diversas formas de *phishing,* nas quais os criminosos escolhem aquelas que melhor se adaptam ao seu objetivo variando de acordo com o tipo de alvo ou o(s) tipo(s) de informação(ões) que esses criminosos desejam roubar. Segundo PEREIRA (2013) as mais comuns são: Pharming, Spear Phishing, iPhishing e Vishing Scam.

3.4.1 Pharming

De acordo com MULING e KIMBALL (2007) o *pharming* é a forma de *phishing* mais avançada tecnologicamente, na qual faz uso de um vírus ou malware que foi instalado no computador da vítima para levá-la a sites fraudulentos. Nesse tipo de ataque é

explorada a vulnerabilidade do sistema DNS (*Domain Name System*) que é responsável por traduzir as URLs (*Uniform Resource Locator*) em um número de IP (*Internet Protocol*), por exemplo ao digitar “google.com” o DNS traduz e direciona para o IP 216.58.222.78.

Desse modo, com o sistema DNS vulnerável, quando o usuário insere um endereço legítimo no navegador este é direcionado para uma imitação do site original e como resultado disso qualquer informação fornecida neste site será enviada diretamente para os criminosos.

3.4.2 Spear Phishing

O *Spear Phishing* é um tipo de *phishing* personalizado, onde o criminoso tem como alvo um grupo muito restrito podendo ser um departamento de uma empresa ou até mesmo um único executivo da alta gerência. Conforme a escolha do alvo é estabelecida são realizadas diversas pesquisas sobre a rotina daquele grupo ou daquela pessoa em específico com o objetivo de deixar o ataque o mais customizado e convincente possível. Segundo PEREIRA (2013) o atacante se molda a rotina do alvo absorvendo jargões e características do dia a dia, o que pode demorar vários dias.

De acordo com MOREIRA (2017) para a obtenção de informações sobre o alvo em uma fase inicial são utilizadas técnicas de *Open Source Intelligence* (OSINT) que são fontes de domínio público tais como rádio, televisão e jornais. Essa focalização torna o *Spear phishing* muito mais perigoso que o *phishing* comum onde segundo PAIS *et al.* (2013) logo sendo provavelmente mais utilizado para ataques visando obter ganhos econômicos, segredos ou informação militar

Normalmente esses ataques surgem através de uma fonte confiável para a vítima, como um e-mail ou site no qual ela normalmente interage e que possa ter sido comprometido, ou pelo qual o atacante esteja se passando.

3.4.3 iPhishing

Conforme o avanço da tecnologia e a forte informatização dos mais diversos dispositivos como: relógios, carros e até geladeiras fizeram-se necessárias diversas mudanças relacionadas ao modo de navegação na internet.

Características físicas destes dispositivos como o tamanho da tela, por exemplo fizeram com que elementos presentes nos navegadores comuns fossem removidos ou redimensionados para se adaptarem às limitações de hardware, onde conforme NIU *et al.* (2008) infelizmente alguns desses recursos são críticos para se defender de ataques de *phishing*.

Normalmente quando o sistema adapta sites para esses novos tipos de dispositivos o usuário perde a capacidade de analisar uma URL por exemplo, tendo em vista que a barra onde normalmente a mesma é exibida fica oculta ou quando ela é exibida é de maneira incompleta.

Segundo MARTINS (2008) a definição de iPhishing é:

> *"...a vertente que visa explorar vulnerabilidades consequentes do avanço excessivamente rápido da tecnologia, que acaba por deixar aspectos de segurança em segundo plano, dando lugar à funcionalidade e ao design."*

O modo de ataque, assim como outros tipos de phishing normalmente ocorre através de e-mails ou SMS (*Short Message Service*) que chegam para o usuário, ainda de acordo com NIU *et. al* (2008) digitar é um processo tedioso e muitas vezes impreciso para usuários não acostumados com uma tela tão pequena. Por conta disso, é tentador seguir links em e-mails em vez de digitar os links manualmente.

De acordo com PEREIRA (2013) essa técnica ainda será bastante explorada por criminosos considerando o surgimento constante de novas tecnologias, que sempre virá acompanhado de grandes vulnerabilidades.

3.4.4 Vishing Scam

O *Vishing Scam* é uma categoria do *Phishing* onde um atacante faz uso do recurso de VOIP (*Voice Over Internet Protocol*) que permite que ligações de voz sejam feitas através da internet. Nessa técnica em vez de levar a vítima para um site falso o criminoso, fazendo uso de engenharia social através de SMS, a induz ligar para um número (via VOIP), onde serão solicitadas informações pessoais ou dados bancários que uma vez digitados são interceptados por um aparelho capaz de reconhecer o som das teclas digitadas e gravá-los.

Segundo CRESPO e SYDOW (2010) o *Vishing* é um ataque muito efetivo, pois através do contato telefônico a vítima se sente mais segura e confiante, uma vez que o agente que atende o telefone simula ser um funcionário de uma companhia real, fazendo com que esta ceda seus dados com mais facilidade.

3.5 FERRAMENTAS E TÉCNICAS EMPREGADAS POR ATACANTES

Uma das principais maneiras de configurar um ataque de *phishing* é através do uso de ferramentas que facilitem o trabalho do atacante, automatizando processos que normalmente seriam maçantes se fossem feitos de maneira manual. Com isso são usadas ferramentas para a clonagem de sites, envio de e-mails em massa e ferramentas para mascarar URL, com o intuito deixar o ataque o mais otimizado possível.

A seguir são apresentadas algumas dessas ferramentas.

3.5.1 Blackeye

É uma ferramenta voltada para o roubo de credenciais de acesso. Através dela é possível realizar a clonagem de até 32 sites e mais um customizável. O atacante escolhe a opção que deseja, a ferramenta replica o site original e gera uma URL que deve ser enviada para o alvo, quando o link é aberto a página falsa é exibida para vítima. Para um usuário comum, as mudanças em relação ao site original são praticamente imperceptíveis.

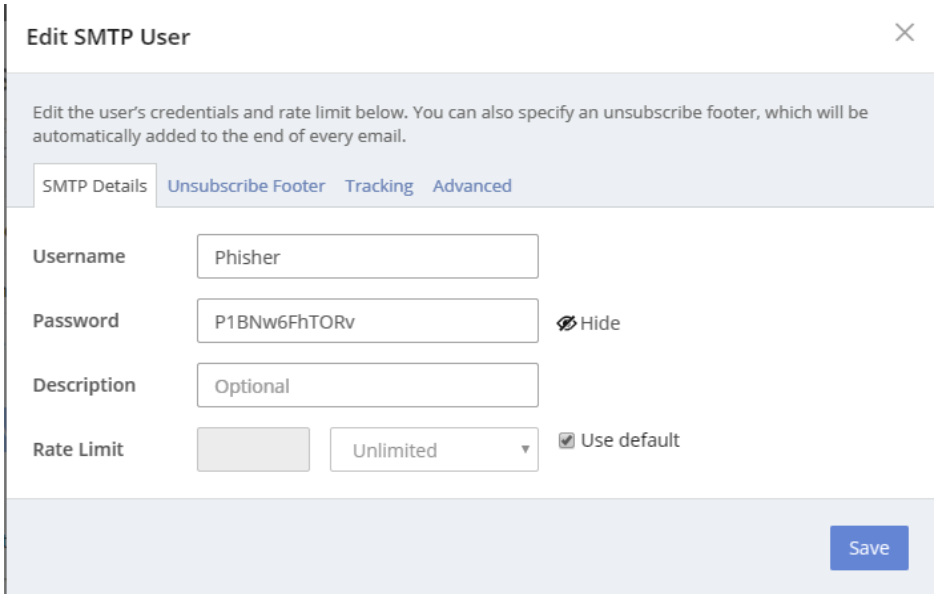
Figura 12. Ferramenta para clonagem de sites “Blackeye”

Fonte. Autoria própria, (2020)

3.5.2 SMTP2Go

Basicamente é um serviço de envio de e-mails para empresas que precisam lidar com um grande volume de envios, como por exemplo e-mails de marketing ou boletins informativos. De modo simplificado esse serviço permite que qualquer usuário se cadastre e crie uma conta para usar durante um período de teste, observando essa possibilidade criminosos perceberam a oportunidade de usar esse serviço ao seu favor.

Figura 13. Credenciais de acesso criadas autenticação no servidor SMTP



Fonte. Autoria própria, (2020)

Após a criação da conta no SMTP2Go um usuário e uma senha são gerados para serem usados no processo de autenticação no servidor SMTP (Simple Mail Transfer Protocol) “mail.smtp2go.com” normalmente na porta 25.

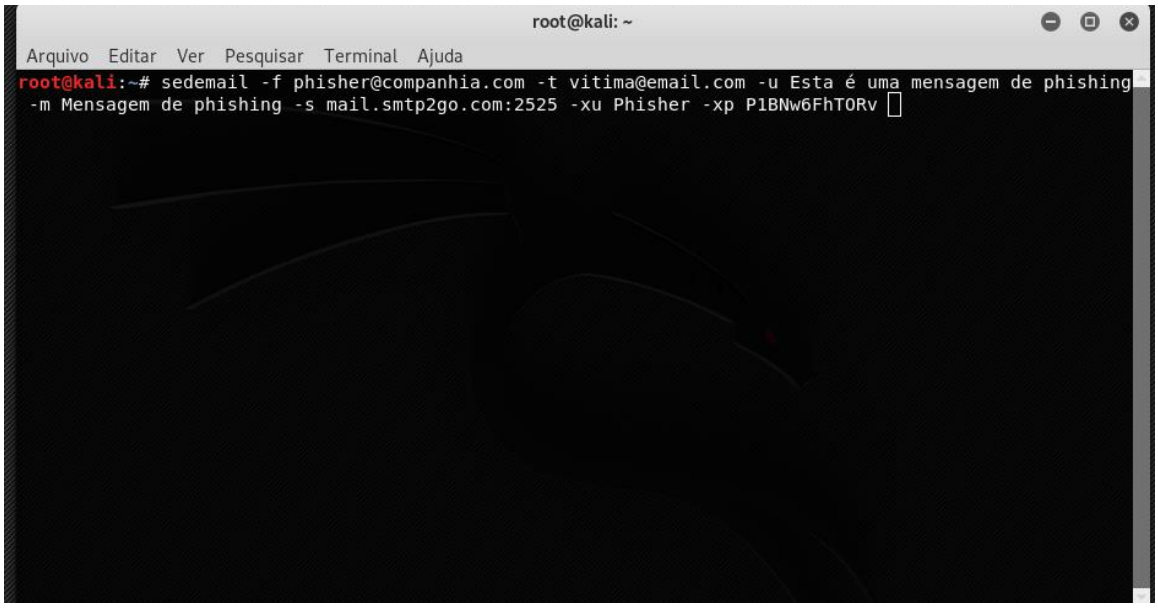
Figura 14. Endereço do servidor SMTP e portas de acesso

Fonte. Autoria própria, (2020)

Explorando a flexibilidade do protocolo SMTP, criminosos conseguem falsificar o remetente de uma mensagem de e-mail, e enviá-la para uma vítima se passando por uma instituição real, sem que esta perceba que se trata de um remetente fraudulento, essa técnica é conhecida como e-mail *spoofing*.

Normalmente, para o envio desses e-mails, os criminosos utilizam ferramentas específicas, como o SendEmail que permite inserção de parâmetros específicos, como o endereço do remetente do e-mail (falso remetente), e-mail do destinatário, endereço do servidor SMTP, nome de usuário e senha para autenticação no servidor.

Figura 15. Envio de um e-mail de phishing com a ferramenta “Sendemail”



Fonte. Autoria própria, (2020)

3.5.3 Homograph Attack

É uma técnica na qual um atacante faz uso do alfabeto conhecido como cirílico que é utilizado como base para a grafia de seis línguas nacionais eslavas (bielorrusso, búlgaro, macedônio, russo, sérvio e ucraniano). Esse alfabeto possui caracteres muito similares aos do alfabeto latino, o que permite que atacantes registrem domínios falsos muito similares aos de companhias autênticas.

A técnica consiste basicamente na utilização do “Punycode”, um protocolo de programação responsável por traduzir caracteres “Unicode” (que abrange o alfabeto cirílico) em uma cadeia de caracteres mais limitada que é permitida para nomes de domínios.

De acordo com ZHENG (2017)

> “O Punycode possibilita o registro de domínios com caracteres estrangeiros. Ele funciona convertendo o rótulo de domínio individual em um formato alternativo usando apenas caracteres ASCII. Por exemplo, o domínio "xn–s7y.co" é equivalente a "短 .co.”
>
> Do ponto de vista da segurança, os domínios Unicode podem ser problemáticos porque é difícil distinguir muitos caracteres Unicode dos caracteres ASCII comuns. É possível registrar domínios como "xn–pple-43d.com", que é equivalente a "apple.com". Pode não ser óbvio à primeira vista, mas "apple.com" usa o cirílico "a" (U + 0430) em vez do ASCII "a" (U + 0061). Isso é conhecido como um ataque homográfico.”

Um exemplo que pode ser aplicado está nos seguintes links: “https://facebook.com” e “https://facebook.com", aparentemente os links levam para o mesmo site, porém quando interpretados pelo navegador são links diferentes. O primeiro é um domínio registrado pela *Facebook Incorporated* e o segundo é um falso domínio usando o alfabeto cirílico. Segundo HAYASHI (2017) ataques de phishing que utilizam essa técnica podem enganar até os profissionais mais experientes.

Não existe uma ferramenta específica que um atacante possa usar para aplicar essa técnica, porém é bastante fácil encontrar tabelas em diversas fontes com o alfabeto cirílico, onde um atacante pode simplesmente copiar e colar o caractere desejado e realizar o ataque homográfico.

Tabela 3. Alfabeto russo parcial

Maiúscula	Minúscula	Nome em Português	Exemplo	Código Unicode
А	**а**	A	'a' em **a**belha	U+0410 / U+0430
Е	**е**[4]	Ye	'ie' em **Ie**manjá	U+0415 / U+0435
З	**з**	Ze	'z' em **z**ebra	U+0417 / U+0437
И	**и**[4]	I	'i' em l**i**vro	U+0418 / U+0438
Й	**й**	I kratkoye	'i' semivogal em *pa**i***	U+0419 / U+0439
К	**к**	Ka	'k' em **k**aiser	U+041A / U+043A
М	**м**	Em	'm' em **m**apa	U+041C / U+043C
Н	**н**	En	'n' em **n**avio	U+041D / U+043D
О	**о**	O	'o' em **o**gro	U+041E / U+043E

Fonte. Adaptado de Wikipédia, (2019).

3.6 CRIPTOGRAFIA

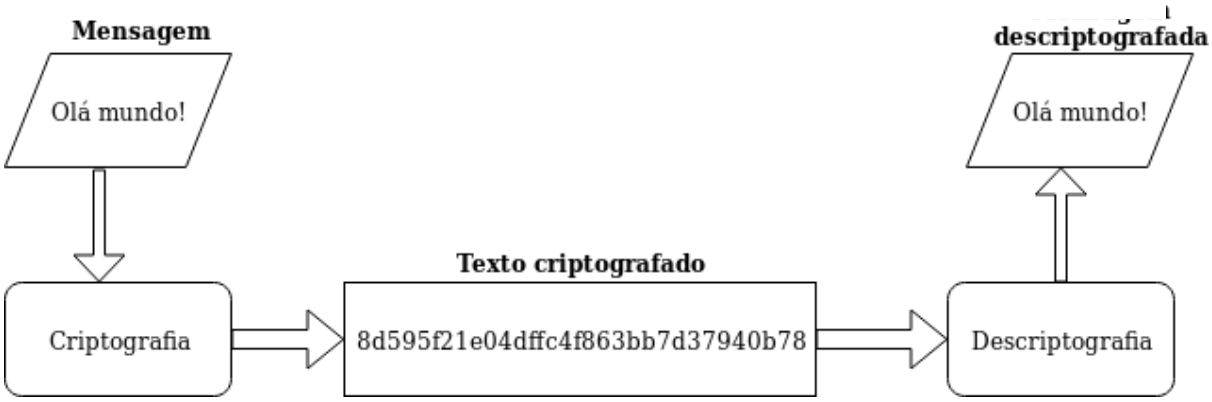
Segredos religiosos, posicionamento de exércitos, mensagens militares, desde o surgimento da civilização o homem sempre se deparou com problemas para compartilhar segredos que somente as partes interessadas pudessem ter acesso. Dada essa necessidade surge a ciência que estuda essa arte de se comunicar secretamente, a criptografia.

Em virtude do acelerado avanço da internet, tecnologias e o grande fluxo de dados e informações que trafegam através destas, surgiu-se a necessidade de manter seguros dados e informações privadas. Transações financeiras, segredos comerciais, informações de clientes se tornaram os maiores ativos das grandes corporações e em virtude disso, essas organizações, tiveram que adquirir métodos a fim de que essas informações fiquem disponíveis apenas para pessoas autorizadas.

A criptografia surgiu com o objetivo de proteger dados e informações privadas que devem ser acessadas e compreendidas apenas por pessoas autorizadas, visto que dentro de um sistema de comunicação informações que trafegam pela rede podem ser interceptadas e/ou alteradas por terceiros.

É a ciência encarregada de desenvolver métodos para transformar textos que são legíveis em mensagens que só poderão ser entendidas por pessoas que têm a devida autorização.

Figura 16. Processo básico de criptografia



Fonte. Autoria própria, (2020)

Com o crescente uso das redes de computadores e a massificação do uso da internet, surgiu a necessidade de impor novos mecanismos de segurança a fim de garantir a confidencialidade dos dados que transitam na rede, desse modo dando espaço para o surgimento da criptografia moderna.

Segundo PAREDES (2006) a criptografia moderna pode foi iniciada após três fatos: o primeiro foi a publicação da “Teoria da Informação”, apresentado por Shannon, o segundo foi o surgimento do DES (Data Encryption Standard) em 1974 e o terceiro com o surgimento do estudo realizado por Whitfield Diffie e Martin Hellman sobre a aplicação de funções matemáticas unidirecionais a um modelo de criptografia, chamada criptografia de chave pública em 1976.

A criptografia moderna pode ser dividida em dois grupos, são eles:

3.6.1 Criptografia Simétrica

Na criptografia de chave simétrica tanto o emissor quanto o receptor da mensagem possuem a mesma chave secreta, ou seja, a mesma chave é que utilizada para cifrar o texto claro é usada para desencriptar esse mesmo texto. Para ser realizada, basta que o emissor, antes de enviar a mensagem criptografada, envie a chave secreta que será utilizada para descriptografá-la.

No seu livro, Criptografia e Segurança de Redes, STALLINGS, (2014) demonstra que um esquema criptografia simétrica possui cinco itens:

Texto claro: essa é a mensagem ou dados originais, inteligíveis, que servem como entrada do algoritmo de encriptação.

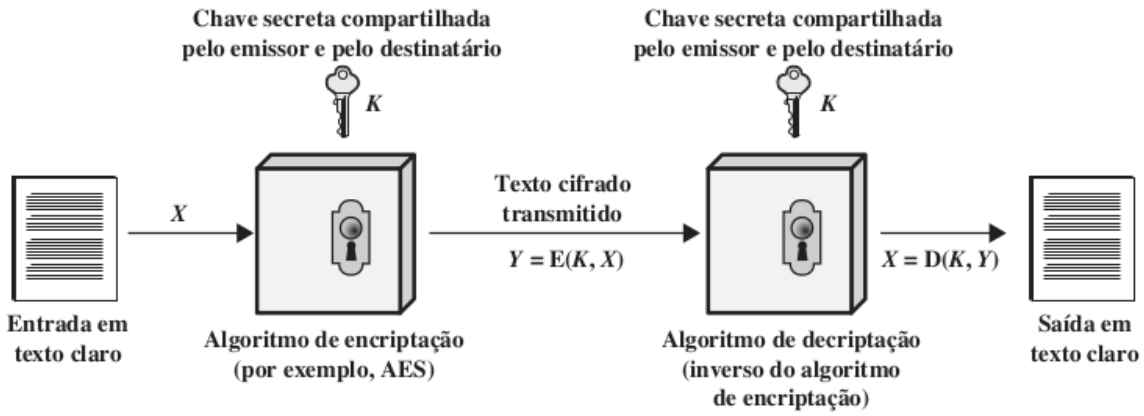
Algoritmo de encriptação: realiza diversas substituições e transformações no texto claro.

Chave secreta: também é uma entrada para o algoritmo de encriptação. A chave é um valor independente do texto claro e do algoritmo. O algoritmo produzirá uma saída diferente, dependendo da chave usada no momento.

Texto cifrado: essa é a mensagem embaralhada, produzida como saída do algoritmo de encriptação. Ela depende do texto claro e da chave secreta. Para determinada mensagem, duas chaves diferentes produzirão dois textos cifrados distintos. O texto cifrado é um conjunto de dados aparentemente aleatório e, nesse formato, ininteligível.

Algoritmo de decriptação: esse é basicamente o algoritmo de encriptação executado de modo inverso. Ele apanha o texto cifrado e a chave secreta e produz o texto claro original.

Figura 17. Esquema de encriptação simétrica



Fonte. Stallings, (2014)

3.6.2 Criptografia Assimétrica

Conforme foram citados os cinco itens da criptografia assimétrica na seção 2.6.1, nesse tipo de criptografia também são utilizados os mesmos itens, apenas adicionando o conceito de chave pública, que no contexto da criptografia assimétrica é a chave usada para desencriptar uma mensagem.

Nesse esquema de criptografia ao contrário da criptografia simétrica que faz uso apenas de uma chave são empregados dois tipos de chaves, uma privada e uma pública que são usadas para cifrar uma mensagem e verificar a identidade de um usuário. O sistema funciona de forma que alguém crie uma chave e envie essa chave à quem quiser mandar informações, essa é a chamada chave pública. Com ela é feita a encriptação da mensagem. Para decriptar será necessário utilizar uma outra chave que deve ser criada, a chave privada, que é secreta.

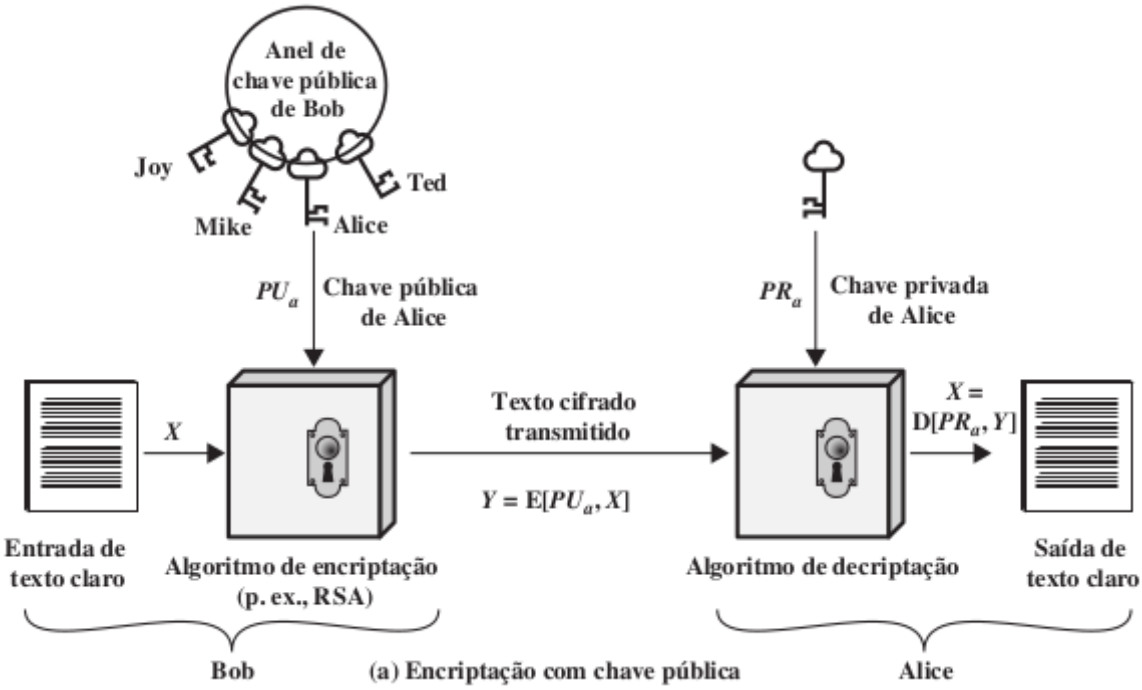
Segundo STALLINGS (2014) como os algoritmos assimétricos contam com uma chave para encriptação e uma chave diferente, porém relacionada, para a decriptação é importante ressaltar duas características desse esquema:

- É computacionalmente inviável determinar a chave de decriptação dado apenas o conhecimento do algoritmo de criptografia e da chave de encriptação;

Além disso, alguns algoritmos como o RSA exibem essa segunda característica:

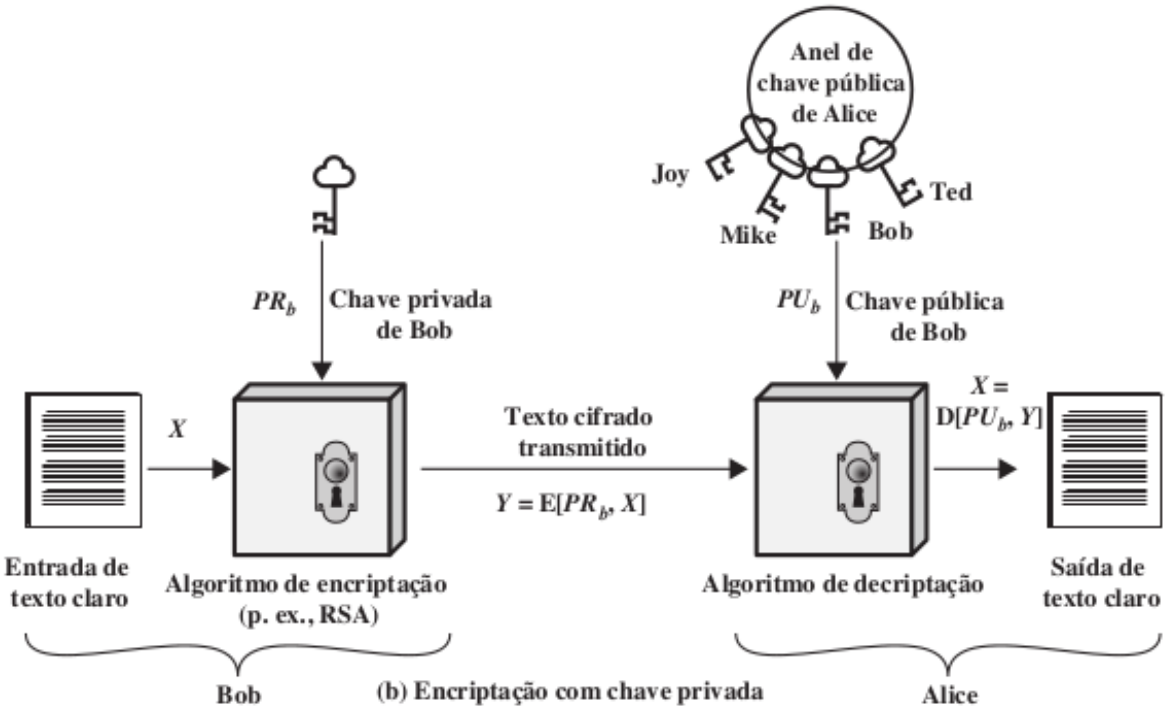
- Qualquer uma das duas chaves relacionadas pode ser usada para encriptação, com a outra para a decriptação, como é possível observar nas figuras 17 e 18.

Figura 18. Esquema de encriptação assimétrica usando chave pública para encriptar os dados



Fonte. Stallings, (2014)

Figura 19. Esquema de encriptação assimétrica usando chave privada para encriptar os dados



Fonte. Stallings, (2014)

3.7 CRIPTOGRAFIA VISUAL

Desenvolvida em 1994 pelos pesquisadores Naor e Shamir, a Criptografia Visual surgiu com o objetivo de permitir a qualquer pessoa a possibilidade de conseguir revelar um segredo que está criptografado sem conhecimentos criptográficos. O objetivo é produzir compartilhamentos de imagens de um determinado segredo de maneira em que estes compartilhamentos pareçam sem sentido quando separados, porém, ao sobrepor estes compartilhamentos o segredo seja novamente revelado.

A fórmula da Criptografia Visual está no sistema visual humano que permite a recuperação do segredo somente com a sobreposição destes compartilhamentos, o que a torna independente de cálculos matemáticos ou computadores, segundo os autores a técnica é perfeitamente segura e muito fácil de ser implementada.

Nesta seção serão apresentadas algumas técnicas; referentes ao modelo de Naor e Shamir e também algumas outras técnicas que surgiram após o lançamento de suas pesquisas.

3.7.1 O MODELO DE NAOR E SHAMIR

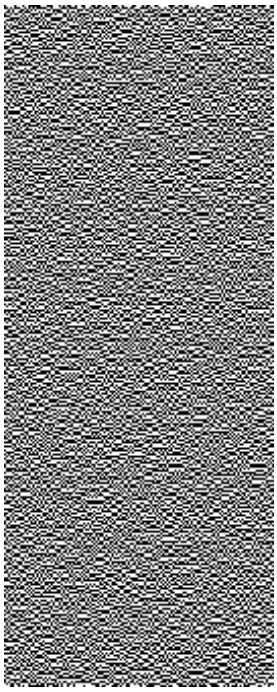
Quando se trata do modelo desenvolvido por Naor e Shamir no artigo *Visual Cryptography* (1994) é preciso estar ciente de que essa foi a primeira técnica de Criptografia Visual implementada, onde a partir do desenvolvimento desta técnica foi possível a criação de outras pesquisas e trabalhos que permitiram a evolução da Criptografia Visual.

Este modelo consiste na transformação de um segredo, que está em forma de imagem (figura 20), em outras *n* imagens separadas (figuras 21 e 22) onde esse segredo só poderá ser recuperado caso o usuário tenha posse dessas *n* imagens e realize a sobreposição das mesas.

Figura 20. Segredo

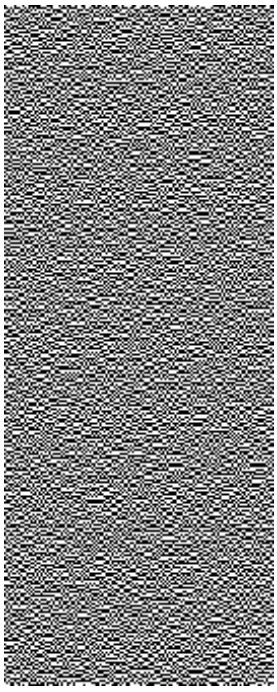
Fonte. Autoria própria, (2020)

Figura 21. Imagem n1



Fonte. Autoria própria, (2020)

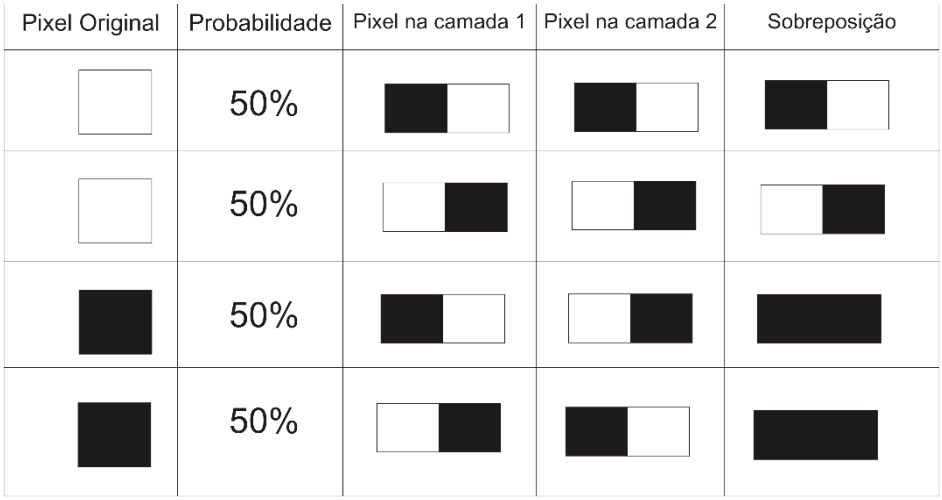
Figura 22. Imagem n2



Fonte. Autoria própria, (2020)

Partindo do princípio de que a imagem a ser criptografada é uma imagem que está em preto e branco e que o segredo será dividido em outras duas imagens, onde estas duas imagens ou camadas são criadas pelo algoritmo de criptografia e preenchidas com base no esquema de pixels exibido na Figura 23.

Figura 23. Esquema de divisão de pixels criado por Naor de Shamir



Fonte. Autoria própria, (2020)

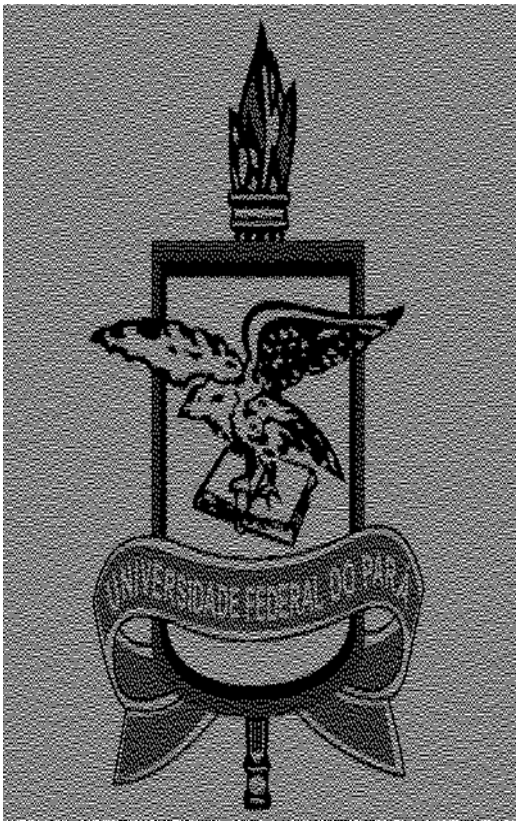
Todo o processo ocorre com a divisão dos pixels pretos e brancos representados por 1 e 0 respectivamente. Como é possível observar na figura, em qualquer uma das duas possibilidades de conversão do pixel branco o pixel resultante (Sub-pixel 1 || Sub-pixel 2) sempre será um sub-pixel preto e branco ou branco e preto, esse resultado, quando interpretado pelo sistema visual humano é visto como uma cor cinza, dado o tamanho pequeno e a proximidade que estes pixels estão um do outro. Essa cor cinza formada pela divisão dos pixels brancos é a cor que ficará no fundo da imagem.

Quando se trata dos pixels pretos, é possível observar que estes são de cores complementares, isso faz com que em qualquer um dos dois casos o sub-pixel resultante sempre seja preto. Esse pixel preto é responsável pela exibição do segredo na imagem secreta, ele também é conhecido como pixel de informação.

Todo o processo de criptografia para a sobreposição dos compartilhamentos toma como base a função “or” da lógica booleana, ou seja, se um pixel branco (0) em um compartilhamento se sobrepõe a outro pixel branco (0) o resultado será um pixel branco (0) e se um pixel preto (1) em um compartilhamento e sobrepuser a um pixel branco (0) ou preto em outro compartilhamento, o resultado será um pixel preto (1). Além do mais é importante ressaltar que imagens quando originalmente estão em preto e branco resultam em um segredo recuperado de maior qualidade em relação às imagens coloridas que criptografadas diretamente como é possível perceber nas figuras a seguir.

.

Figura 24. Imagem colorida criptografada



Fonte. Autoria própria, (2020)

Figura 25. Imagem preto e branco criptografada

Fonte. Autoria própria, (2020)

No entanto, uma das características da técnica é que ao realizar o processo de criptografia e consequentemente a divisão de um pixel em um conjunto de dois sub-pixels a imagem acaba ficando distorcida, “esticada”, com o dobro de altura da imagem original como é possível observar nas figuras 24 e 25.

O modelo de Criptografia Visual de NAOR e SHAMIR (1994) pode ser dividido em dois esquemas: Esquema *k out of k* e esquema de *k out of n:*

Na metodologia (*k out of k*) conhecida também como (2,2) a imagem original é dividida em duas partes onde caso uma pessoa possua apenas um destas partes não poderá revelar quaisquer informações sobre a imagem original, a revelação só ocorre quando há a sobreposição de todas as parcelas que foram criadas durante o processo de criptografia.

Já o esquema (*k out of n*) foi desenvolvido para que fosse mais flexível para o usuário, pois através deste não é necessário ter todos os compartilhamentos gerados para que o segredo seja revelado. Neste esquema podem ser gerados *n*

compartilhamentos da imagem original onde essa imagem poderá ser recuperada, apenas com uma quantidade mínima de compartilhamentos, ou seja, apenas se *k* ou mais compartilhamentos forem sobrepostas, se um número de compartilhamentos menor que *k* forem sobrepostos o segredo não poderá ser revelado, desse modo caso o usuário perca um dos *n* compartilhamentos ainda será possível revelar o segredo.

3.7.2 O MODELO RANDOM GRIDS DE KAFRI E KEREN

Implementado em 1997 por Kafri e Keren no artigo *Encryption of pictures and shapes by Random Grids*, o modelo de *Random Grids* surgiu com o objetivo de prover uma melhoria no método de Naor e Shamir no qual ao encriptar um segredo há uma distorção na imagem recuperada em relação a imagem original devido a expansão dos pixels, no modelo de Kafri e Keren o segredo não sofre nenhum tipo de distorção.

Figura 26. Modelo Random Grids de Kafri e Keren

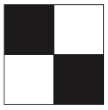
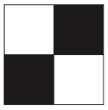
Fonte. Autoria própria, (2020)

O processo realizado para encriptar um segredo usando o modelo de Kafri e Keren, de modo básico, não se difere muito do modelo de Naor e Shamir. Uma imagem I é escolhida para ser enviada; no processo de encriptação I será transformada em duas transparências $T1$, também denominada de grade principal, e $T2$ onde o segredo só poderá ser recuperado com a sobreposição dessas duas transparências e que qualquer uma dessas parcelas separadas não revele nenhuma informação sobre I.

Para corrigir o problema da imagem distorcida “esticada” o método, ao invés de realizar a divisão de um pixel em outros dois subpixels como no método de Naor e

Shamir,este modelo utiliza a divisão de cada um dos pixels em quatro subpixels. Isso faz com que as transparências e o segredo recuperado não fiquem distorcidos, mantendo a proporção de uma imagem quadrada, porém com quatro vezes o tamanho da imagem original. O esquema da subdivisão dos pixels está representado na figura 27.

Figura 27. Divisão em 4 subpixels

Pixel Original	Probabilidade	Pixel na camada 1	Pixel na camada 2	Sobreposição
	50%			
	50%			
	50%			
	50%			

Fonte. Autoria própria, (2020)

A técnica de encriptação pode ser realizada a partir de três métodos diferentes e se dá da seguinte maneira:

Método Ⅰ:

A transparência *T1* é gerada com as mesmas dimensões de *I*, composta por pixels brancos[0] e pretos[1] que são gerados aleatoriamente onde a possibilidade de escolha é de ½ ou 50% para cada cor de pixel, o segundo passo consiste em gerar *T2* com as mesmas proporções de *I*, onde, se o pixel na posição *(i , j)* de *I* for branco então o pixel presente em *(i , j)* em *T2* assume a mesma cor do pixel presente na posição *(i , j)* de *T1*, no caso de o pixel ser preto em *I* na posição *(i, j)* o pixel em *T2* na posição *(i, j)* assume o valor de complemento do pixel (Isso quer dizer que se o pixel em T1 que foi escolhido aleatoriamente for branco, então o valor de complemento em T2 será preto) que está em *T1* na posição *(i, j).*

Método Ⅱ:

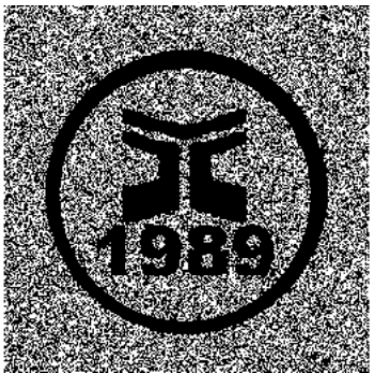
T1 é gerada com as mesmas dimensões de *I*, composta por pixels brancos[0] e pretos[1] que são gerados aleatoriamente onde a possibilidade de escolha é de 50% para cada cor de pixel, o segundo passo consiste em gerar *T2* com as mesmas dimensões de *I*, onde, se o pixel na posição *(i, j)* de *I* for branco então o pixel na posição *(i , j)* de T2 assume a mesma cor do pixel presente na posição *(i , j)* de *T1,* no caso do pixel ser preto, o pixel localizado na posição *(i , j)* de *T2* pode receber a cor branca ou preta, isso é escolhido de forma aleatória pelo algoritmo.

Método Ⅲ:

Gerar *T1* com as mesmas dimensões de *I* composta por pixels brancos[0] e pretos[1] que são gerados aleatoriamente onde a possibilidade de escolha é de 50% para cada cor de pixel, o segundo passo consiste em gerar *T2* com as mesmas dimensões de *I,* onde, se o pixel na posição *(i , j)* de *I* for branco, então o pixel localizado em *T2* na posição *(i , j)* a recebe a cor a branca ou preta escolhida aleatoriamente, e se o pixel em *I* na posição *(i , j)* for preto então *T2* na posição *(i , j)* recebe o valor de complemento do pixel na posição *(i , j)* de T1.

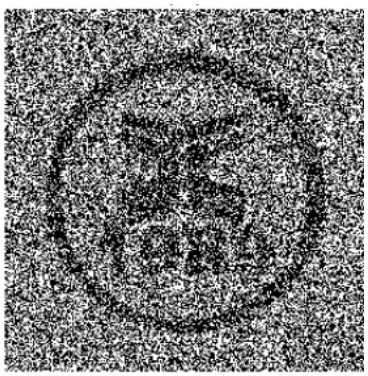
A diferença entre cada um desses métodos está na transmissão de luz nas partes transparentes das imagens, o primeiro método gera uma taxa de 100% de pixels pretos em áreas que devem ser pretas, ou seja, 0% de transparência e 50% de pixels pretos em áreas que devem ser brancas, o segundo método gera uma porcentagem de 75% de pixels pretos nas áreas que devem ser pretas e 50% de pixels pretos na áreas que devem ser brancas e o terceiro método gera 100% de pixels pretos em áreas que devem ser pretas e 75% de pixels pretos em áreas que devem ser brancas. Nas figuras 28, 29 e 30 é possível observar os resultados dos métodos 1, 2 e 3 respectivamente.

Figura 28. Método I



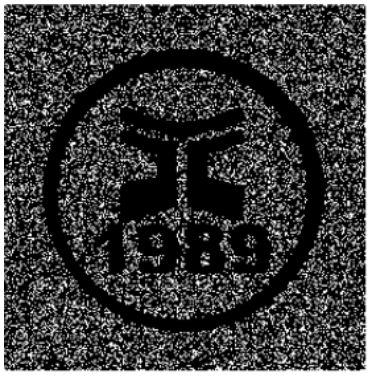
Fonte: Wang e Lee, (2010)

Figura 29. Método II



Fonte: Wang e Lee, (2010)

Figura 30. Método III



Fonte: Wang e Lee, (2010)

CAPÍTULO 4

PROJETO DE UMA FERRAMENTAS BASEADA EM CRIPTOGRAFIA VISUAL PARA COMBATER ATAQUES DE PHISHING

Neste capítulo serão abordadas as principais características, técnicas e ferramentas utilizadas no desenvolvimento do projeto. A Seção 4.1 apresenta uma breve introdução da proposta, na Seção 4.2 é demonstrada uma visão geral do funcionamento da solução proposta. Em seguida, na Seção 4.3, são demonstradas as telas que compõem a proposta. Por fim, na Seção 4.4, são explorados os aspectos técnicos usados no desenvolvimento da proposta.

4.1 INTRODUÇÃO

A informação, desde os primórdios da sociedade tem sido um ativo de imenso valor, para tomadas de decisões e o bom funcionamento de empresas. Mediante a importância atrelada, diversos sistemas de computação surgiram com intuito de auxiliar pessoas e instituições a gerir esse ativo tão importante.

A informatização da sociedade permitiu a resolução de problemas, e agilidade em diversas operações que são consolidadas através do meio digital, porém diante disso criminosos perceberam novas possibilidades para realizar ataques e obter retorno financeiro tirando proveito da imaturidade que muitas empresas têm quando se trata de segurança da informação. Mediante o constante crescimento dessas ameaças surgiu-se a necessidade de criação de uma proposta para a mitigação destes crimes.

4.2 VISÃO GERAL DA PROPOSTA

Este trabalho é inspirado na solução apresentada por PIETZ (2014) apresentado na seção 2.4.

Tomando como base a utilização da câmera dos dispositivos para a sobreposição das parcelas o propósito do trabalho gira em torno do uso da câmera destes dispositivos para exclusivamente identificar e mitigar ataques de phishing, o sistema utilizará uma técnica para a geração de tokens que possibilitará o usuário

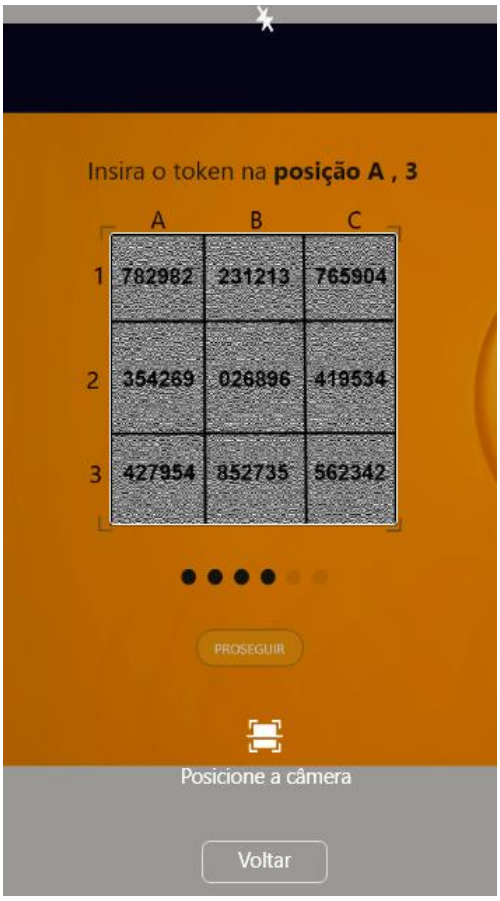
identificar se uma página é fraudulenta ou não. A seguir será possível observar em mais detalhes o funcionamento da proposta em questão.

A ferramenta proposta faz uso da técnica de criptografia visual onde um segredo será dividido em *n* partes de modo que não seja possível identificar esse segredo de posse de apenas *n-1* das partes. O sistema exibe uma tabela com tokens assim que o usuário sobrepõe duas imagens, sendo que, um compartilhamento vai estar no seu dispositivo móvel e outra estará contida no website. A sobreposição ocorrerá através da câmera do dispositivo.

O processo de envio da parcela para o usuário funcionará através de um aplicativo da instituição, que estará previamente instalado no dispositivo, partindo do princípio de que o sistema enviará a transparência para o dispositivo móvel com toda a segurança necessária.

Ao realizar a sobreposição e visualizar a tabela com tokens é solicitado ao usuário um dos tokens exibidos onde a posição do mesmo será dada através das coordenadas de linha e coluna que serão exibidas no monitor. A sobreposição ocorrerá da seguinte maneira como mostra a figura 31.

Figura 31. Sobreposição da tabela de tokens



Fonte. Autoria própria, (2020)

Para que o usuário possa dar continuidade ao processo de login, é essencial que o *token* inserido pelo usuário esteja na posição solicitada, somente desse modo será possível passar para a próxima fase, que consiste na inserção de uma senha pessoal que foi criada pelo mesmo previamente no momento do cadastro, a partir disso o usuário poderá prosseguir para a tela de pós login da aplicação e utilizar o serviço normalmente.

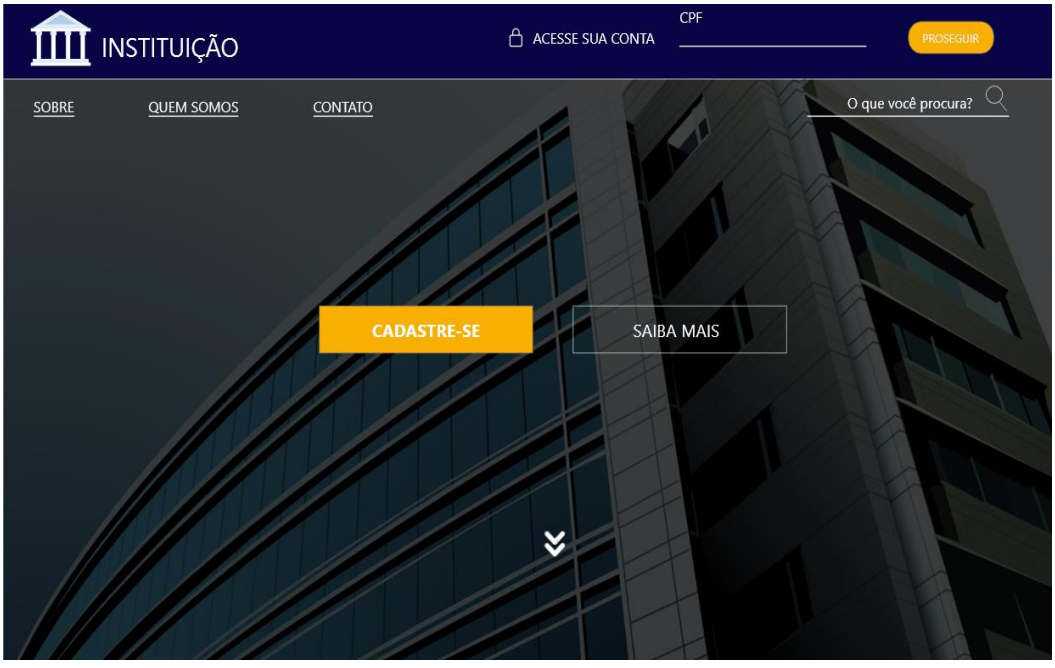
4.3 PROPOSTA DE SOLUÇÃO

Esta proposta visa a facilidade no uso, visto que para que o procedimento seja realizado é necessário somente a sobreposição das parcelas a partir do dispositivo do usuário, portanto com o propósito de detalhar a interface do sistema e como o usuário irá interagir com os elementos e funções que existem na proposta, neste tópico serão demonstradas as telas do sistema.

As telas serão apresentadas com base no passo a passo que normalmente seria realizado por um usuário ao utilizar o sistema, que consiste em: acessar a página inicial do sistema, realizar o cadastro, realizar o download do aplicativo, logar no aplicativo e realizar a sobreposição para visualização do token.

4.3.1 Tela inicial

Figura 32. Tela inicial

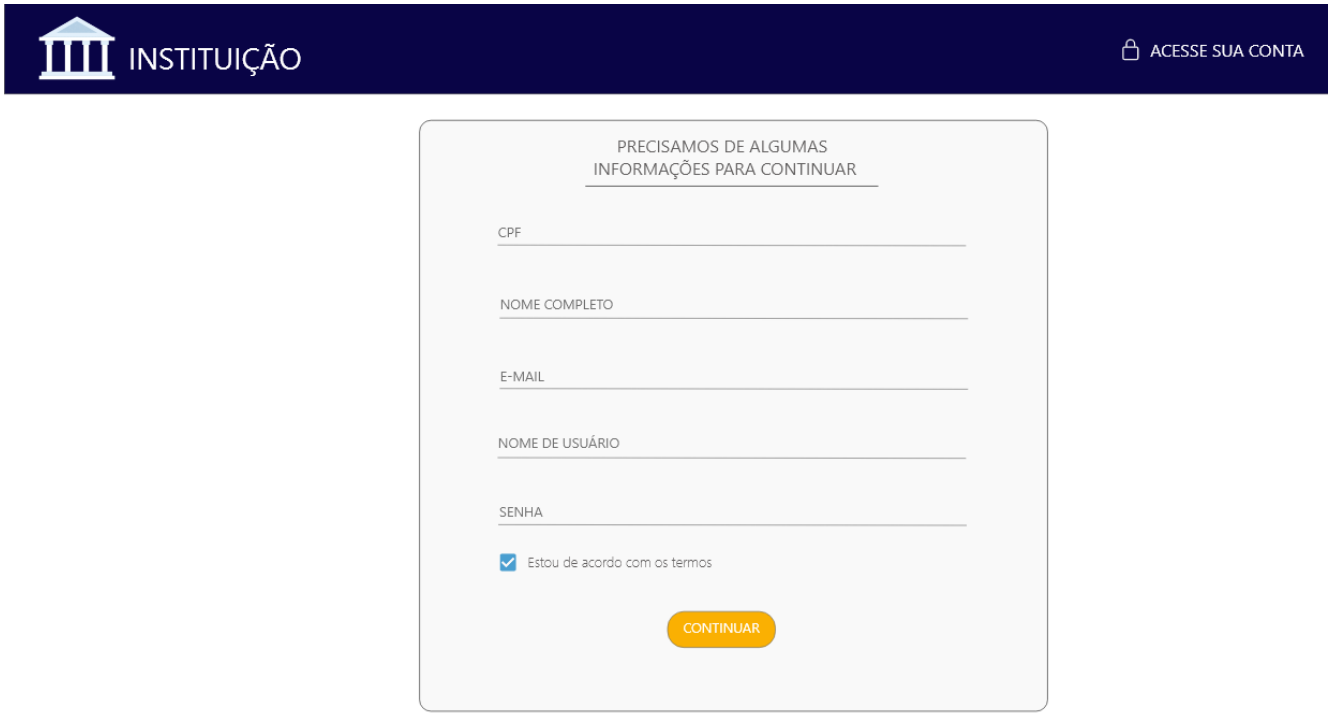


Fonte. Autoria própria, (2020)

Ao acessar o sistema da instituição esta será a página inicial exibida para o usuário, onde será possível efetuar o cadastro ou login no sistema, levando em consideração que o usuário ainda não tenha realizado seu cadastro estes serão os passos a serem seguidos:

4.3.2 Realizar o cadastro

Figura 33. Tela de cadastro

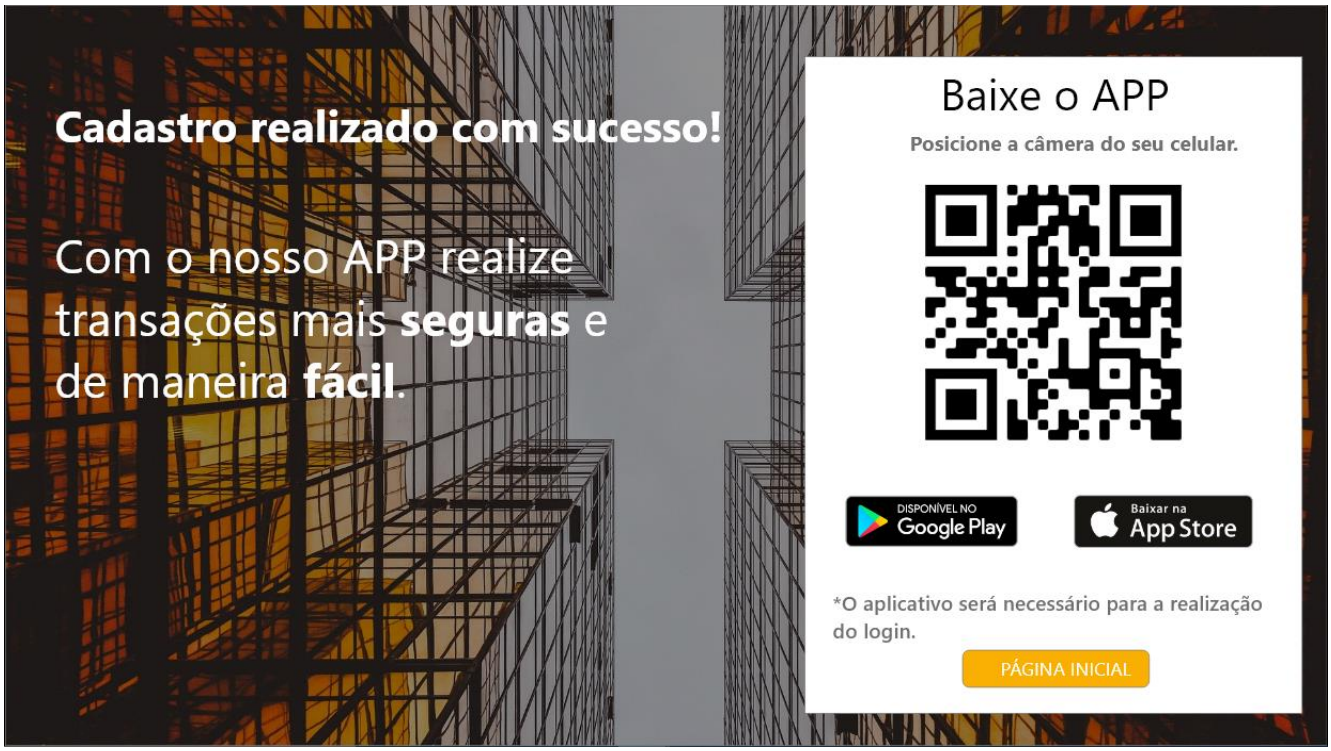


Fonte. Autoria própria, (2020).

Nesta tela serão solicitadas as informações básicas para o cadastro e podem variar de acordo com a instituição.

4.3.3 Realizar o download do APP

Figura 34. Baixar APP



Fonte. Autoria própria, (2020).

Ao apontar a câmera para o código QR será possível estar realizando o download do APP, desse modo será possível realizar o login posteriormente utilizando a criptografia visual com a devida segurança.

Após realizar o cadastro o usuário já poderá utilizar o sistema, neste caso é necessário apenas navegar para a tela inicial do site (Figura 32), inserir o CPF cadastrado e ser direcionado para a tela de inserção do token, como é possível perceber na figura 35.

Para o login na página web, a primeira informação solicitada será o CPF onde funcionará como uma chave primária para que o sistema reconheça aquele usuário e encaminhe uma das parcelas de criptografia para o aplicativo que o usuário possui.

Figura 35. Tela de sobreposição no computador

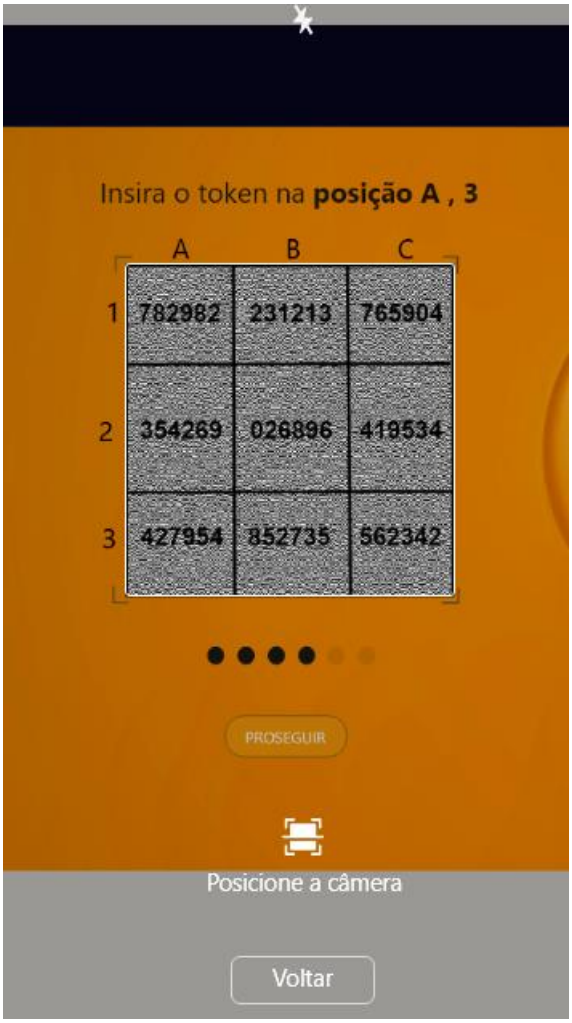
Fonte. Autoria própria, (2020).

Nesta tela é solicitado ao usuário que insira o token que será exibido ao realizar a sobreposição das duas parcelas de criptografia visual, a parcela que é exibida no monitor e a parcela que foi encaminhada para o aplicativo do usuário. O procedimento no aplicativo pode ser visualizado na figura 37.

Figura 36. Tela inicial do APP

Fonte. Autoria própria, (2020).

Figura 37. Tela sobreposição no APP

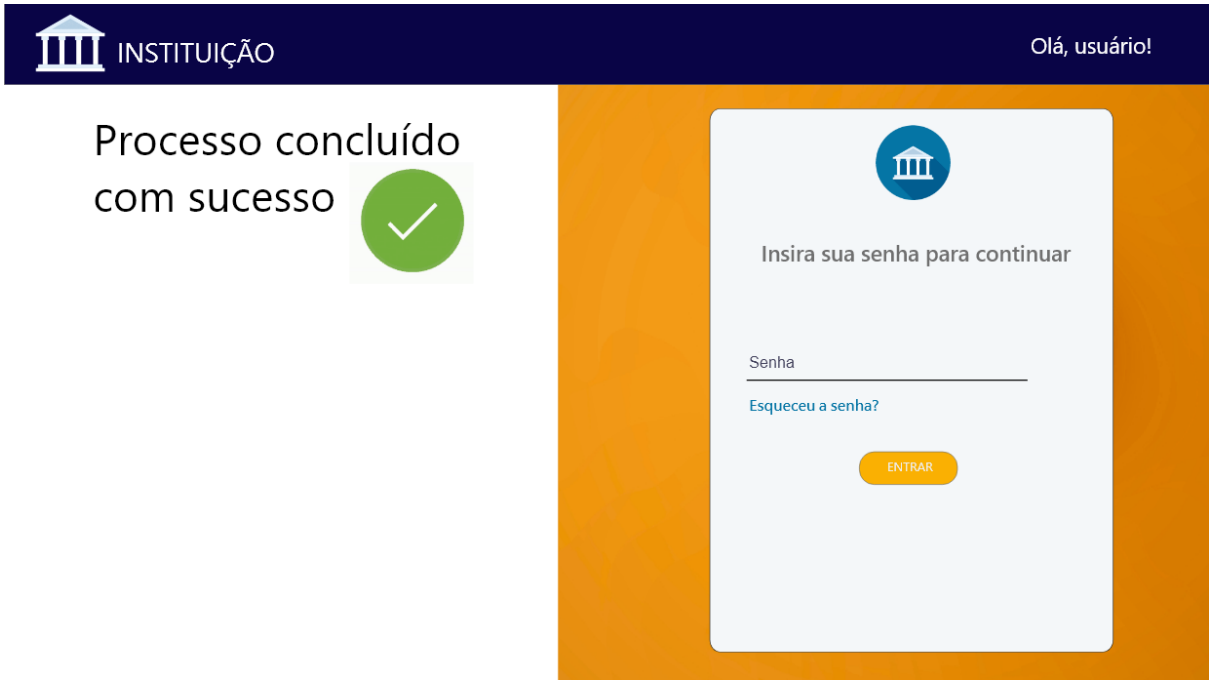


Fonte. Autoria própria, (2020).

Ao clicar no botão “Token” presente na figura 36 o usuário será encaminhado para a tela exibida na figura 37, assim que sobrepuser a parcela que foi encaminhada para o aplicativo com a parcela que está sendo exibida no monitor, os tokens serão exibidos, desse modo o usuário poderá inserir o token da posição solicitada, neste caso o token “427954”.

Ao inserir o token corretamente o usuário é levado para a página onde então poderá inserir sua senha, como é exibido na figura 38.

Figura 38. Tela de inserção de senha



Fonte. Autoria própria, (2020).

Após a inserção do token o usuário pode então prosseguir para realizar a inserção de sua senha de maneira segura, mitigando consideravelmente ataques de phishing.

Focando na segurança e facilidade de uso esta proposta elimina necessidades de memorização de *captchas*, conceito apresentado nas propostas de JAMES E PHILIP (2012) e CHAUDHARI *et. al* (2019) visto que pode ser muito custoso para usuário memorizar uma sequência de caracteres aleatórios.

Além da dispensabilidade da memorização de informações extras também não é necessário o armazenamento de parcelas de criptografia visual nos dispositivos, o que evita perdas por roubos ou exclusões acidentais, outro ponto a ser considerado é a mobilidade do usuário já que este poderá realizar o procedimento em dispositivos não pessoais sem a necessidade de transportar compartilhamentos ou realizar uploads de imagens para a validação.

Outros fatores levados em consideração foram atributos técnicos da segurança da informação, a proposta proporciona um aumento na proteção contra ataques que usam *keyloggers, screenloggers e man-in-the-middle.*

Keylogger de acordo a CERT.BR, (2017) são dispositivos ou programas usados para a leitura de teclas digitadas a fim de roubar senhas e informações confidenciais, pois ainda que haja o roubo da senha do usuário será necessária a autenticação através dos tokens.

Em ataques que também usam *screenloggers* onde segundo a CERT.BR, (2017) são programas capazes de armazenar a posição do cursor e a tela apresentada no monitor, o ataque poderá ser mitigado pois se houver no computador em questão não será possível visualizar a tabela com tokens devido ao fato de ser apresentado somente um dos compartilhamentos.

Man-in-the-Middle (Homem no meio) conforme KASPERSKY, (2013) é um ataque onde um invasor se posiciona entre duas partes que tentam se comunicar (ex: banco e cliente) e intercepta dados os dados que são enviados, partindo do princípio de que um atacante consiga capturar um dos compartilhamentos que é enviado para o usuário no momento do login o uso deste não será possível visto que de posse de apenas um compartilhamento não é possível revelar quaisquer informações sobre o segredo.

4.4 PROJETO DE IMPLEMENTAÇÃO DA PROPOSTA

Para melhor documentação e exemplificação nesta seção serão apresentados detalhes relativos à implementação focando na demonstração das técnicas e recursos utilizados.

Dentre estes detalhes serão apresentados os diagramas onde será possível observar e entender de maneira mais clara sobre o funcionamento do sistema e suas características, serão apresentadas também trechos de códigos com algumas funções do sistema. Os diagramas apresentados serão:

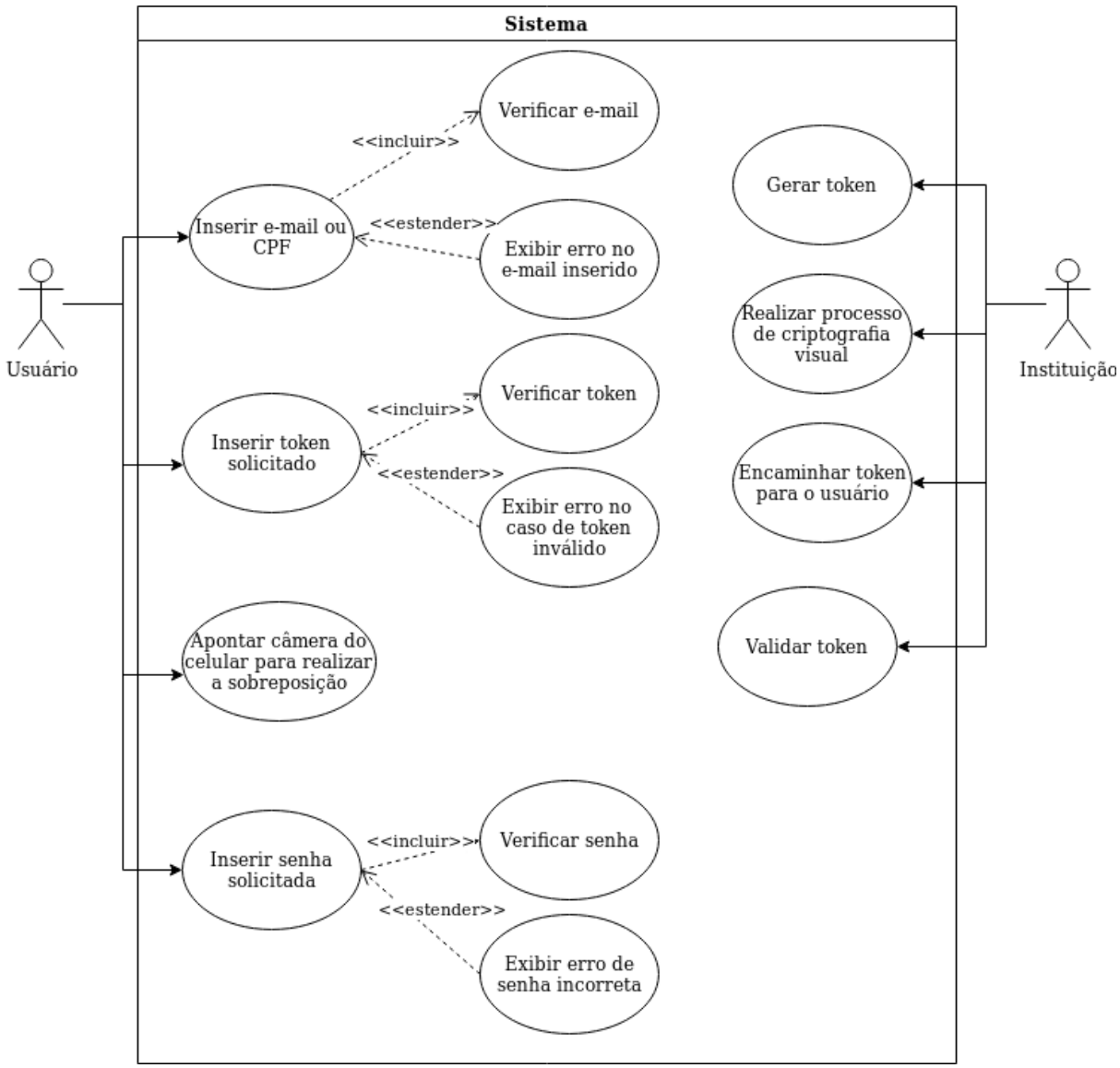
4.4.1 Diagramas de funcionamento do sistema

Serão abordados os diagramas de caso de uso e fluxogramas.

4.4.1.1 Diagrama de caso de uso

Neste diagrama são apresentadas as funcionalidades básicas do sistema e como ocorre a interação dos usuários com as mesmas.

Diagrama 1. Casos de uso



Fonte. Autoria própria, (2020).

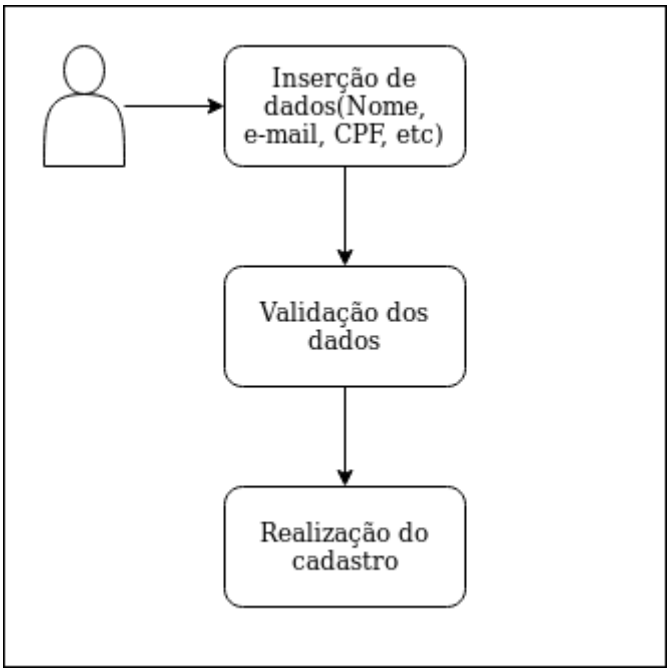
Para acessar o sistema o ator do tipo usuário deverá, como pré-condição, estar com o aplicativo da instituição baixado em seu dispositivo e deverá também estar na página web de acesso ao sistema, dado que estas condições foram atendidas o usuário poderá iniciar o processo de acesso ao sistema.

Em relação ao ator do tipo instituição, como pré-condição, será necessário apenas estar com o sistema disponível e operante para o usuário para que todo o processo ocorra como esperado.

4.4.1.2 Fluxogramas de registro e login

A arquitetura do sistema é dividida em duas fases: a fase de registro, e a fase de login. Na primeira fase o usuário irá inserir informações básicas de registro solicitados pela instituição como: nome, e-mail, CPF, contatos e outros dados que forem solicitados pela instituição, o processo é bem simples e não há necessidade de realizar uploads de imagens ou gravar *captchas*, portanto não se difere de outros cadastros que são comumente realizados em outros sistemas apresentados neste trabalho. O processo pode ser observado no diagrama 02.

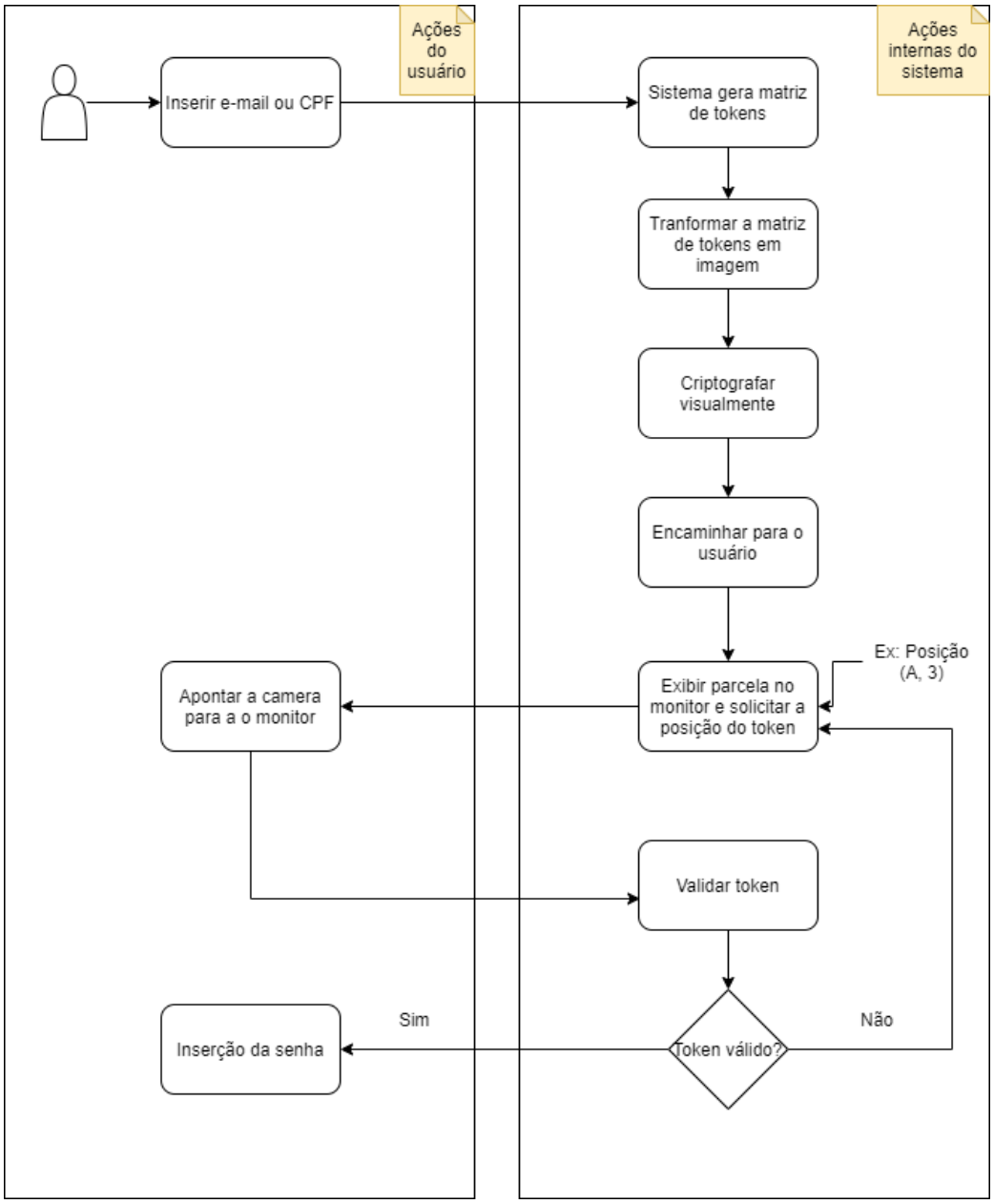
Diagrama 2. Fase de registro



Fonte. Autoria própria, (2020).

Após a realização do cadastro o usuário poderá realizar o login no sistema, onde será realizado de fato o processo de verificação daquele sistema e a constatação de que não se trata de uma página de phishing, como explicado anteriormente nesta fase será necessária a utilização de um aplicativo da instituição em questão onde uma das parcelas de criptografia visual será recebida. O processo pode ser visualizado no diagrama 3**.**

Diagrama 3. Fase de login



Fonte. Autoria própria, (2020).

4.4.2 Funções detalhadas

Nesta seção serão apresentados os detalhes da implementação da proposta. Apesar da proposta apresentada ser somente um protótipo não funcional, as funções consideradas como principais foram desenvolvidas a fim de exemplificar como seria o funcionamento real do sistema. Quanto a linguagem de programação, a escolhida foi

Python, que dentre as outras linguagens existentes foi a que apresentou um código fonte mais sucinto e de melhor entendimento.

As funções que serão apresentadas: Geração da tabela com os tokens, processo de criptografia visual da tabela, e preparação para o uso do segredo.

4.4.2.1 Geração da tabela com os tokens

A construção da tabela terá como base uma matriz de tamanho 3x3 na qual totaliza nove posições onde os *tokens* serão alocados, cada *token* gerado possuirá o tamanho de seis dígitos que podem se repetir entre si, para o processo de geração foi escolhida a função *SystemRandom()* do *Python* onde conforme a documentação são gerados valores criptograficamente seguros a partir de fontes do próprio sistema operacional, o que impede que estes valor gerados sejam reproduzidos posteriormente. O processo de criação da matriz e a geração dos números aleatórios está representada na figura 39.

Figura 39. Processo de criação da matriz de tokens

```
7   systemRandom = random.SystemRandom()
8   matriz = [[0,0,0], [0,0,0], [0,0,0]]
9   for l in range(0, 3):
10      for c in range(0, 3):
11          matriz[l][c] = (systemRandom.randint(100000,999999))
12  l = randint(0,2)
13  c = randint(0,2)
14  token = matriz[l][c]
```

Fonte. Autoria própria, (2020).

Na linha 7 é definida a função para gerar valores aleatórios criptograficamente seguros, onde logo na linha conseguinte está sendo representado o processo para a criação da matriz 3x3, nas linhas de 9 a 11 é realizado o preenchimento da matriz com os valores inteiros gerados aleatoriamente. A partir da linha 12 é definida a posição da linha e coluna na qual o *token* escolhido se encontra, essa informação ficará armazenada na variável chamada “*token”.*

A partir do momento em que a matriz já está preenchida com os valores aleatórios, a próxima etapa consiste na geração da tabela em si. Para que isso aconteça o sistema carrega um modelo de tabela que já está predefinido e desse modo preenche com tokens quem foram gerados, este processo pode ser visualizado na figura 40.

Figura 40. Processo de criação da tabela de tokens

```
20  imagem=Image.open('index.jpg').convert("RGB")
21  draw = ImageDraw.Draw(imagem)
22  string = str(matriz)
23
24  for l in range (0, 3):
25    for c in range(0, 3):
26
27      draw.text((55, 53),str(matriz[0][0]), (0, 0, 0))
28      draw.text((155, 53),str(matriz[0][1]), (0, 0, 0))
29      draw.text((255, 53),str(matriz[0][2]), (0, 0, 0))
30      draw.text((55, 103),str(matriz[1][0]), (0, 0, 0))
31      draw.text((155, 103),str(matriz[1][1]), (0, 0, 0))
32      draw.text((255, 103),str(matriz[1][2]), (0, 0, 0))
33      draw.text((55, 153),str(matriz[2][0]), (0, 0, 0))
34      draw.text((155, 153),str(matriz[2][1]), (0, 0, 0))
35      draw.text((255, 153),str(matriz[2][2]), (0, 0, 0))
```

Fonte. Autoria própria, (2020).

A função responsável por realizar todo o processo é a chamada *ImageDraw* que pertence a biblioteca PIL (*Python Imaging Library*) na qual é possível realizar procedimentos para criação e manipulação de imagens em duas dimensões. Dentro do intervalo da linha 27 a 35 são definidos os parâmetros para a escrita dos *tokens* na tabela, o primeiro parâmetro faz referência as coordenadas X,Y do *token* na imagem, o segundo trata-se do índice na matriz e o terceiro define a cor em RGB. O resultado deste processo está representado na figura 41.

Figura 41. Tabela gerada com tokens

	A	B	C
1	524618	975802	113198
2	410404	952518	465364
3	681884	790706	101330

Fonte. Autoria própria, (2020).

4.4.2.2 Processo de Criptografia Visual da tabela

A fase de criptografia visual ocorre através de um *script* chamado *viscrypt* do autor PHILIPP TROMMLER (2016), através deste é possível realizar a criptografia visual da tabela gerada anteriormente, este modelo usa a técnica desenvolvida por Naor e Shamir, portanto a questão da expansão de pixels não está sendo tratada e desse modo os compartilhamentos resultantes possuirão o dobro de altura da imagem original. O sistema recebe a imagem da tabela gravada com os *tokens* e realiza a divisão desta imagem em outras duas.

O processo pode ser observado nas figuras 42, 43 e 45.

Figura 42. Preparação dos compartilhamentos

```
7   def two_of_two(filename):
8
9       original = Image.open(filename)
10
11      original = original.convert("1")
12      o_pixels = original.load()
13
14      first = Image.new("1", (original.size[0], original.size[1] * 2))
15      f_pixels = first.load()
16
17      second = Image.new("1", (original.size[0], original.size[1] * 2))
18      s_pixels = second.load()
```

Fonte. Autoria própria, (2020).

Nas linhas 11 e 12 ocorre o processo de conversão da tabela em pontilhamentos de preto e branco, o objetivo é preparar a tabela para o processo de criptografia facilitando a divisão dos pixels posteriormente, no intervalo de linhas 14 a 18 é realizada a criação de duas novas imagens que serão os dois compartilhamentos, essas imagens terão o dobro de altura para agregar os pixels expandidos.

Na figura 34, entre as linhas 23 e 43 é onde de fato ocorre o processo de

Figura 43. Processo de criptografia visual

```
20      for i in range(original.size[0]):
21          for j in range(original.size[1]):
22              if o_pixels[i,j] == 0:
23                  if random.randint(0, 1):
24                      f_pixels[i,j * 2    ] = 1
25                      f_pixels[i,j * 2 + 1] = 0
26                      s_pixels[i,j * 2    ] = 0
27                      s_pixels[i,j * 2 + 1] = 1
28                  else:
29                      f_pixels[i,j * 2    ] = 0
30                      f_pixels[i,j * 2 + 1] = 1
31                      s_pixels[i,j * 2    ] = 1
32                      s_pixels[i,j * 2 + 1] = 0
33              else:
34                  if random.randint(0, 1):
35                      f_pixels[i,j * 2    ] = 0
36                      f_pixels[i,j * 2 + 1] = 1
37                      s_pixels[i,j * 2    ] = 0
38                      s_pixels[i,j * 2 + 1] = 1
39                  else:
40                      f_pixels[i,j * 2    ] = 1
41                      f_pixels[i,j * 2 + 1] = 0
42                      s_pixels[i,j * 2    ] = 1
43                      s_pixels[i,j * 2 + 1] = 0
```

Fonte. Autoria própria, (2020).

criptografia com a divisão de cada um dos pixels da tabela, os zeros e uns são as cores branco e preto respectivamente, a figura 39 apresenta o esquema de combinações dos pixels para um melhor entendimento desse processo.

Figura 44. Esquema de combinação dos pixels

Pixel Original	Probabilidade	Pixel na camada 1	Pixel na camada 2	Sobreposição
	50%			
	50%			
	50%			
	50%			

Fonte. Autoria própria, (2020).

4.4.2.3 Preparação para o uso do segredo

Na criptografia visual os pixels pretos são um fator determinante para a qualidade na recuperação do segredo, estes pixels são conhecidos como pixels de informação pois é através deles que é possível visualizar o segredo, já os pixels brancos funcionam como uma base para toda informação contida nos compartilhamentos. Após o processo de criptografia visual estes compartilhamentos são gerados com pixels brancos e não transparentes o que tornaria impossível a sobreposição através de métodos digitais como câmeras.

Nesta etapa os compartilhamentos que foram gerados na fase de criptografia visual são preparados de modo em que seja possível realizar a sobreposição e visualizar o segredo através da câmera de um dispositivo. Para isso o sistema utiliza um script para transformar todos os pixels brancos dos compartilhamentos em pixels transparentes. Na figura 45 é possível observar o funcionamento script.

Figura 45. Transformação dos pixels brancos em transparentes

```
4   def convertToPNG():
5       img = Image.open('./segredo.png')
6       img = img.convert("RGBA")
7       data = img.getdata()
8       newData = []
9       for item in data:
10          if item[0] == 255 and item[1] == 255 and item[2] == 255:
11              newData.append((255, 255, 255, 0))
12          else:
13              newData.append(item)
14      img.putdata(newData)
```

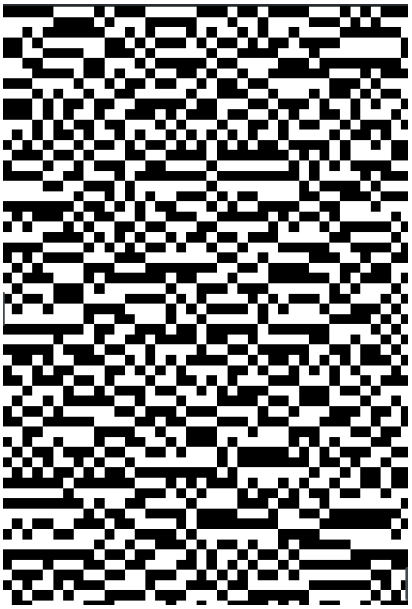
Fonte. Autoria própria, (2020).

O script converte o compartilhamento para o sistema de cores R,G,B,A (*red, green, blue, alpha)* percorre pelo compartilhamento e identifica cada pixel branco como é possível observar na linha 10, após a identificação, este pixel é transformado em um pixel transparente (linha 11) através do quarto parâmetro que representa o índice de opacidade da cor, no caso zero. Nas figuras 46 e 47 é possível notar a

Fonte. Autoria própria, (2020).

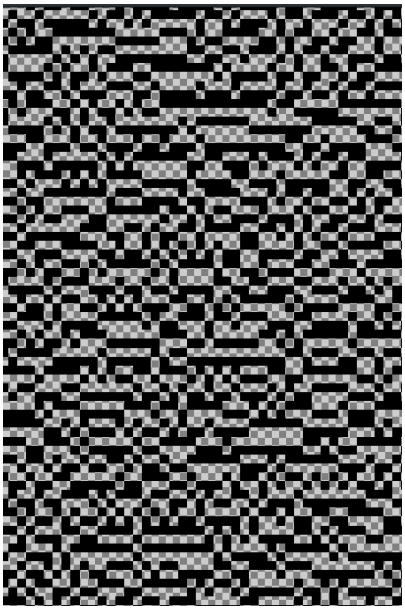
diferença do antes e depois do uso do script.

Figura 46. Compartilhamento com pixels brancos



Fonte. Autoria própria, (2020).

Figura 47. Compartilhamento com pixels transparentes



Fonte. Autoria própria, (2020).

CAPÍTULO 5

CONSIDERAÇÕES FINAIS

Percebendo as grandes proporções que os crimes envolvendo phishing tem tomado, este trabalho teve como objetivo apresentar uma ferramenta de proteção. Dessa forma, ele adiciona uma barreira a mais de segurança entre o atacante e o usuário.

Ao longo do desenvolvimento da pesquisa foi possível concluir que criminosos têm desenvolvido as mais diversas técnicas a fim de obter ganhos sobre pessoas e empresas contornando muitas vezes as regras de segurança criadas. Portanto é imprescindível estar sempre investindo no desenvolvimento de técnicas que visam a proteção ao usuário e a mitigação destes ataques.

Percebeu-se que utilização da técnica de criptografia visual unida a utilização de tokens para a validação das operações propõe ao usuário uma experiência mais agradável e segura ao navegar na internet visando a diminuição da incidências de crimes de phishing, além disso a oportunidade de realizar a validação através de dispositivo móvel possibilita uma maior flexibilidade para usuário tornando o processo o mais simples e seguro possível possibilitando que até mesmo usuários menos experientes consigam utilizar a ferramenta.

Por outro lado, desafios durante a implementação desta proposta em um ambiente real podem surgir. Como apresentado na seção 3.1 os humanos, em geral, são o ponto mais fraco da segurança, portanto certamente é necessário investir recursos na conscientização e treinamento do usuário para que este possa usufruir da ferramenta de maneira correta, um ponto interessante seria levar em consideração a gerencia do fator humano como um dos pilares da segurança da informação, ademais também se faz necessário a implementação de hardware adicional para processamento das parcelas de criptografia visual, o que pode tornar um infraestrutura mais robusta.

Além disso, foi possível constatar que para um fortalecimento ainda maior da segurança da informação também é necessário levar em consideração a gerencia do fator humano como um dos pilares da segurança da informação.

No que tange a criptografia visual, foi analisado ainda que, para garantir o melhor uso do sistema, deve-se usar imagens estejam em preto e branco resultando em um segredo recuperado de maior qualidade em relação às imagens coloridas, para a fonte usada na exibição dos tokens é recomendável usar negrito com o tamanho da

fonte ocupando a maior área possível de cada célula da tabela. Além disso, é indicado que seja utilizado o modelo Random Grids de Kafri e Keren (1997) para que não haja a expansão dos pixels, assim evitando a distorção no segredo recuperado em relação a imagem original.

É importante observar que os trechos de códigos apresentados foram desenvolvidos apenas com o objetivo de exemplificar o funcionamento das partes consideradas com principais para o sistema e apesar de serem funcionais não são apropriadas para uso comercial, pois não foram testadas com este propósito.

Ao longo da realização deste estudo foi possível observar os esforços que estão sendo tomados para a mitigação do phishing no Brasil e no mundo, entretanto apesar de existirem diversas técnicas e métodos para evitar este tipo de crime é importante ter ciência de que os atacantes estão sempre criando novos tipos de ataques, portanto é fundamental que os estudos na área continuem dessa forma reduzindo ao máximo as incidências de phishing e tornando a internet um lugar mais seguro para todos.

4.1 TRABALHOS FUTUROS

Espera-se que esta pesquisa venha servir de base para trabalhos futuros que poderão ser desenvolvidas nesta área, para dar continuidade a esta pesquisa seria interessante o desenvolvimento da aplicação para os dispositivos móveis e para plataforma web, outro ponto a ser considerado seria a implantação do alinhamento automático de parcelas para facilitar a sobreposição para o usuário.

O capítulo 4 apresentou o projeto de uma ferramenta para combater ataques de phishing. No entanto, a ferramenta não foi totalmente implementada. Assim, como trabalho futuro propõem-se o desenvolvimento da aplicação para os dispositivos móveis e para plataforma web. Além disso, propõem-se a implantação do alinhamento automático de parcelas para facilitar a sobreposição para o usuário.

Nesse sentido, levar em consideração o controle de exceções da aplicação também é um tópico que pode ser explorado, aspectos como o tempo para a expiração da tabela de tokens caso por exemplo um usuário inserisse o CPF de outra pessoa que também faz uso da aplicação, ou o que aconteceria caso o usuário inserisse o token incorretamente muitas vezes, poderiam tornar a utilização da aplicação mais viável e segura para o usuário.

REFERÊNCIAS

KASPERSKY. **35% dos brasileiros não sabem como proteger sua privacidade online**. 2019. Disponível em: https://www.kaspersky.com.br/about/press-releases/2019_digital-privacy-fatigu. Acesso em: 29 out. 2020.

WIKIPEDIA. **Alfabeto Russo**. 2019. Disponível em: https://pt.wikipedia.org/wiki/Alfabeto_russo. Acesso em: 20 out. 2019.

ALVES, Cássio. **Segurança Da Informação Vs. Engenharia Social:** Como se proteger para não ser mais uma vítima. 2010. Disponível em: https://monografias.brasilescola.uol.com.br/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm. Acesso em: 17 set. 2019.

BRASIL. **Cartilha de Segurança:** Phishing. 2017. Disponível em: https://cartilha.cert.br/golpes/. Acesso em: 16 out. 2019.

CHAUDHARI, Megha et al. Phishing Attack Prevention Using Visual Cryptography. **International Journal of Advanced Research in Computer and Communication Engineering**. n. 4, ed. 8, 4 abr. 2019. Disponível em: https://ijarcce.com/wp-content/uploads/2019/05/IJARCCE.2019.8428.pdf. Acesso em: 24 abr. 2020.

CIALDINI, Robert. **Influence:** The Psychology of Persuasion. 1. ed. 2006. v. 1.

COMER, Douglas E. **Internetworking with TCP/IP** – Volume I: Principles, Protocols and Architecture. Fourth Edition. Prentice Hall, 2015.

CRESPO, Marcelo; SYDOW, Spencer**. Novas Tendências da Criminalidade Telemática.** 2010. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/viewFile/41656/40852. Acesso em: 17 out. 2020.

NORTON. **Cyber Safety Insights Report Global Results**. 2019. Disponível em: https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018_Norton_LifeLock_Cyber_Safety_Insights_Report_US_Media_Deck.pdf?promocode=DEFAULTWEB%20. Acesso em: 29 out. 2020.

DHILLON, Gurpreet; BACKHOUSE, James. **Information System Security Management in the New Millennium**. 2000. Disponível em: https://www.researchgate.net/publication/242104189_Technical_opinion_Information_system_security_management_in_the_new_millennium. Acesso em: 26 mar. 2019.

BRASIL. **NBR ISO/IEC 17799:2000. 2000**. Disponível em: https://www.informabr.com.br/nbr.htm. Acesso em: 17 set. 2019.

JAMES, Divya; PHILIP, Mintu. A novel anti phishing framework based on Visual Cryptography. **International Journal of Distributed and Parallel Systems**, v. 3, ed.

1, 1 jan. 2012. Disponível em: https://www.researchgate.net/publication/254023502_A_Novel_Anti_Phishing_Framework_Based_On_Visual_Cryptography. Acesso em: 23 abr. 2020.

KAFRI, O; KEREN, E. **Encryption of pictures and shapes by Random Grids. Optics Letters**, v. 12, ed. 6, 1987. Disponível em: https://www.researchgate.net/publication/26800062_Keren_E_Encryption_of_pictures_and_shapes_by_random_grids_Opt_Lett_12_377-379. Acesso em: 30 abr. 2020.

INVASÃO. **Kevin Mitnick explica o que é engenharia social**. 2010. Disponível em: http://www.invasao.com.br/2010/02/01/kevin-mitnick-explica-o-que-e-engenharia-social/. Acesso em: 13 set. 2019.

KHATRI, Chaitali *et al*. Phishing detection system using visual cryptography. **Multidisciplinary Journal of Research in Engineering and Technology**. 2015. Disponível em: https://www.researchgate.net/publication/328064154_PHISHING_DETECTION_SYSTEM_USING_VISUAL_CRYPTOGRAPHY. Acesso em: 23 abr. 2020.

MARTINS, Diego. **Phishing Scam:** A fraude do Século 21. 2008. Disponível em: https://securityinformationnews.files.wordpress.com/2014/02/phishing_scam.pdf. Acesso em: 17 out. 2020.

MEIRELLES, Fernando. **Brasil tem 424 milhões de dispositivos digitais em uso, revela a 31ª Pesquisa Anual do FGVcia**. 8 jun. 2020. Disponível em: https://portal.fgv.br/noticias/brasil-tem-424-milhoes-dispositivos-digitais-uso-revela-31a-pesquisa-anual-fgvcia. Acesso em: 29 out. 2020.

MOREIRA, Rafael**. O uso do phishing como vetor de ataque na guerra cibernética contemporânea**. 2017. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/4231. Acesso em: 16 out. 2019.

MULIG, Elizabeth; KIMBALL, V. **Phishing, pharming and identity theft**. 2007. Disponível em: https://www.semanticscholar.org/paper/PHISHING%2C-PHARMING-AND-IDENTITY-THEFT-Brody-Mulig/c3f9bedf86614a9ca7cf18197bfbb978f56e6e56?p2df. Acesso em: 16 out. 2019.

NAOR, Moni; SHAMIR, Adi. **Visual Cryptography**. 1994. Disponível em: https://www.cs.jhu.edu/~fabian/courses/CS600.624/NaorShamir-VisualCryptography.pdf. Acesso em: 30 abr. 2019.

NASSARO, Davies**. Engenharia Social Explorando o Fator Humano dos Sistemas de Segurança da Informação**. 2012. Monografia (Especialização em segurança de redes de computadores) - Instituto Voz do Mestres. 2012. Disponível em: https://pt.scribd.com/document/244783660/engenharia-social-explorando-o-fator-humano-dos-sistemas-de-seguranc3a7ada-pdf. Acesso em: 17 set. 2019.

NIL, Yuan *et al*. **IPhishing:** Phishing Vulnerabilities on Consumer Electronics. 2008. Disponível em: https://web.cs.ucdavis.edu/~hchen/paper/upsec2008.pdf. Acesso em: 17 out. 2019.

NORTON. **Norton Cyber Security Insights Report Global Results**. 2017. Disponível em: https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf?promocode=DEFAULTWEB%20. Acesso em: 14 out. 2020.

PAREDES, Gibrán. Introducción a la criptografía. **Revista Digital Universitaria**, v. 7, ed. 7, 10 jun. 2006. Disponível em: http://ru.tic.unam.mx/bitstream/handle/123456789/1105/jul_art55.pdf?sequence=1&isAllowed=y. Acesso em: 26 out. 2019.

PEREIRA, Cleber. **PHISHING:** Conceitos e ações preventivas aplicadas à empresa. 2013. Trabalho de conclusão de curso (Pós graduação em re-des de computadores) - Instituto CEUB de Pesquisa e Desenvolvimento. 2013. Dis-ponível em: https://repositorio.uniceub.br/jspui/bitstream/235/8136/1/50910909.pdf. Acesso em: 16 out. 2019.

PEREIRA, Leandro; MARTINS, Daves. **Engenharia Social:** Segurança Da Infor-mação Aplicada À Gestão De Pessoas - Estudo De Caso. 2014. Disponível em: https://seer.cesjf.br/index.php/cesi/article/download/129/49. Acesso em: 24 set. 2019.

APWG. **Phishing Activity Trends Report**. 12 set. 2019. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf. Acesso em: 14 out. 2019.

ZHENG, Xudong. **Phishing With Unicode Domains**. 14 abr. 2017. Disponível em: https://www.xudongz.com/blog/2017/idn-phishing/. Acesso em: 18 out. 2019.

PIETZ, Franz. **Criptografia Visual:** método de alinhamento automático de parcelas utilizando dispositivos móveis. 2014. Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual de Campinas. 2014. Disponível em: http://repositorio.unicamp.br/jspui/handle/REPOSIP/275550. Acesso em: 24 abr. 2020.

SECURITY REPORT. **Punycode:** quando o que você lê não é onde quer ir. 5 maio 2017. Disponível em: https://www.securityreport.com.br/destaques/punycode-quando-o-que-voce-le-nao-e-onde-quer-ir/#.X694U8hKjIV. Acesso em: 18 out. 2019.

SERAFIM, Vinicius et al. **Técnicas de Segurança da Informação:** da Teoria à Prática. 2017. Disponível em: http://www.segurancalegal.com/wp-content/uploads/2017/09/T%C3%A9cnicas-de-Seguran%C3%A7a-da-Informa%C3%A7%C3%A3o-da-Teoria-%C3%A0-Pr%C3%A1tica.pdf. Acesso em: 8 mar. 2019.

SILVA, Francisco. **Classificação Taxonômica dos Ataques de Engenharia Social**. 2013. Dissertação (Mestrado em Segurança dos Sistemas de Informação) - Universidade Católica Portuguesa. 2013. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/15690/1/Tese%20de%20Mestrado%20-%20Engenharia%20Social.pdf. Acesso em: 12 fev. 2019.

SILVA, Maicon; COSTA, Veridiana. O fator humano como pilar da Segurança da Informação: uma proposta alternativa. **IX Jornada de Ensino Pesquisa e Extensão**

(JEPEX). 2009. Disponível em: https://www.researchgate.net/publication/325273412_O_fator_humano_como_pilar_da_Seguranca_da_Informacao_uma_proposta_alternativa. Acesso em: 17 set. 2019.

STALLINGS, William. **Criptografia e segurança de redes:** Princípios e Práticas – 6. ed. – São Paulo: Pearson Education do Brasil, 2015.