FACULDADE DE TECNOLOGIA ALCIDES MAYA - AMTEC
CURSO TECNOLÓGICO EM REDES DE COMPUTADORES

CÁSSIO DOS SANTOS MOREIRA

GAMIFICAÇÃO COMO SOLUÇÃO DE TREINAMENTO EM CIBERSEGURANÇA NA PREFEITURA MUNICIPAL DE ESTEIO/RS

Porto Alegre
2019

CÁSSIO DOS SANTOS MOREIRA

GAMIFICAÇÃO COMO SOLUÇÃO DE TREINAMENTO EM CIBERSEGURANÇA NA PREFEITURA MUNICIPAL DE ESTEIO/RS:

Projeto de Pesquisa apresentado como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores, pelo Curso Superior de Tecnologia em Redes de Computadores da Faculdade de Tecnologia Alcides Maya - AMTEC

Orientadores: Prof. Esp. Cristiano Goulart Borges

Prof. Fagner Coin

Porto Alegre

2019

AGRADECIMENTOS

Agradeço primeiramente os principais incentivadores por todos os meus projetos de vida, Flávia Beatriz dos Santos e Fernando Eduardo dos Santos, minha mãe e meu tio/dindo/considerado pai, por ter me apoiado durante esta longa jornada, e sempre ter me incentivado a seguir em frente.

Aos meus orientadores, Cristiano Goulart Borges e Fagner Coin, por todo o apoio que recebi durante a realização deste projeto, pelas suas exaustivas correções e grandes incentivos.

Ao professor, Cristiano Goulart Borges, que me incentivou, com suas aulas, a entrar para a área de Segurança de TI e aprofundar sobre estudos na área.

A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

A gamificação está relacionada ao uso de elementos de jogos em contextos não relacionados com jogos e fornece uma alternativa de engajar e motivar os usuários durante o processo de aprendizagem. Diante desse cenário, encontra-se na gamificação os instrumentos para prender a atenção dos funcionários. Este projeto mostra o que a gamificação pode oferecer para atingir um bom processo de ensino.

Palavras-chaves: cibersegurança, educação, gamificação, motivação

ABSTRACT

Gamification is related to the use of game elements in non-game contexts and provides an alternative to engaging and motivating users during the learning process. Given this scenario, gamification is the instrument to hold the employees attention. This project shows what gamification can offer to achieve a good teaching process.

Keywords: cybersecurity, education, gamification, motivation

LISTA DE FIGURAS

Figura 1 – Pergunta para os gestores sobre o conhecimento dos subordinados ….. 7
Figura 2 – Pergunta sobre o uso de pendrives no ambiente corporativo ……. 8
Figura 3 – Política sobre política de segurança da informação ……....11
Figura 4 – Exemplo de arquivos encriptados pelo Dharma ransomware …….. 13
Figura 5 – Arquivo informando a chave para pagar o resgate dos arquivos ……..14
Figura 6 – Exemplo de phishing bancário ……....15
Figura 7 – Exemplo de phishing que foi enviado para a Prefeitura de Esteio …….. 16
Figura 8 – Email falso sobre mensagens do Whatsapp ……..... 16
Figura 9 – Página falsa do Banco do Brasil ……. 17
Figura 10 – Resultado de uma varredura de um PC infectado com Adware ……..... 18
Figura 11 – Contextualização da gamificação ……20
Figura 12 – Conceito de Gamificação …….. 21
Figura 13 – Richard Bartle identificou que há quatro tipos de jogadores …….. 22
Figura 14 - Ações que podem induzir a diversão ……... 23
Figura 15 - Tela inicial da plataforma Hacker Rangers ……..28
Figura 16 - Ranking semanal gerado automaticamente pela plataforma …….... 29
Figura 17 - Exemplo de curso EAD …….. 29
Figura 18 - Sistema de quiz da plataforma …….. 30
Figura 19 - Algumas das medalhas disponíveis na plataforma ……... 31
Figura 20 - Formulário de ciberatitude …… 32
Figura 21 - Dashboard da página de administrador ……... 33
Figura 22 - Tela de gerenciamento de usuários ……..34

Figura 23 - Tela de gerenciamento de cursos 35
Figura 24 - Página de gerenciamento de medalhas 36
Figura 25 - Tipos de Cyber Atitudes 37
Figura 26 - Pergunta da segunda pesquisa para medir o nível de maturidade em segurança 39
Figura 27 - Pergunta referente ao uso de Pen Drive 40
Figura 28 - Comparativo do número de chamados relativos a segurança 41
Figura 29 - Reporte de E-mail suspeito 44
Figura 30 - Usuários reportaram incidentes através do módulo Ciberatitudes 44
Figura 31 - Categoria “Ajudei um Colega” do módulo de Ciberatitudes 45
Figura 32 - Categoria “Ajudei um Colega” do módulo de Ciberatitudes 46

LISTA DE ABREVIATURAS E SIGLAS

AVA	Ambiente Virtual de Aprendizagem
IPTU	Imposto sobre a Propriedade Predial e Territorial Urbana
LGPD	Lei Geral de Proteção de Dados
T.I	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

1. INTRODUÇÃO 10
1.1 Definição do Tema ou Problema 10
1.2 Delimitações do Trabalho 11
1.3 Objetivos 11
1.3.1 Objetivo Geral 12
1.3.2 Objetivos Específicos 12
1.4 Justificativa 12
2. REVISÃO BIBLIOGRÁFICA 14
2.1 Prefeitura Municipal de Esteio/RS 14
2.2 Cibersegurança 15
2.3 Ameaças do cenário 16
2.4 Gamificação 23
2.4.1 Características da Gamificação 24
3. DESCRIÇÃO DA SOLUÇÃO 28
3.1 Plataforma de usuário do Hacker Rangers 28
3.2 Regulamento da campanha do Hacker Rangers 28
3.3 Funcionalidades para os usuários do Hacker Rangers 29
3.3.1 Sistema de Ranking 30
3.3.2 Cursos EAD 31
3.3.3 Quiz 32
3.3.4 Medalhas 32
3.3.5 Cyber Atitude 33
3.4 Funcionalidades para os Administradores do Hacker Rangers 34
3.4.1 Página inicial de Administrador 34
3.4.2 Página de criação de usuários 35
3.4.3 Página de cursos 36
3.4.4 Página de administração de medalhas virtuais 37
3.4.5 Cyber Atitudes 38
4. METODOLOGIA 40
5. VALIDAÇÃO 43
6. CONCLUSÃO 47
7. REFERÊNCIAS BIBLIOGRÁFICAS 49
ANEXO A - BANNER DA COMPETIÇÃO 52
ANEXO B - REGULAMENTO DA COMPETIÇÃO 53
ANEXO C - PRIMEIRA PESQUISA DE SEGURANÇA 56

ANEXO D - SEGUNDA PESQUISA DE SEGURANÇA …….. 64

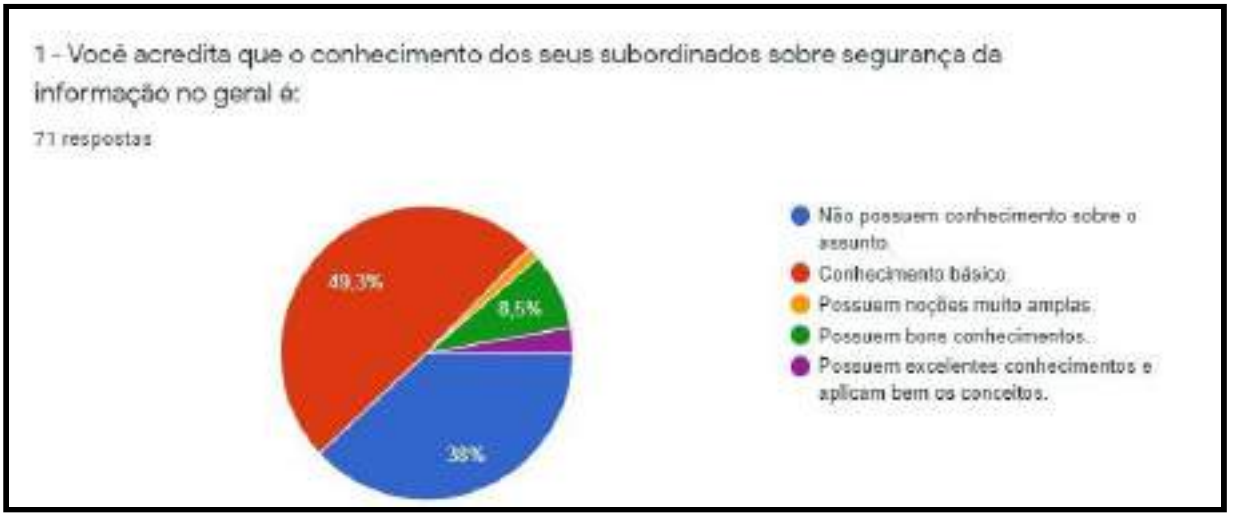
1. INTRODUÇÃO

1.1 Definição do Tema ou Problema

Os usuários internos da Prefeitura Municipal de Esteio têm tido atitudes que comprometem a segurança dos ativos. Por diversas vezes os usuários não abrem chamados com a equipe de TI por não possuírem conhecimento das ameaças, fazendo com que os riscos se tornem maiores e mais frequentes.

A primeira pesquisa , vide figura número 1, mostrou que cerca de 87% dos gestores acreditam que os seus subordinados não possuem ou possuem pouco conhecimento sobre segurança.

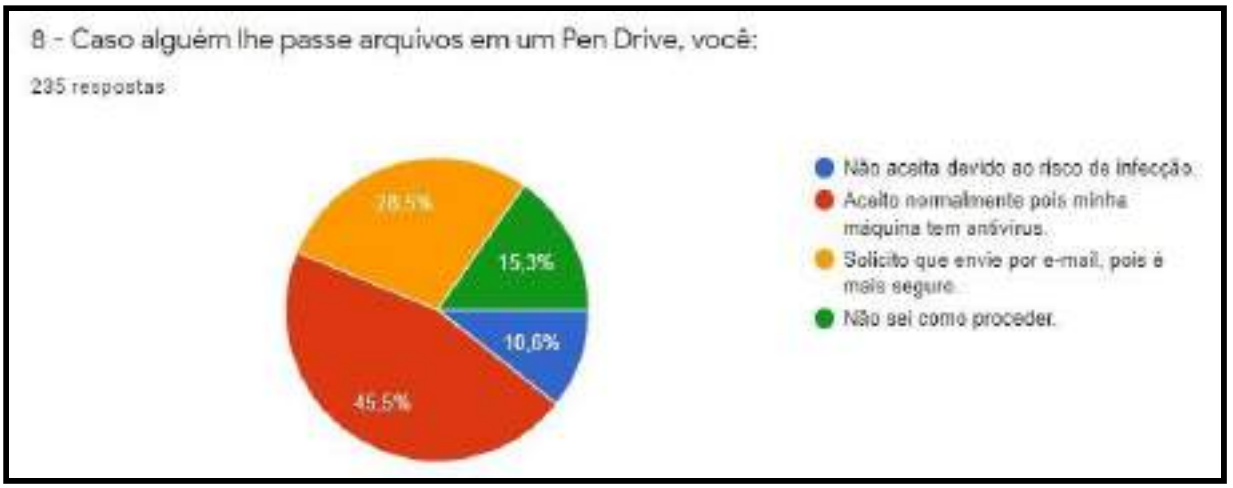
Figura 1 - Pergunta para os gestores sobre o conhecimento dos subordinados



Fonte: Elaborado pelo autor

Outro dado preocupante, vide figura 2, se refere ao uso do pen drive no ambiente corporativo. Esta pergunta foi destinada a todos que responderam o questionário, seja gestor ou não.

Figura 2 - Pergunta sobre o uso de pendrives no ambiente corporativo



Fonte: Elaborado pelo autor

Nesta última pergunta, apenas 10,6% agiria de modo seguro, tendo em vista que receber arquivos por e-mail ou aceitar por ter antivírus não garante a segurança.

Considerando estes e outros problemas recorrentes, por conta da falta de conscientização em segurança e, visando aumentar o nível de maturidade em segurança da informação na prefeitura, propõe-se um Ambiente Virtual de Aprendizagem (AVA) com técnicas de Gamificação como solução para o presente projeto, através da plataforma Hacker Rangers.

1.2 Delimitações do Trabalho

O presente estudo limita-se a realizar estudo ao Hacker Rangers , plataforma que tratou de fornecer materiais relacionados a segurança da informação, abordando assuntos como Boas Práticas em cibersegurança e Lei Geral de Proteção de Dados (LGPD), phishing, engenharia social, criação de Senhas .

1.3 Objetivos

Os objetivos dividem-se em: geral e específicos.

1.3.1 Objetivo Geral

Adaptar um Ambiente Virtual de Aprendizagem (AVA) utilizando técnicas gamificadas na prefeitura municipal de Esteio/RS.

1.3.2 Objetivos Específicos

a) Apontar vantagens do uso da Gamificação no processo de ensino e aprendizagem dos funcionários;
b) Apresentar a plataforma Hacker Rangers como solução viável de gamificação para os funcionários da Prefeitura;
c) Promover a cibersegurança através da plataforma de gamificação e aumentar a maturidade em segurança da informação.

1.4 Justificativa

Se faz necessário fornecer treinamentos para os usuários internos da Prefeitura Municipal de Esteio por conta da falta de instrução dos funcionários.

Uma pesquisa ,que teve o objetivo de apontar os problemas relacionados a segurança, foi realizada com funcionários da instituição onde percebeu-se, que os colaboradores não têm domínio sobre procedimentos internos do ambiente.

De acordo com as respostas fornecidas pelos gestores, somente a minoria possui um bom/excelente conhecimento de segurança, enquanto a maioria tem problemas de compreensão sobre o assunto.

A solução apresentada neste projeto ajudará a conduzir os funcionários a entender como a segurança da informação funciona , e também auxiliará a guiar seus trabalhos de forma mais segura.

O projeto contribuirá para a comunidade acadêmica mostrando uma forma diferenciada de engajar os usuários nos treinamentos de segurança através de um

ambiente virtual de aprendizagem (AVA) com técnicas de gamificação, mostrando a eficiência do mesmo.

2. REVISÃO BIBLIOGRÁFICA

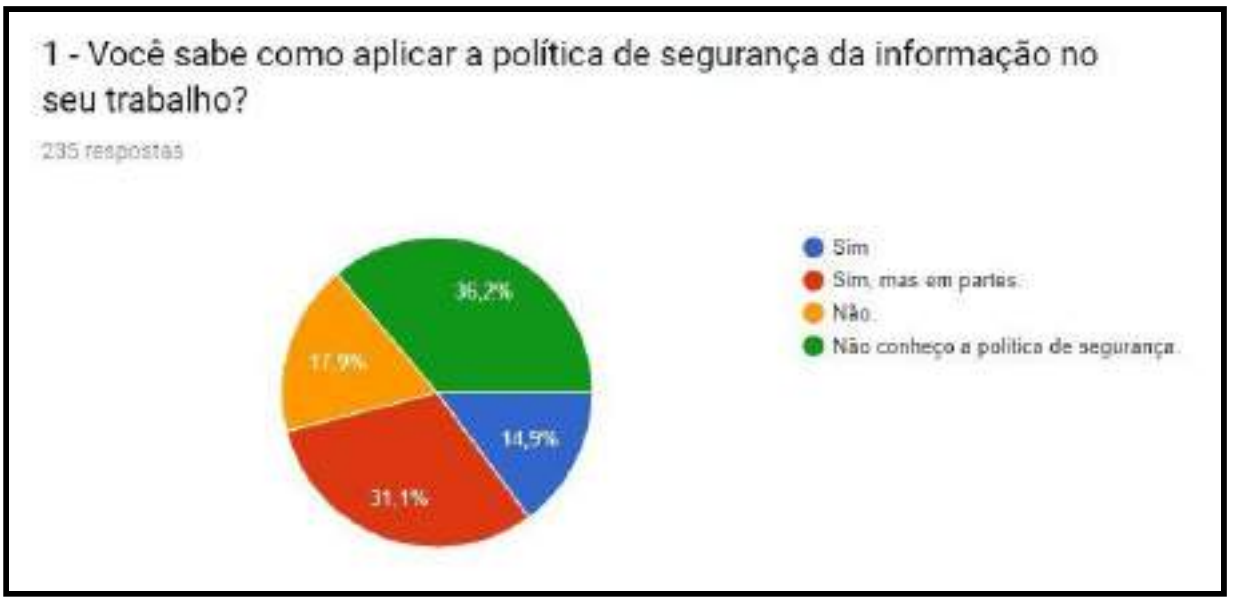
Este capítulo apresenta os conceitos que auxiliarão no entendimento do conteúdo do projeto:

2.1 Prefeitura Municipal de Esteio/RS

Esteio é uma pequena cidade que se tornou independente de São Leopoldo nos anos 50 e se encontra na região metropolitana de Porto Alegre e fica a 20Km da capital. A Prefeitura Municipal de Esteio foi criada 1954 e tem 64 anos. Segundo o site do IBGE(2018), a cidade de Esteio possui a população estimada de 83.121 pessoas.

Atualmente, a prefeitura conta com cerca de 2.300 funcionários que estão divididos entre 11 secretarias,sendo que ela possui apenas um setor dedicado à Tecnologia da Informação e Comunicação e está vinculada à Secretaria Municipal de Administração, os 9 servidores lotados neste setor atuam na área de gestão, desenvolvimento de sistemas, infraestrutura, telecomunicações e suporte técnico. No momento, não há ninguém designado para cuidar da segurança da informação e da rede do órgão, tornando o cenário vulnerável a qualquer ameaça interna e externa. A figura número 3 mostra uma questão da pesquisa feita recentemente na Prefeitura aponta que a maturidade em segurança dos funcionários é baixa. Este é apenas um dado inicial da pesquisa, outras questões desta mesma pesquisa serão aprofundadas no decorrer do projeto.

Figura 3 - Política sobre política de segurança da informação



Fonte: Elaborado pelo autor

A baixa porcentagem de usuários que possuem conhecimento da política mostra que maturidade de segurança da informação não é boa. Apenas 14.9% têm certeza de que conhece totalmente a política.

Os principais problemas do cenário são: senhas fracas dos usuários e sem alterações regulares, tentativas constantes de phishing, ataques de ransomware, senhas anotadas em quadros e perto das estações de trabalho. Com o objetivo de mitigar os riscos de segurança na Prefeitura e em razão do desconhecimento dos usuários de TI, o presente projeto propõe a adaptação de um Ambiente Virtual de Aprendizagem com técnicas de Gamificação para treinamento em cibersegurança.

2.2 Cibersegurança

Segundo a Kaspersky Lab (2018), empresa russa e desenvolvedora de software de segurança para a Internet, cibersegurança é a prática que tem o objetivo de proteger os computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques maliciosos. E ainda afirma que o termo é abrangente e que pode se aplicar a tudo referente a segurança de computadores, recuperação de

desastres e conscientização do usuário final. O termo também pode ser chamado de segurança de tecnologia da informação ou segurança das informações eletrônicas.

Segundo InfoProtect (2017), alguns problemas que podem ocorrer com a falta de cibersegurança, e são eles: perda de dados, roubos de senhas e publicação de informação sigilosa.

De acordo com a CompTIA (2016), empresa de certificação de TI, os erros humanos representam 58% das falhas em segurança contra 42% de erros apontados por problemas técnicos da tecnologia .

2.3 Ameaças do cenário

Um conjunto de ameaças virtuais ou problemas,de diversos tipos, relativos a segurança, foram detectadas na Prefeitura Municipal de Esteio/RS.

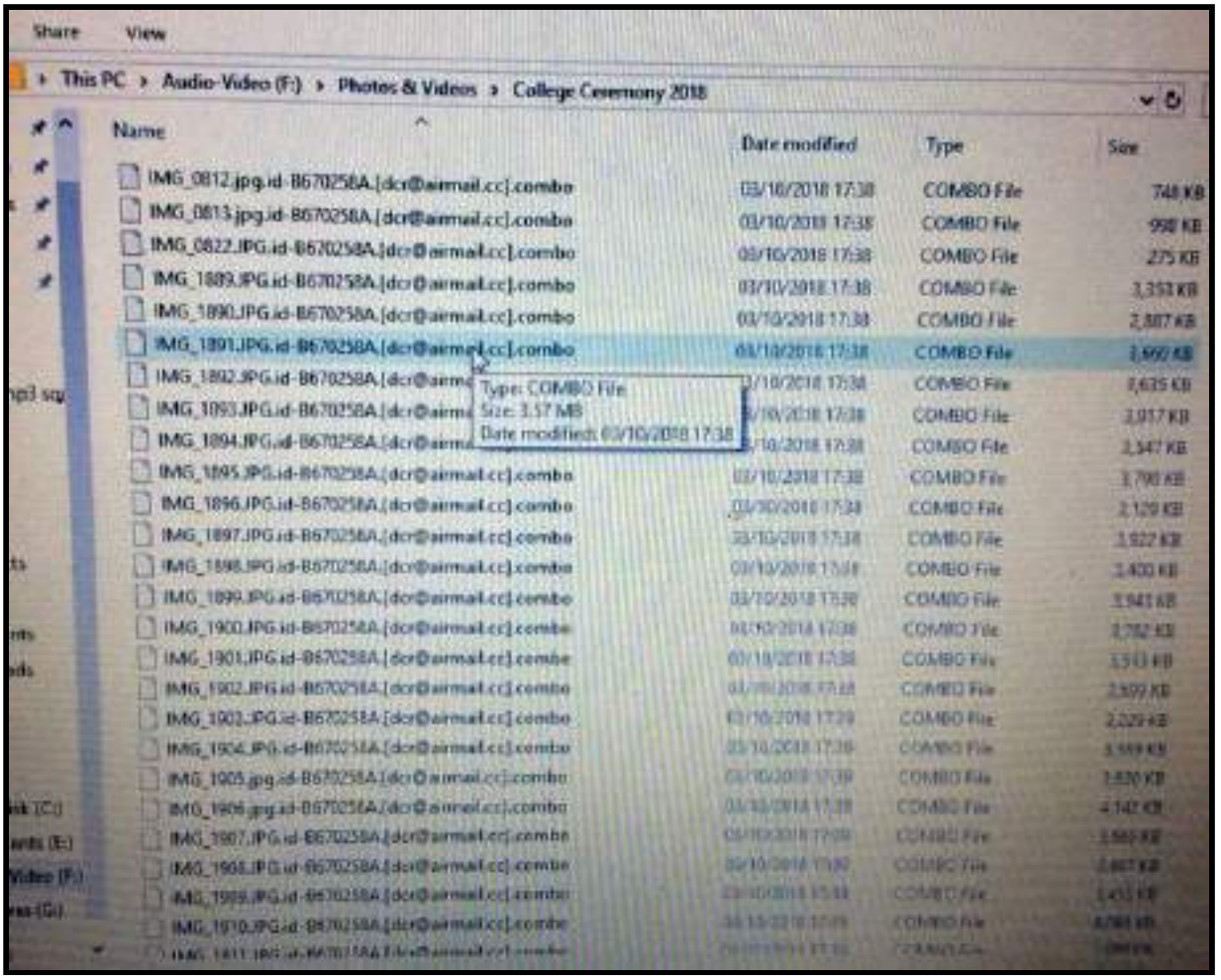
Entre eles:

- Ransomware
- Adware
- Botnet
- Phishing
- Falta de criptografia

Uma das principais ameaças de cibersegurança e um dos motivadores deste projeto é o Ransomware, devido á duas infecções á Prefeitura Municipal de Esteio nos últimos 2 anos. Em 2017 os arquivos das pastas de rede e dos computadores locais foram encriptados pelo WhiteRose e em 2018 pelo Dharma-Combo, ambos ransomware.

A figura número 4 a seguir mostra um exemplo de arquivos encriptados, semelhantemente ao incidente que ocorreu em 2018 na Prefeitura.

Figura 4 - Exemplo de arquivos encriptados pelo Dharma ransomware

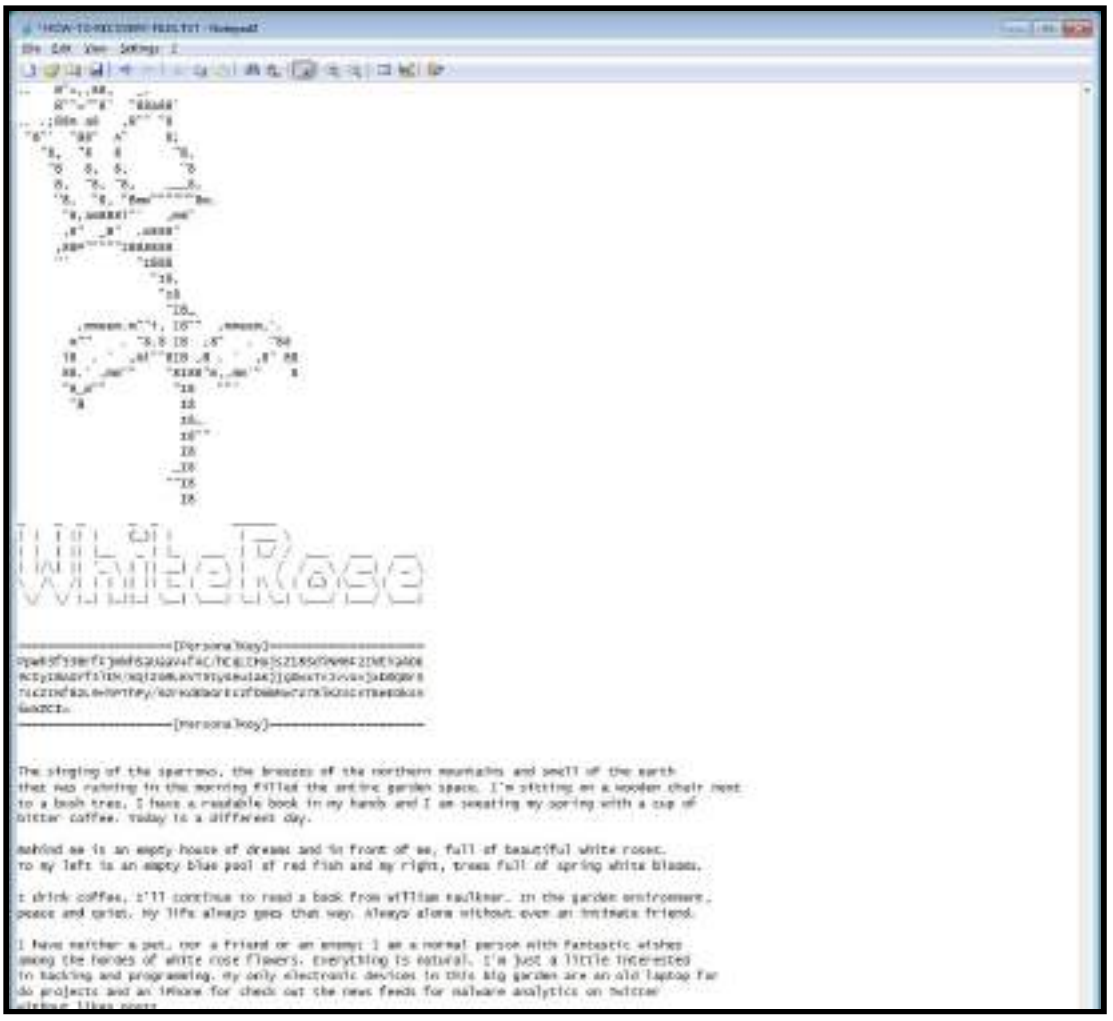


Fonte : soft2secure (2018)

Nos casos da Prefeitura de Esteio, quase 100% dos arquivos que estavam na rede foram encriptados, afetando atributos de segurança da informação como a disponibilidade e integridade, porém poucos arquivos foram perdidos por conta do servidor de backup. Uma característica deste tipo de ataque é que sempre é solicitado dinheiro para resgatar estes arquivos, neste caso, após o ataque, foi gerado o arquivo chamado FILES ENCRYPTED.txt, contendo informações de como efetivar o pagamento ao sequestrador virtual, geralmente exigindo o pagamento em Bitcoins, por conta da dificuldade de rastrear o cibercriminoso.

A figura de número 5 mostra um exemplo mostra este mesmo tipo de arquivo, só que desta vez acompanhado do WhiteRose ransomware.

Figura 5 - Arquivo informando a chave para pagar o resgate dos arquivos.



Fonte: Enigma Software (2018).

De acordo com o site Enigma Software (2018), após a infecção é gerado o arquivo “HOW-TO-RECOVERY-FILES.TXT”, instruindo o usuário infectado a realizar o pagamento para resgatar os seus arquivos. Com o pagamento em bitcoin é impossível de rastrear e o sequestrador dos dados, e o mesmo não garante a devolução dos arquivos após o pagamento.

Outra ameaça constante no cenário é o phishing. Pessoas mal intencionadas se passam por técnicos em TI, bancos e até mesmo por outros funcionários a fim de roubar informações sigilosas. Os métodos mais usados são: telefonemas e e-mails falsos.

Conforme o site da Avast (2018), a definição é: Phishing é uma maneira desonesta que cibercriminosos usam para enganar as pessoas a revelar

informações pessoais. Como por exemplo: senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos. As figuras de números 6, 7 e 8 mostram alguns exemplos de phishing que foram enviados para os e-mails funcionais dos servidores da Prefeitura.

Figura 6 - Exemplo de phishing bancário

Fonte - Google Imagens (2019)

Figura 7 - Exemplo de phishing que foi enviado para a Prefeitura de Esteio

Fonte: Elaborado pelo autor

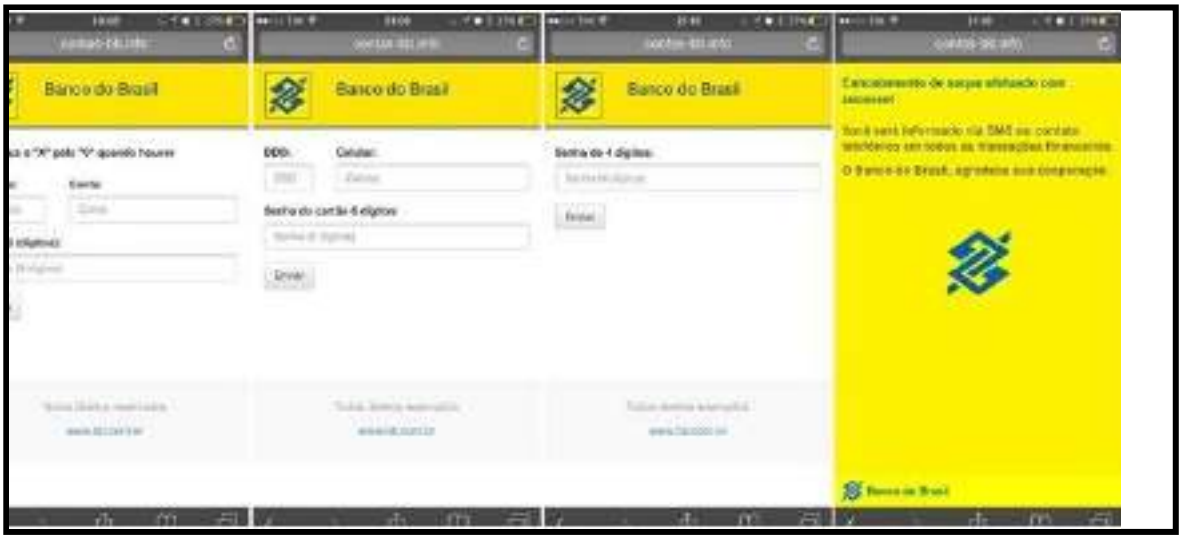
Figura 8 - Email falso sobre mensagens do Whatsapp

Fonte: Elaborado pelo autor

Nas figuras anteriores, mostram que os cibercriminosos tentaram se passar pelos sistemas do Banco do Brasil, Correios e Whatsapp com o objetivo de simular uma comunicação oficial e roubar os dados. Na figura 6 , após clicar em

recadastramento, o usuário é levado à uma página falsa do banco.A figura de número 9 mostra um exemplo de página falsa que foi criada pelos criminosos.

Figura 9 - Página falsa do Banco do Brasil

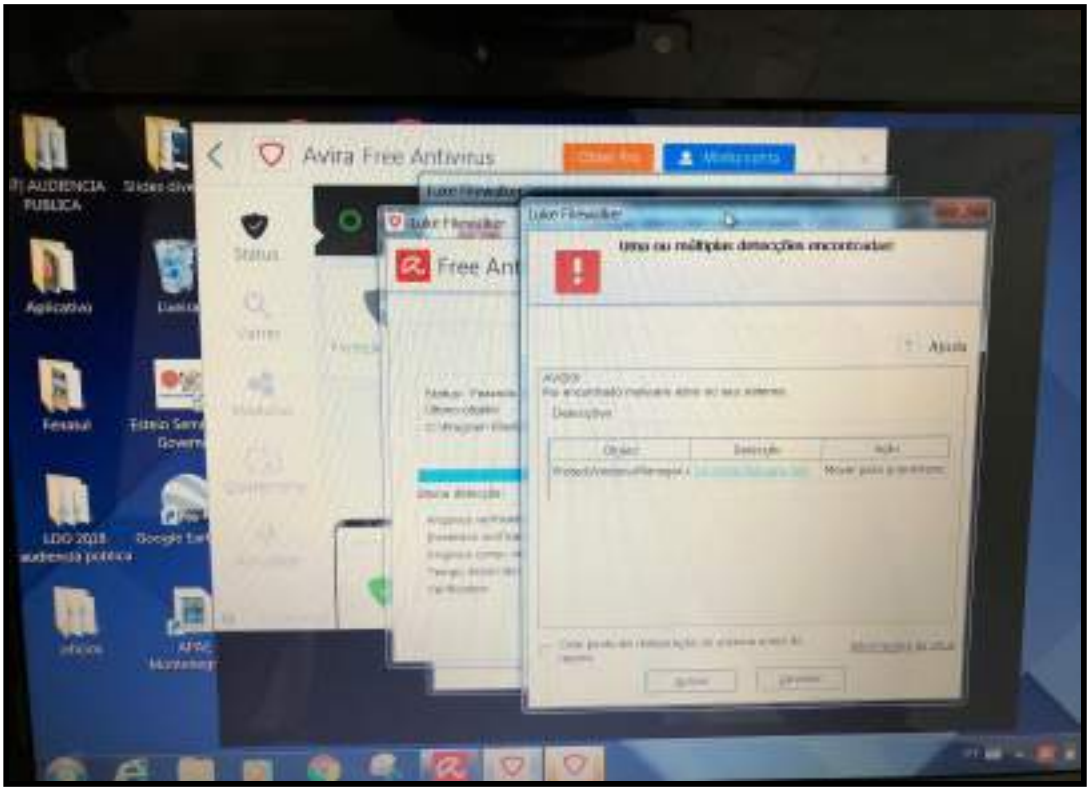


Fonte:Tecmundo (2017)

Antes da Adaptação do Hackers Rangers, os casos de phishing só eram reportados ao setor de TIC somente depois de algum incidente de segurança, tanto em contas de e-mail privadas quanto corporativas.

Outra ameaça que aparece consecutivamente nos computadores da Prefeitura é o Adware. Conforme o site TecMundo(2008) o termo vem do inglês (**ad**=anúncio,soft**ware**=programa),e mostram propagandas e anúncios sem que o usuário autorize a sua exibição. A figura de número 10 mostra o resultado de uma varredura do Avira Antivirus em um dos computadores infectados com a praga.

Figura 10 - Resultado de uma varredura de um PC infectado com Adware



Fonte: Elaborada pelo autor

As soluções de proteção gratuitas, conforme mostra a figura, conseguem detectar esta praga e proteger o usuário final.

De acordo com o livro Segurança da Informação Princípios e Controle de Ameaças (2014), a criptografia serve para alterar os dados originais, que são chamados de texto simplificado, em algo que é aparentemente ilegível e aleatório, conhecido por texto cifrado. Esta técnica é um dos principais métodos de segurança utilizado para proteger a informação contra os riscos associados ao princípio da confidencialidade.

A falta do uso de criptografia no cenário ainda é uma realidade da Prefeitura. Na plataforma há questões relacionadas á criptografia e sua importância para que os usuários tenham conscientização deste método de proteção de dados.

Por conta do decreto de número 5069 de 2014, oriunda da Prefeitura de Esteio , a criptografia não poderá ser aplicada nos memorandos online. Mas não impõe nenhum impeditivo nos e-mails corporativos e outros sistemas.

2.4 Gamificação

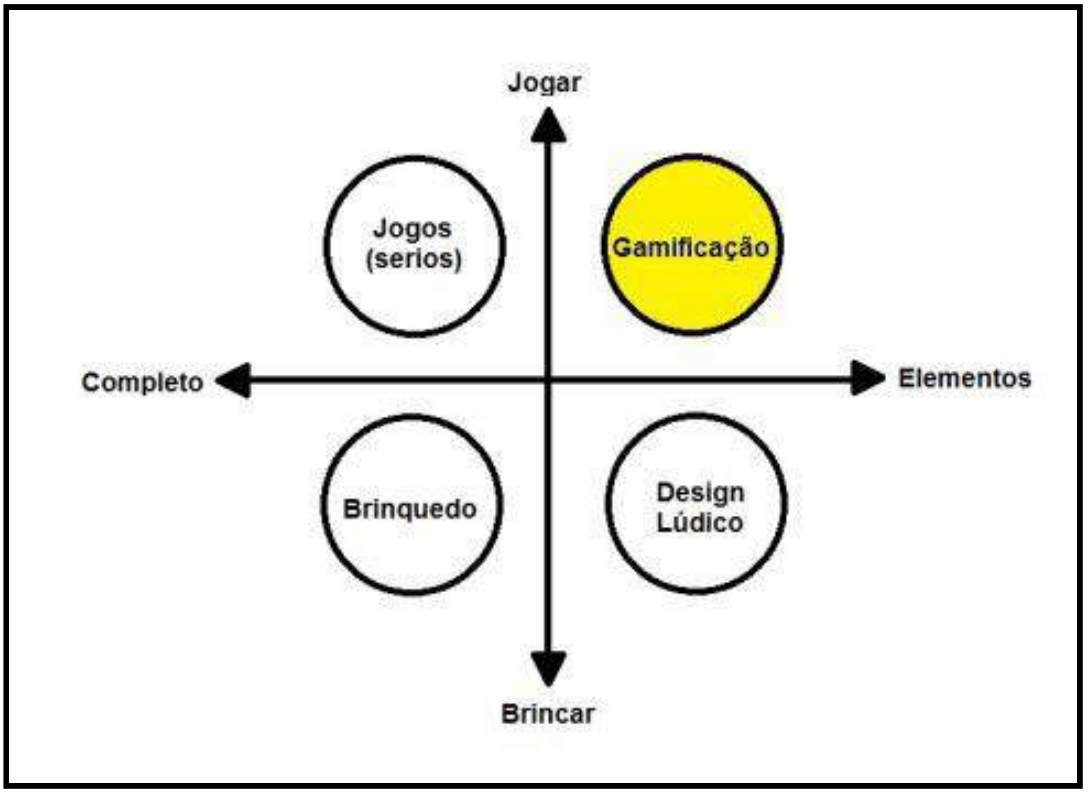
Neste trabalho serão utilizadas técnicas de gamificação para conscientizar e engajar os usuários, encontra-se abaixo o que significa Gamificação do ponto de vista de um dos autores.

> Gamificação é um sistema utilizado para a resolução de problemas através da elevação e manutenção dos níveis de engajamento por meio de estímulos à motivação intrínseca do indivíduo. Utiliza cenários lúdicos para simulação e exploração de fenômenos com objetivos extrínsecos, apoiados em elementos utilizados e criados em jogos. (BUSARELLO, 2016, p.18).

O conceito parte do princípio de se pensar e agir como se estivesse em um jogo, mas em contexto fora de um.

A gamificação abrange a utilização de mecanismos e sistemáticas de jogos para a resolução de problemas e para a motivação e o engajamento de determinado público (VIANNA et al., 2013). A figura 11 mostra a contextualização da gamificação.

Figura 11 - Contextualização da gamificação.



Fonte: (DETERDING et al., 2011).

A gamificação é encontrada, hoje em dia, em inúmeras áreas. Exemplos: produtividade na indústria, finanças, saúde, entretenimento, sustentabilidade e na educação. (KLOCK, CARVALHO, ROSA, GASPARINI, 2014).

O gráfico da figura 12 a seguir mostra o conceito da Gamificação.

Figura 12 - Conceito de Gamificação.

Fonte: Oniria

Como é possível observar na figura acima, a Gamificação é projetada como um game e possui elementos do mesmo, mas ainda faltam alguns conceitos ,como por exemplo ser usado como um game e ser usado apenas para diversão, para que se torne um game.

2.4.1 Características da Gamificação

De acordo Vianna et al. (2013), há quatro características de mecânicas que são básicas para montar um ambiente de gamificação: meta, regras, sistema de feedback e participação voluntária. Segue abaixo a explicação das características:

1)A meta é o motivo pelo qual o indivíduo realiza a atividade.

2)As regras determinarão o modo que o usuário agir para concluir os desafios

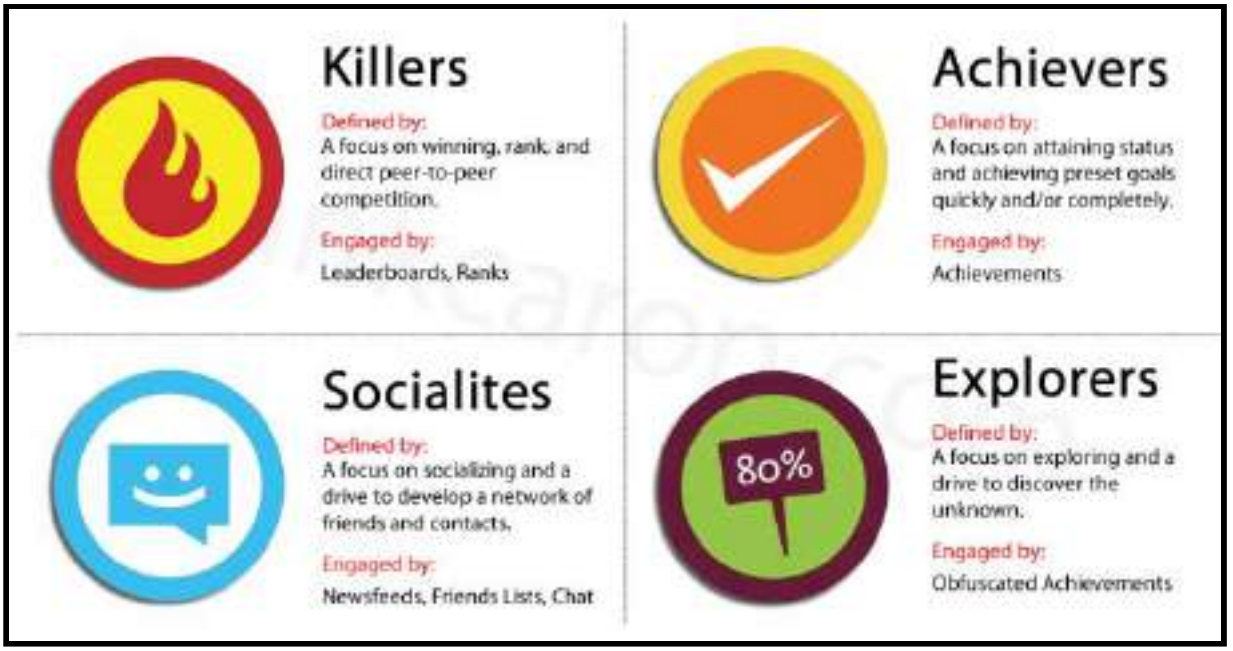
da plataforma.

3)O sistema de feedback mostra ao usuário o quanto ele está avançando em relação a meta da plataforma.Fazendo com que o indivíduo siga sempre orientado.Todo o feedback é em tempo real.

4)A participação voluntária estabelece que só há a real interação se o usuário estiver disposto a se relacionar com a plataforma.

Richard Allan Bartle , pesquisador de jogos, apontou através de um estudo chamado de arquipélago de Bartle que existem quatro tipo de jogadores que são encontrados na execução dos jogos, são eles: Killers (Assassinos), Achievers (Conquistadores ou Empreendedores), Socialites (Socializadores) e Explorers (Exploradores).

Figura 13 - Richard Bartle identificou que há quatro tipos de jogadores



Fonte : Techtudo (2016)

Conforme o site Techtudo (2016), para os socializadores o fator que mais importa é a interação com os outros usuários, ou seja, desenvolver uma network, seja dentro ou fora do game. Os exploradores gostam de sondar o jogo inteiro e descobrir coisas novas,seja o seu cenário, seus personagens ou curiosidades. Os

conquistadores são os indivíduos que tendem a concentrar riquezas, pontos e conquistas dentro do jogo. Os assassinos adoram vencer os outros usuários e/ou ambiente do game, a fim de mostrar que é superior através de suas habilidades.

O fator diversão não é necessário em uma plataforma “gamificada”, porém se mostra muito efetiva, portanto, deve ser uma das métricas para o sucesso (FADEL, L. ET AL., 2014).

A figura de número 14 fala um pouco do que a plataforma precisa para induzir o usuário final a se divertir e melhorar a experiência do aprendizado.

Figura 14 - Ações que podem induzir a diversão

Nome	Descrição
Analisar idade do público alvo	A diversão pode ser relativa conforme a idade das pessoas, alguns padrões podem existir conforme a idade. Exemplo: Crianças de 8 a 9 anos tem tendências a ter coleções diversas, isto pode ser explorado no sistema "gamificado" (PAULO GERALDO, 2001).
Fácil aprendizado	Um sistema difícil de manusear pode causar estresse no usuário.
Dificuldade para todos os níveis	A plataforma ter uma dificuldade balanceada para todos os usuários.
Imersão	Fazer com que o usuário sinta-se parte do sistema faz com que ele se divirta.

Fonte: (FADEL, L. ET AL., 2014).

As mecânicas de um ambiente gamificado podem dar um retorno significativo por parte dos usuários. (Zichermann e Cunningham, 2011) Segue abaixo as mecânicas (pontos, nível de jogo,nível de dificuldade, nível de jogador) usadas na plataforma Hacker Rangers:

Os pontos são obtidos através das tarefas da plataforma e podem ser conquistadas sempre após a conclusão de alguma tarefa. É possível aumentar a pontuação concluindo quizz, indicando alguma “Ciberatitude” relativa a segurança, ou concluindo os cursos.

A patente indica o seu nível dentro do sistema . Segundo Kapp (2012), existem três tipos de níveis que são descritos a seguir:

O esperado é que um sistema de níveis de jogo atinja três objetivos principais.

O primeiro objetivo é manter o entendimento de que há progresso no sistema, o que proporciona o engajamento do usuário; O segundo objetivo é tem foco na expansão de habilidades do usuário;O terceiro objetivo indica que os níveis ajudarão na motivação do jogador/usuário, ao subir de nível, ele vai querer completar as novas etapas do nível atual e prosseguir para os níveis mais difíceis.

Manter a mesma dificuldade pode criar um problema. Se os níveis de dificuldade forem fáceis demais isto poderá acarretar em uma desaprovação de quem gosta de desafio, e se a dificuldade for muito alta, afastará os jogadores que gostam que a dificuldade aumente gradativamente.(Kapp, 2012)

Nível que demonstra o progresso do jogador. Ele é atribuído ao jogador conforme o avanço na plataforma, ou seja, realizando tarefas. O sentimento de domínio e realização é gerado pelo avanço de nível de jogador, pois cada novo nível possui uma dificuldade maior do que o nível anterior. (Kapp, 2012)

3. DESCRIÇÃO DA SOLUÇÃO

A solução para os presentes problemas apresentados neste projeto trata-se de um Ambiente Virtual de Aprendizagem com técnicas de gamificação. A proposta é fornecer treinamento em cibersegurança para os funcionários da Prefeitura Municipal de Esteio/RS e sensibilizá-los quanto aos riscos de seus atos no meio digital, diminuir vulnerabilidades no cenário, ajudar a entender o básico da Lei Geral de Proteção de Dados (LGPD) e implementar regras de segurança digital.

Seguem abaixo algumas características específicas da plataforma de estudo:

3.1 Plataforma de usuário do Hacker Rangers

A plataforma, a ser utilizada no projeto, foi desenvolvida pela empresa brasileira de segurança chamada Perallis Security e, chama-se Hacker Rangers.

Segundo o site da desenvolvedora (2019), é uma plataforma de gamificação para treinamento e engajamento de usuários e tem como finalidade levar os colaboradores de uma organização a adotarem hábitos “ciberseguros” através da motivação intrínseca.

Com o uso da plataforma, é possível deixar de utilizar métodos de ensino não tradicionais.

3.2 Regulamento da campanha do Hacker Rangers

Antes do início da campanha foram determinadas algumas regras, vide anexo B, para que o Administrador da plataforma possa fazer a gestão adequada e orientar os jogadores. As regras se mantiveram as mesmas do início ao fim.

3.3 Funcionalidades para os usuários do Hacker Rangers

No Hacker Rangers, cada usuário precisa completar uma jornada. A jornada é composta por fases, sendo que o nível de dificuldade de cada fase aumenta conforme a evolução do usuário.

Segundo o site da plataforma Hacker Rangers (2018), a solução conta com diversas funcionalidades e devem cumprir diferentes missões, tais como: concluir 12 módulos de cursos EAD, responder a quizzes, adquirir medalhas virtuais, não cair em mensagens de phishing (disparada a partir do próprio Hacker Rangers), ocupar boas posições nos rankings semanal, mensal ou geral da plataforma, praticar cyber atitudes (mecanismo que será explicado mais adiante), participar de CTF (Capture the Flag) para usuários técnicos, patentes, alertas educativos e provas.

No sistema de ranking da plataforma há diversos meio de ganhar pontos. Exemplos: fazendo cursos de cibersegurança, reportando problemas, sugerindo melhorias, respondendo quizzes e testes, praticando cyber atitudes e não cair em mensagens de phishing.

A plataforma permite adicionar conteúdos específicos também. Como explicado, através de e-mail, pela Ana Luisa Bezerra (2018), Analista Comercial da empresa Perallis Security, é possível a personalização de diversas partes da plataforma, como logos e medalhas.

O Hacker Rangers possui uma aparência bem simples, e isso ajuda muito na tarefa de repassar o conhecimento em cibersegurança na Prefeitura Municipal de Esteio. A figura número 15 mostra que a tela inicial da plataforma.

Figura 15 - Tela inicial da plataforma Hacker Rangers

Fonte: Elaborado pelo autor

Em sua tela inicial é possível obter um resumo do seu progresso na plataforma. Os itens destacados nesta página são : cursos, cyberatitudes, quiz, medalhas, jornada e ranking (geral, mensal e semanal).

3.3.1 Sistema de Ranking

Um dos sistemas que a plataforma possui e que ajudará a tornar o cenário competitivo é o de ranking. A plataforma permite que os usuários acessem três tipos de ranking: ranking semanal, ranking mensal e ranking geral. Isto possibilita o engajamento de todos os colaboradores, independentemente do tempo de casa que possuem, uma vez que colaboradores menos antigos têm tanta possibilidade de ficar em evidência quanto colaboradores mais antigos.

A figura 16 mostra como é gerado este ranking semanal na plataforma.

Figura 16 - Ranking semanal gerado automaticamente pela plataforma

Fonte: Elaborado pelo autor

3.3.2 Cursos EAD

De início, foram disponibilizados alguns cursos EAD , sendo que mais cursos podem ser adicionados à plataforma, caso seja necessário. Os cursos foram: Boas práticas em cibersegurança e Lei Geral de Proteção de Dados. (LGPD)

Figura 17 - Exemplo de curso EAD

Fonte: Elaborado pelo autor

3.3.3 Quiz

O Hacker Rangers também oferece quizzes, de forma a auxiliar os usuários na fixação dos conteúdos abordados nos cursos EAD disponíveis. Responder a quizzes também é uma forma de avançar na jornada. A figura número 18 mostra que é possível saber o assunto do quiz e a sua pontuação máxima.

Figura 18 - Sistema de quiz da plataforma

Fonte: Elaborado pelo autor

3.3.4 Medalhas

As medalhas (Badges) que estão inclusas na plataforma são uma forma de recompensar o jogador toda vez que ele completar algum objetivo. O objetivo pode estar relacionado ao fluxo comum ou não, ou seja, o usuário da plataforma ganhará as medalhas por finalizar os objetivos que estão relacionados ao fluxo de execução da Hacker Rangers (Exemplo : Visitar todas as páginas do site) ou também finalizar as tarefas que não estão relacionadas ao fluxo comum da plataforma (Exemplo: Permanecer em 1º no ranking por uma semana), com o propósito de induzir o usuário a realizar determinadas ações.

A figura número 19 mostra algumas medalhas que foram desbloqueadas com pouco tempo de uso da plataforma.

Figura 19 - Algumas das medalhas disponíveis na plataforma

Fonte: Elaborado pelo autor

Conforme o usuário avançar no jogo, é possível desbloquear mais de 30 medalhas existentes na plataforma.

3.3.5 Cyber Atitude

Uma das maneiras de avançar na jornada é praticar Cyber Atitudes. Uma Cyber Atitude é uma maneira do usuário interagir diretamente com a plataforma, submetendo atitudes relacionadas à Segurança da Informação que tenha tomado no dia a dia da organização. Uma Cyber Atitude poderia ser, por exemplo, travar a tela de um colega de trabalho que tenha esquecido de fazê-lo. Na figura de número 20 é possível ver o formulário disponível para os usuários.

Figura 20 - Formulário de ciberatitude

Fonte: Elaborado pelo autor

Por este mesmo formulário, é possível anexar um documento ou foto a fim de comprovar para o administrador a conclusão de alguma ação, caso o usuário julgar necessário.

3.4 Funcionalidades para os Administradores do Hacker Rangers

A página de administrador possibilita o gerenciamento de toda a plataforma. Através desta página é possível adicionar, editar ou excluir vários tipos de conteúdos do Hacker Rangers, como por exemplo: Quizz, cursos, medalhas e aprovar ciberatitudes.

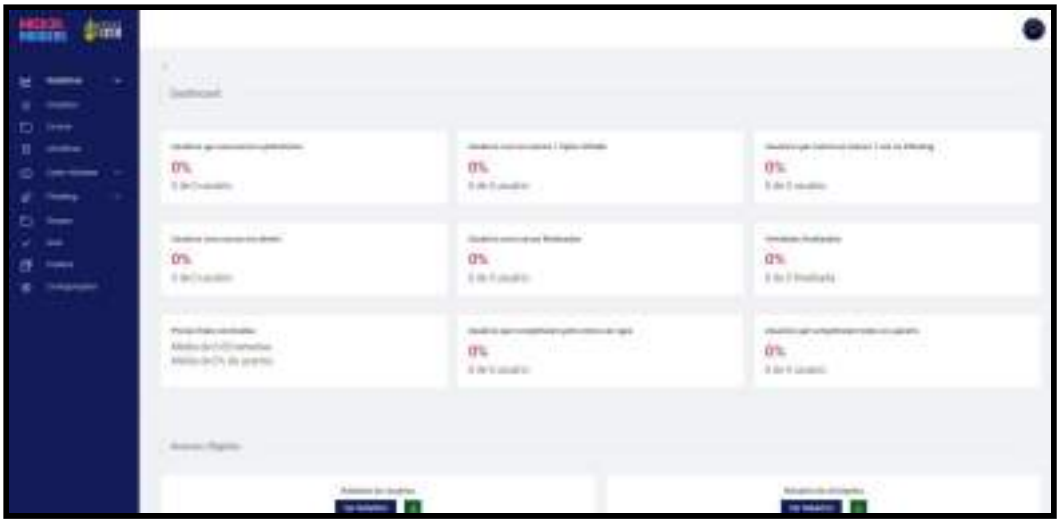
A seguir algumas é possível saber um pouco mais sobre as funcionalidades disponíveis aos administradores:

3.4.1 Página inicial de Administrador

A figura a seguir mostra a tela inicial da página de administração e destaca as

estatísticas gerais dos usuários. Nesta dashboard é possível acompanhar a progressão dos jogadores.

Figura 21 - Dashboard da página de administrador



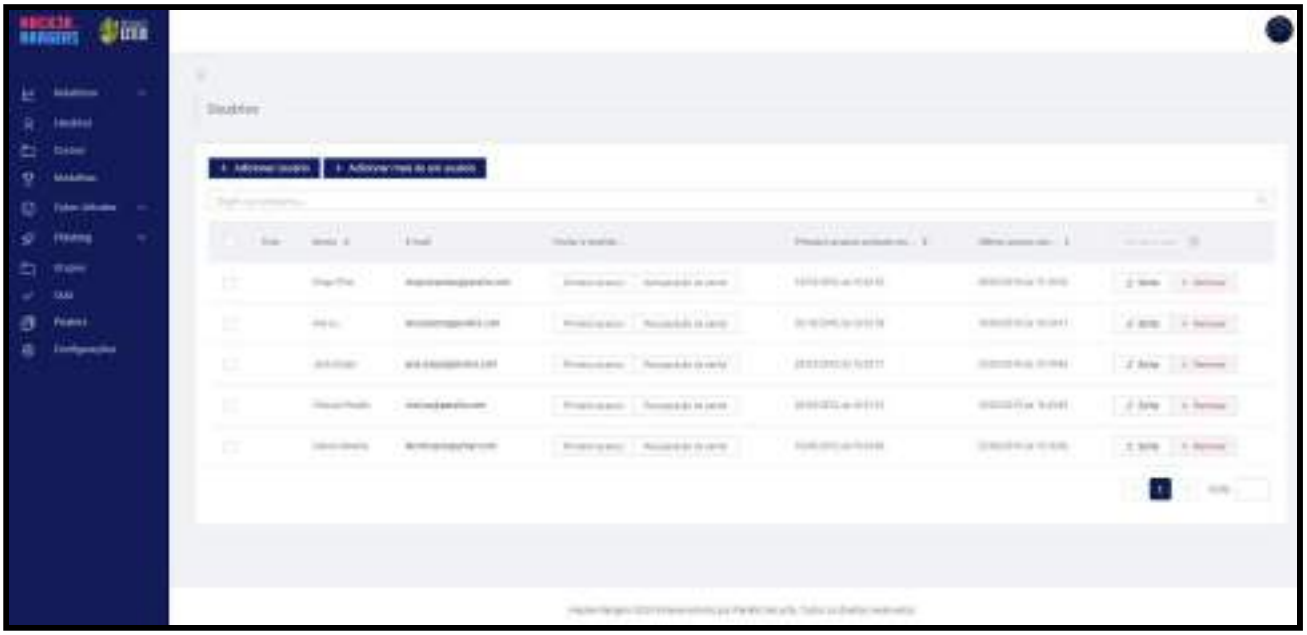
Fonte: Elaborado pelo autor

A tela inicial é simples e intuitiva permite ter uma visão geral dos usuários e facilita o administrador no monitoramento da campanha. Para um melhor controle,o relatório gerado nesta página é sempre atualizado em tempo real.

3.4.2 Página de criação de usuários

A próxima figura diz respeito a tela de criação usuários que serão cadastrados na plataforma.

Figura 22 - Tela de gerenciamento usuários



Fonte: Elaborado pelo autor

Nessa tela é possível adicionar um ou mais de um usuário ao mesmo tempo, além de disponibilizar convite por e-mail e também encaminhar, por e-mail,um link para a troca de senha, caso o usuário tenha esquecido.

3.4.3 Página de cursos

A página de cursos , mostrada na figura 19, permite adicionar, remover ou editar os cursos do Hacker Rangers. Neste projeto, inicialmente, foram disponibilizados os cursos de Boas práticas em Cibersegurança e Lei Geral de Proteção de Dados. Cursos, módulos e tarefas podem ser editados a qualquer momento na página de administrador. A pontuação concedida por cada tarefa pode ser qualquer valor.

Figura 23 - Tela de gerenciamento de cursos

Fonte: Elaborado pelo autor

Os cursos ofertados podem, a qualquer momento, sofrer alterações de seu conteúdo, pontuação e disponibilidade.

3.4.4 Página de administração de medalhas virtuais

Na figura, de número 24, é possível ver algumas das medalhas disponíveis, que já acompanham a plataforma. Cada uma delas representa uma conquista diferente. Nesta mesma página é possível adicionar, editar e remover as medalhas.

Figura 24 - Página de gerenciamento de medalhas

Fonte: Elaborado pelo autor

3.4.5 Cyber Atitudes

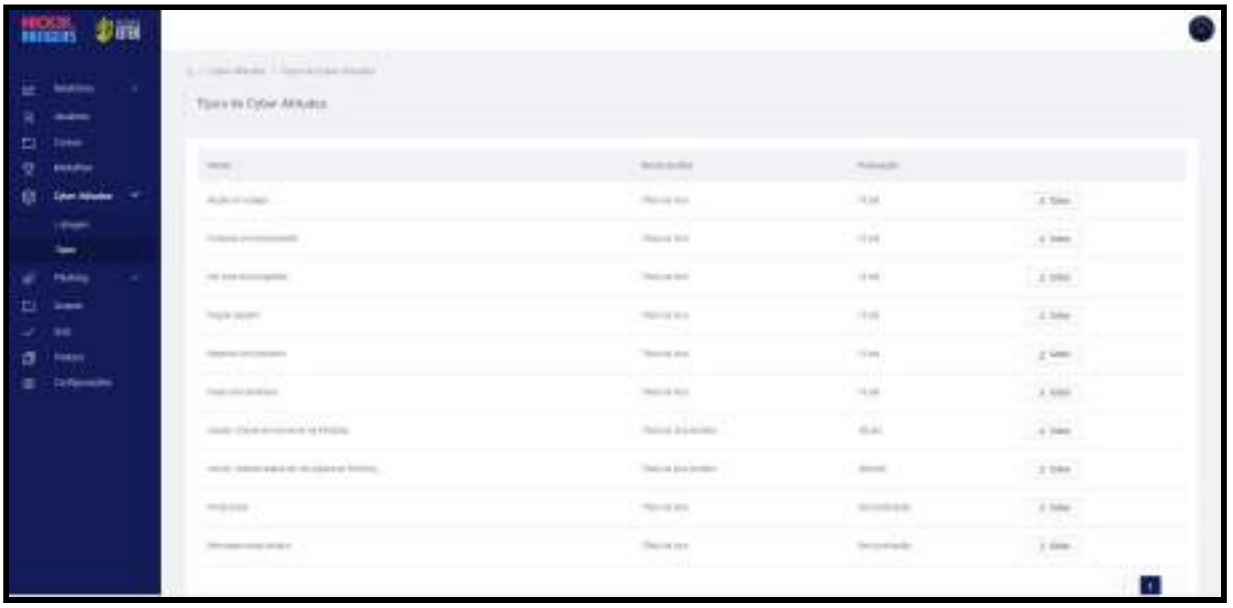
Nesta página é possível editar os tipos de Cyber Atitudes. Na adaptação a única Cyber Atitude que gerou pontuação é a de “Reportar um risco de segurança” , valendo +1 ponto, quando aprovada pelo administrador da plataforma.

Segundo anexo B, referente ao regulamento, as demais atitudes não pontuam, porém concedem medalhas e são critérios para evolução de patentes. A Cyber Atitude “Reportar um risco de segurança” tem o objetivo de auxiliar a Prefeitura de Esteio na detecção de riscos de segurança da informação. Esse objetivo será considerado na aprovação das cyber atitudes cadastradas pelos usuários para pontuação. São exemplos de cyber atitudes “Reportar um problema” passíveis de aprovação:

- Reportar o recebimento de um Phishing (simulado ou não).
- Reportar dados sensíveis armazenados ou publicados em lugares indevidos.
- Reportar uma vulnerabilidade em sistemas internos.
- Reportar uma vulnerabilidade em serviços/sistemas usados pelos contribuintes.
- Reportar uma vulnerabilidade de procedimento.

A figura 25 mostra a página de edição das cyber atitudes, todas elas já vieram pré-estabelecidas na plataforma.

Figura 25 - Tipos de Cyber Atitudes



Fonte:Elaborado pelo autor

A próxima figura ilustra a tela de Phishing da plataforma. O Hacker Rangers oferece o serviço de Engenharia Social via Campanhas de Phishing, onde são realizadas ações para analisar o comportamento dos usuários, principalmente na utilização dos e-mails e, a partir disso, aplicar ações de conscientização.

Esta plataforma disponibiliza alguns cursos , quiz e testes relativos a boas práticas de cibersegurança no ambiente corporativo, e outros poderão ser adicionados conforme necessidade do ambiente.

Durante o andamento da campanha, os usuários terão boas noções de segurança e poderão auxiliar os seus colegas e provavelmente até fornecer treinamentos dentro da Prefeitura, aumentando a cultura de segurança.

Ao término da campanha de conscientização, será realizada uma nova pesquisa a fim saber sobre a maturidade de segurança da informação dos usuários da plataforma.

4. METODOLOGIA

Este projeto trata-se de uma pesquisa qualitativa, que tem como o objetivo a busca pela resolução de problemas práticos do cotidiano, entre outros, conforme (CHERRY, 2017):

> Applied research refers to scientific study and research that seeks to solve practical problems. Applied research is used to find solutions to everyday problems, cure illness, and develop innovative technologies. (CHERRY, 2017).

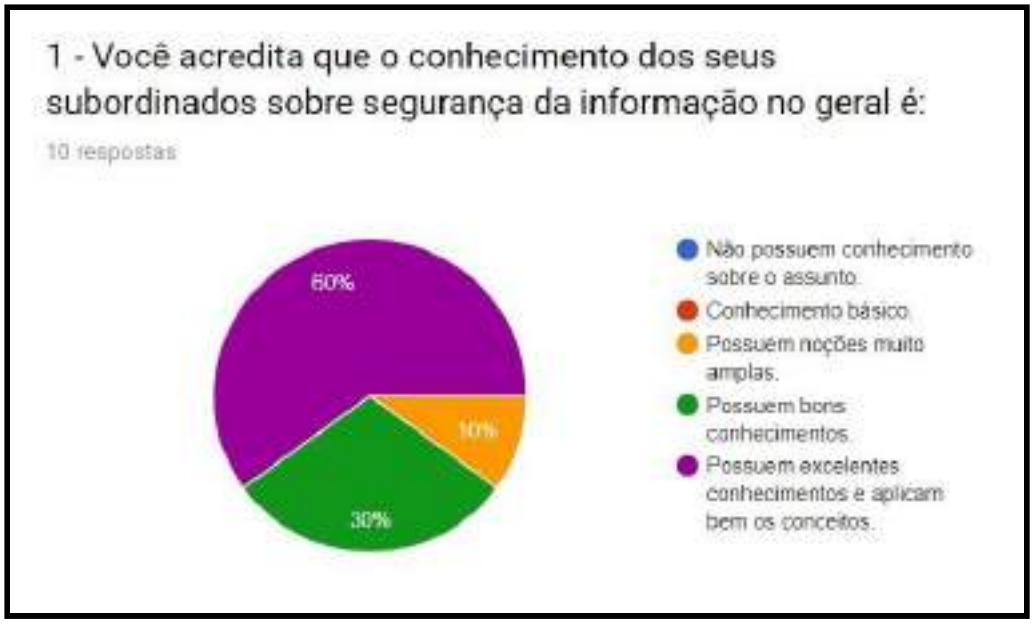
Os métodos de coleta de dados deste projeto são os questionários que têm o intuito de medir o nível de maturidade em segurança da informação dos funcionários da Prefeitura municipal de Esteio-RS, bem como, apontar algumas estatísticas importantes deste cenário.

No total, foram realizadas duas pesquisas. Uma antes do início do projeto e outra após. A segunda pesquisa apresentada indicará o sucesso da plataforma.

De acordo com a figura , relacionada a primeira pesquisa, de número 1 deste projeto, mostra que os usuários, inicialmente, não mostraram muitos conhecimentos na área de segurança, o que ocasionaram em muitos incidentes dentro da Prefeitura.

Já na segunda pesquisa, figura número 26, o resultado aponta que os usuários aumentaram o conhecimento sobre segurança, tornando o ambiente mais seguro.

Figura 26 - Pergunta da segunda pesquisa para medir o nível de maturidade em segurança

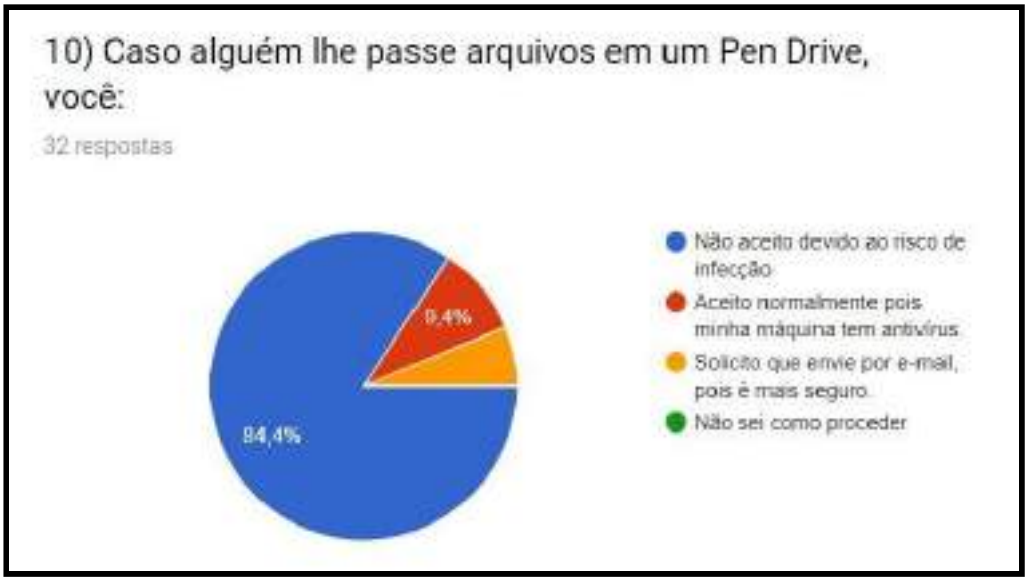


Fonte: Elaborado pelo autor

A pergunta acima foi respondida apenas por gestores que optaram participar da plataforma, ou seja, apenas 10 usuários. Nota-se que a confiança dos gestores em relação aos seus subordinados aumentaram.

Outros dados importantes do presente projeto são os resultados da segunda pesquisa. O número de pessoas que aceitariam receber arquivos por pendrive caiu após o início deste projeto, conforme a figura 27.

Figura 27 - Pergunta referente ao uso de Pen Drive



Fonte: Elaborado pelo autor

A primeira pesquisa mostrou que apenas 10,6% não aceitaria pendrive de terceiros devido ao risco de infecção, contra 84,4% da última pesquisa. Indicando aumento a maturidade dos usuários.

5. VALIDAÇÃO

Para validar a solução apresentada neste projeto, foram adquiridas licenças da plataforma Hacker Rangers e foram realizadas duas pesquisas a fim de medir o nível de maturidade em Segurança da Informação dos usuários internos da Prefeitura Municipal de Esteio - RS.

Após o início deste projeto, dia 10 de setembro de 2019 , foi constatado que o número de reportes relativos a segurança aumentaram. Através sistema interno de Help Desk, denominado GLPI, e também através do módulo “ciberatitudes” foi apontado que houve um aumento significativo dos chamados, resultado que foi obtido somente após o início do projeto, indicando que os usuários se conscientizaram sobre das ameaças, que antes eram desconhecidas pelos funcionários.

A figura de número 28 mostra o número de chamados anteriores ao projeto e após.

Figura 28 - Comparativo do número de chamados relativos a segurança

Fonte: Elaborado pelo autor

Como é possível ver na figura acima, o número de chamados relativos ao mesmo período do ano anterior aumentou de 5 para 18, ou seja, 260% a mais, provando a eficácia da conscientização .

Os chamados anteriores ao projeto indicavam problemas que surgiam pela falta de sabedoria dos usuários em algumas situações, e os chamados após o início do projeto, os chamados abertos indicavam incidentes quase que inofensivos, alerta de spam é um exemplo, e também solicitaram que seus e-mails e arquivos

confidenciais fossem criptografados, conforme indica o curso de Boas Práticas de Cibersegurança da plataforma.

A figura de número 29 mostra um dos chamados, aberto após o início da campanha de conscientização, relativo a um e-mail suspeito enviado para o e-mail do IPTU da Prefeitura de Esteio.

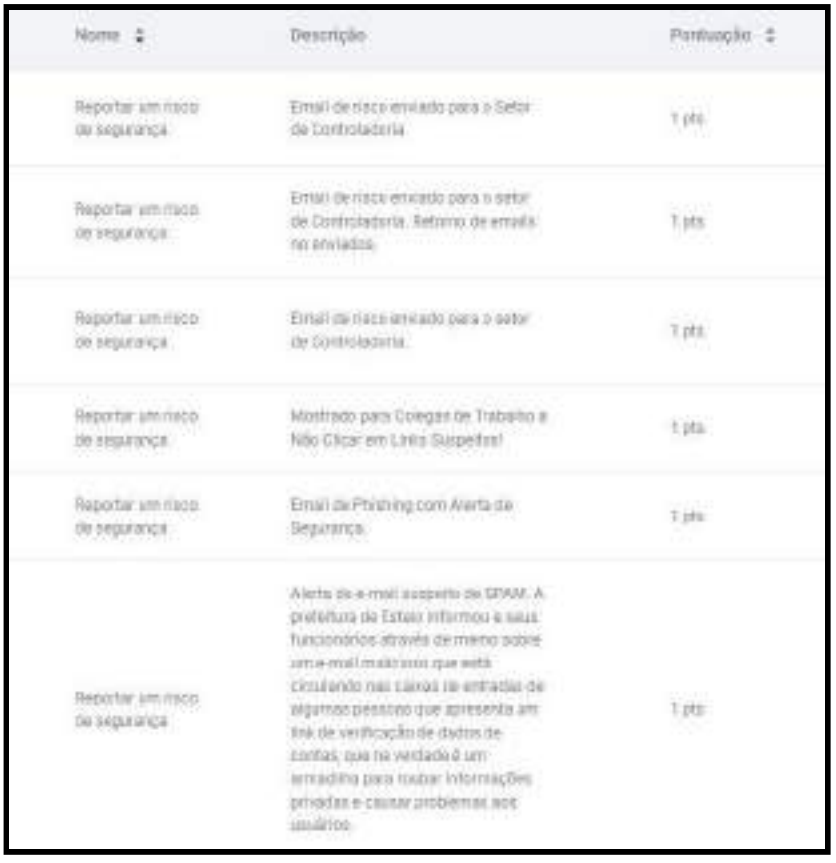
Figura 29 - Reporte de E-mail suspeito

Fonte: Elaborada pelo autor

Este tipo de chamado nunca foi aberto antes da campanha,indicando que os usuários estão atentos às ameaças.

A segundo a figura de número 30, os usuários criaram a cultura de reportar , constantemente, os incidentes com spam.

Figura 30 - Usuários reportaram incidentes através do módulo Ciberatitudes



Fonte: Elaborada pelo autor

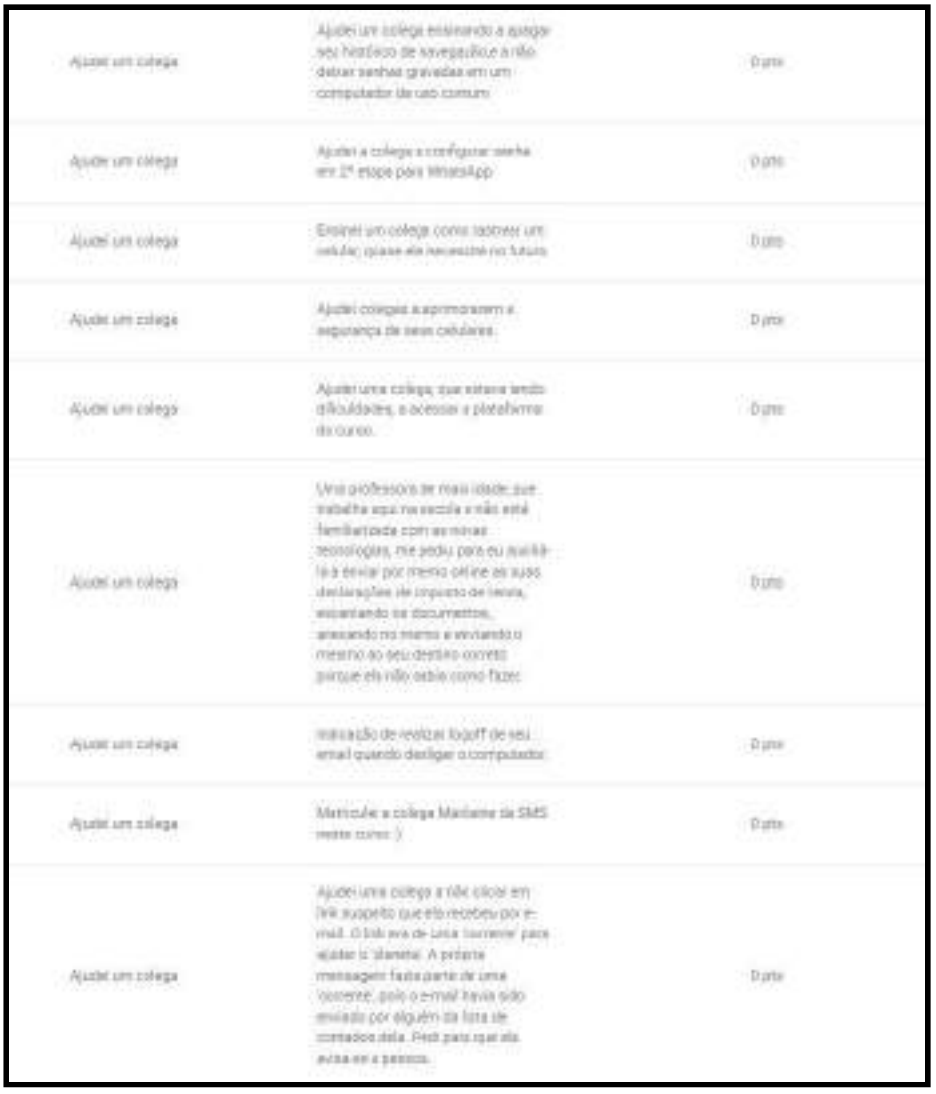
Os usuários,conforme aponta as imagens 31 e 32, também criaram a cultura de repassar os seus conhecimentos para seus colegas e familiares,atingindo indiretamente as pessoas que não utilizaram a plataforma.

Figura 31- Categoria “Ajudei um Colega” do módulo de Ciberatitudes.

Ajudei um colega	Ensinei um colega a não clicar em redirecionamento de páginas enviadas por e-mail, pois pode ser página falsa para coletar seus dados.	5 pts
Ajudei um colega	Ensinei um Colega não clicar em links enviados por e-mail por risco de phishing.	5 pts
Ajudei um colega	Ajudei a configurar a chamada de caixa postal em número desconhecido como spam (era 011)	5 pts
Ajudei um colega	Aconselhando em não clicar naquela oferta do facebook de origem duvidosa	5 pts
Ajudei um colega	Ajudei a um colega a colocar uma senha mais forte no seu email	5 pts
Ajudei um colega	Ajudei um colega a não colocando salvo o e-mail e senha automaticamente no note de escola.	5 pts
Ajudei um colega	Ensinei um colega a jamais clicar em links que recebem nos e-mails e avisar o Setor de TIC quando for conta da Prefeitura	5 pts
Ajudei um colega	Colega Recebeu e-mail de Phishing e informei o para abrir chamado junto a TIC de Esteio.	5 pts
Ajudei um colega	Orientei um colega a não clicar em links nos e-mails!	5 pts
Ajudei um colega	Ajudei um colega explicando o risco de clicar em links suspeitos com uma procedência suspeita.	5 pts

Fonte:Elaborada pelo autor

Figura 32 - Categoria “Ajudei um Colega” do módulo de Ciberatitudes.



Fonte: Elaborada pelo autor

Esta categoria ajudou a entender como os próprios usuários estão cuidando da segurança do ambiente. Como aponta os resultados deste projeto, conforme as pesquisas realizadas, obtivemos um aumento na maturidade de segurança da informação.

6. CONCLUSÃO

Pode-se afirmar que o objetivo geral do projeto foi atingido durante o desenvolvimento deste.

Os objetivos específicos propostos também foram alcançados, demonstrando, através das pesquisas e chamados abertos no GLPI para a equipe de TIC, que as técnicas de Gamificação ajudaram na aprendizagem. Segundo os usuários, foi possível afirmar, através da solução apresentada, que é possível aprender sobre um determinado assunto de um modo divertido sem atrapalhar o andamento do serviço.

Observou-se também que o Hacker Rangers aumentou o nível de maturidade em segurança da informação do cenário, o que o torna viável, fazendo com que os usuários tenham melhores noções sobre o uso dos sistemas computacionais.

Nota-se isso pela forma que os usuários abriram chamado após o início da campanha e como agiram durante a campanha.

O módulo de “ciberatitudes”, nativa da plataforma, foi essencial para a coleta de informações sobre como os usuários estão agindo no seu cotidiano. Conforme validação, este módulo apresentou-se como uma importante ferramenta para o registro de atividades dos jogadores.

Através do monitoramento do servidor de email foi possível identificar que o número de botnet e, consequentemente, o envio de spam para endereços aleatórios foi reduzido.

Desde o início da adaptação da campanha, não houve nenhum registro de Ransomware no ambiente, e o número de outras ameaças caiu consideravelmente.

O projeto trouxe para a Prefeitura a cultura de reportar incidentes e, ao mesmo tempo, tomar conhecimento de ameaças que podem prejudicar os usuários.

Segundo a pesquisa final, pode-se afirmar que um dos principais atrativos da plataforma, segundo os usuários, são as premiações e a diversão.

Durante a realização do projeto, foi observado muitos pontos fortes referente a plataforma de uma forma geral. As opções de administrador do Hacker Rangers, para gerenciar a maioria das suas funcionalidades, proporcionou um ambiente de

administração centralizado, objetivo e simplificado,visto que não exige nenhum treinamento para operar a plataforma. Através da segunda pesquisa, aplicada no final do projeto aos usuários, foi observado que a maioria dos usuários participaria novamente do projeto. Conclui-se também que foi obtido um aumento na maturidade de segurança da informação, visto que os incidentes foram reduzidos e os demandantes aprenderam do que tratam as ameaças.

Os trabalhos futuros que irão partir destas pesquisas e servirão para, possivelmente, uma nova adaptação futura de um novo Ambiente Virtual de Aprendizagem , como por exemplo o Moodle , a fim de capacitar os funcionários do órgão e ampliar a oferta de cursos de segurança na Prefeitura.

7. REFERÊNCIAS BIBLIOGRÁFICAS

What is CyberSecurity ?
https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security<Acesso em: 05/12/2018>

O que é cibersegurança ?
http://www.infoprotect.com.br/blog/o-que-e-ciberseguranca/<Acesso em:05/12/2018>

Análise das técnicas de Gamificação em Ambientes Virtuais de Aprendizagem
https://www.researchgate.net/publication/280923773_Analise_das_tecnicas_de_Gamificacao_em_Ambientes_Virtuais_de_Aprendizagem <Acesso em: 06/12/2018>

How to decrypt .combo ransomware

https://soft2secure.com/knowledgebase/combo-ransomware <Acesso em : 18/12/2018>

Oniria. **Diferentes soluções baseada em games**https://oniria.com.br/voce-sabe-a-diferenca-entre-simuladores-virtuais-games-e-gamificacao/grafico/ <Acesso em: 11/12/2018>

Vasconcellos, Paulo.**O que é Gamificação? Conheça a ciência que traz os jogos para o cotidiano.**
https://www.techtudo.com.br/noticias/noticia/2016/07/o-que-e-gamificacao-conheca-ciencia-que-traz-os-jogos-para-o-cotidiano.html <Acesso em: 11/12/208>

https://cidades.ibge.gov.br/brasil/rs/esteio/panorama <Acesso em : 24/12/2018>

Brasil está entre os países mais vulneráveis do mundo, segundo a CompTIA <https://cio.com.br/brasil-esta-entre-os-paises-mais-vulneraveis-do-mundo-segundo-a-comptia/> <Acesso em: 25/12/2019>

O que é Phishing. https://www.avast.com/pt-br/c-phishing <Acesso em: 24/12/2018>

O que é Phishing Scam ? https://canaltech.com.br/hacker/O-que-e-Phishing-Scam/ <Acesso em: 15/12/2018>

Hacker Rangers. Disponível em:<https://hackerrangers.com/><Acesso em: 14/12/2018>

Hacker Rangers: Plataforma usa gamificação para promover cibersegurança. https://www.tecmundo.com.br/seguranca/145852-hacker-rangers-plataforma-usa-gamificacao-promover-ciberseguranca.htm <Acesso em 26- 06 - 2019>

Payão, Felipe. **Cibercriminosos estão simulando mensagens do Banco do Brasil no WhatsApp.**https://www.tecmundo.com.br/whatsapp/115078-cibercriminosos-simulando-mensagens-banco-do-brasil-whatsapp.htm <Acesso em:16/12/2018>

O que é Adware? https://www.tecmundo.com.br/spyware/271-o-que-e-adware-.htm <Acesso em:17/12/18>

WhiteRose Ransomware https://www.enigmasoftware.com/pt/whiteroseransomware-remocao/ <Acesso em 18/12/2018>

Abrams, Lawrence. **The WhiteRose Ransomware is Decryptable & Tells a strange Story**.Disponível em: <https://www.bleepingcomputer.com/news/security/the-whiterose-ransomware-is-decryptable-and-tells-a-strange-story/> <Acesso em 18/12/2018>

Bezerra, Ana Luisa. Publicação eletrônica [mensagem pessoal]. Mensagem recebida por <segurancadainformacao@esteio.rs.gov.br> em 30 Nov. 2018.

BUSARELLO, Raul. **Gamification princípios e estratégias**. São Paulo: Pimenta Cultural, 2016.

CHERRY, Kendra. **What Is Applied Research?.** Disponível em: <https://www.verywell.com/what-is-basic-research-2794876>. Acesso em: 21/12/2019.

DETERDING, S.; DIXON, D.; KHALED, R.; NACKE, L. **From game design elements to gamefulness: Defining "gamification"**. MindTrek '11 Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments. 9-15. (2011a).

KAPP, Karl M. **The gamification of learning and instruction: game-based methods and strategies for training and education.** San Francisco: Pfeiffer, 2012.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação: princípios e controles de ameaças.** São Paulo: Erica, 2014.

PRENSKY, Marc. **Aprendizagem baseada em jogos digitais.** São Paulo: SENAC São Paulo, 2012.

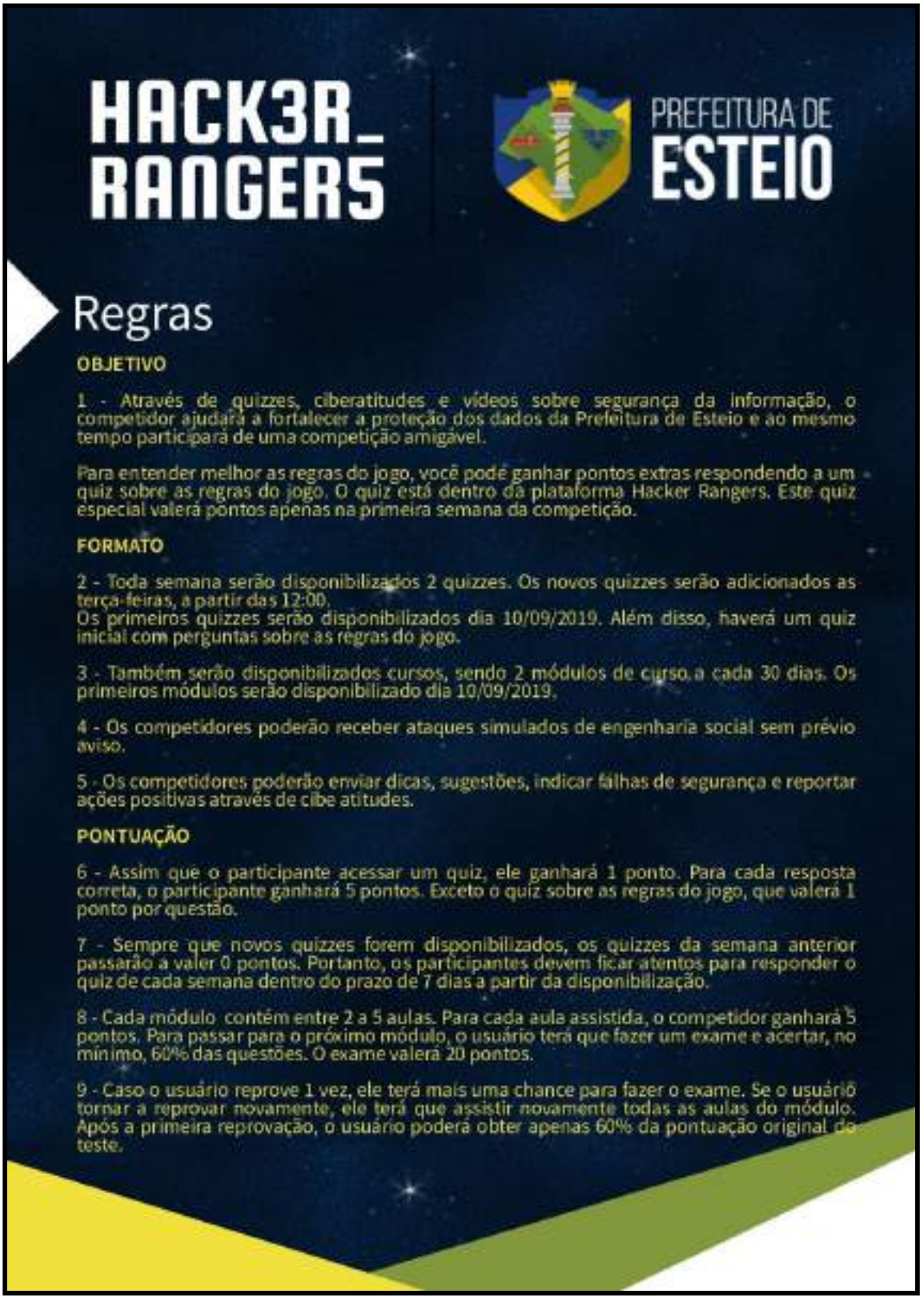
VIANNA, Y. et al. **Gamification, Inc.: como reinventar empresas a partir de jogos.** Rio de Janeiro: MJV Press,2013.

ZICHERMANN, G.; CUNNINGHAM, C. **Gamification by Design. Implementing Game Mechanics in Web and Mobile Apps.** Canada: O'Reilly Media, 2011.

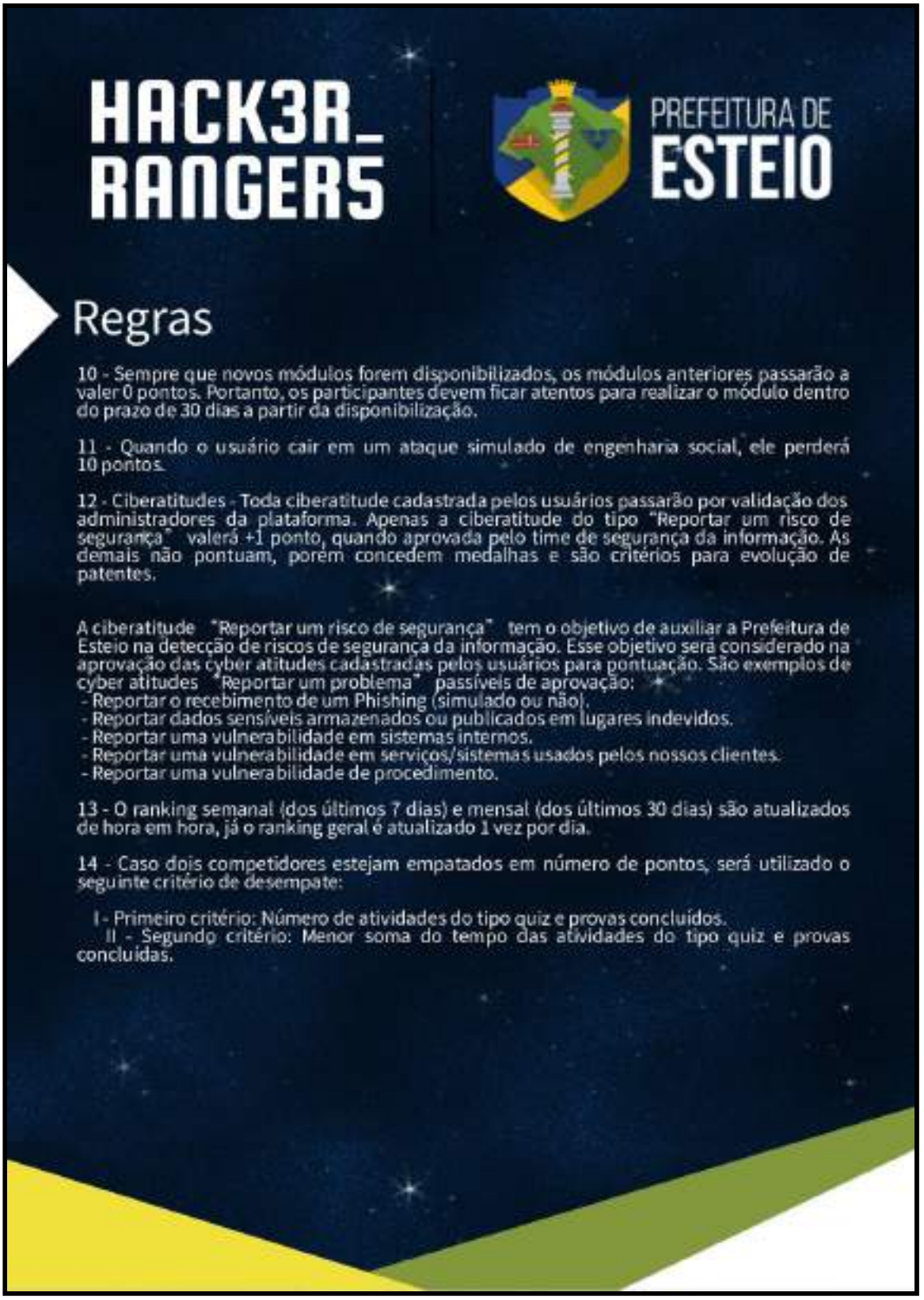
ANEXO A - BANNER DA COMPETIÇÃO

Fonte: Próprio autor

ANEXO B - REGULAMENTO DA COMPETIÇÃO



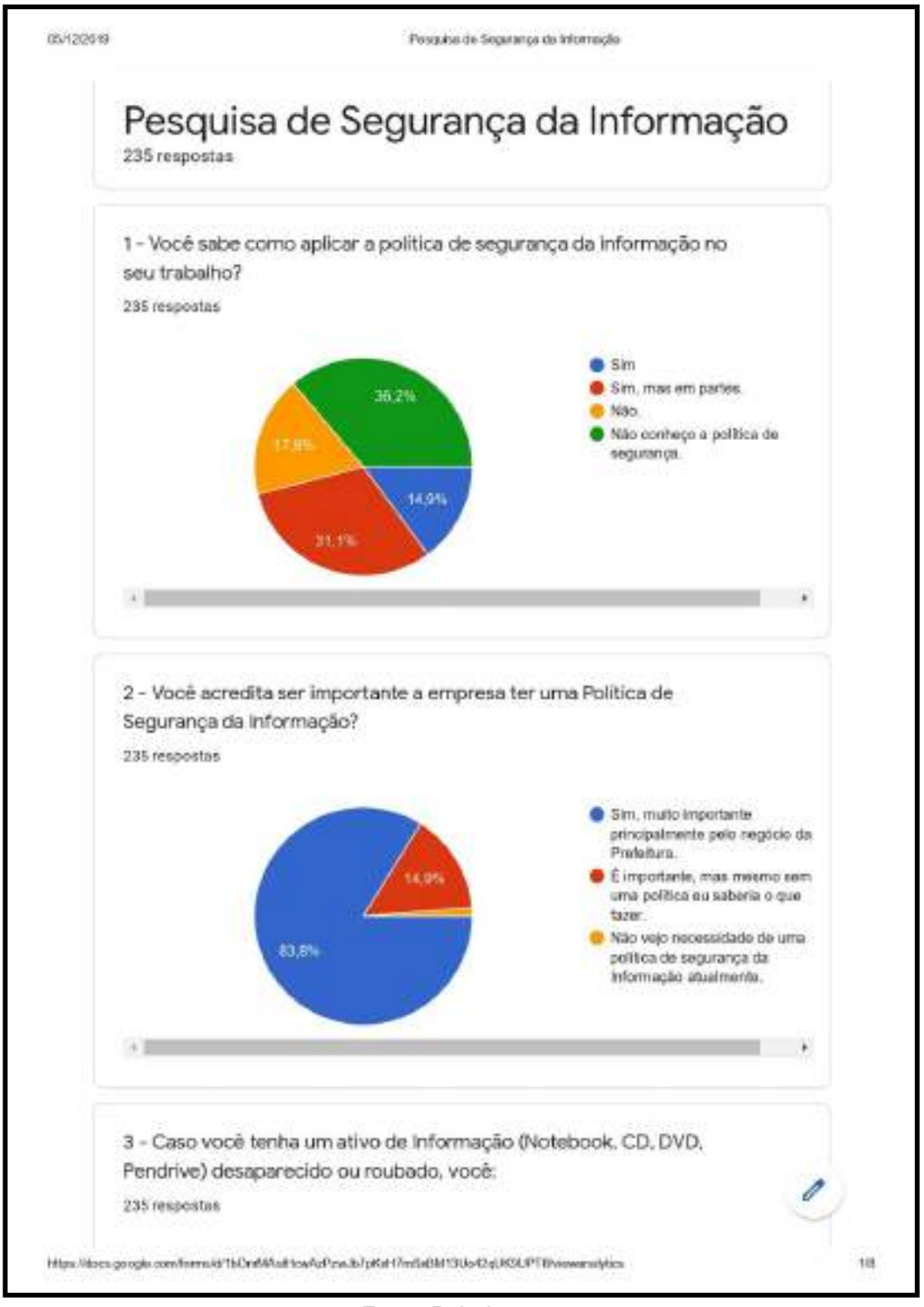
Fonte: Próprio autor



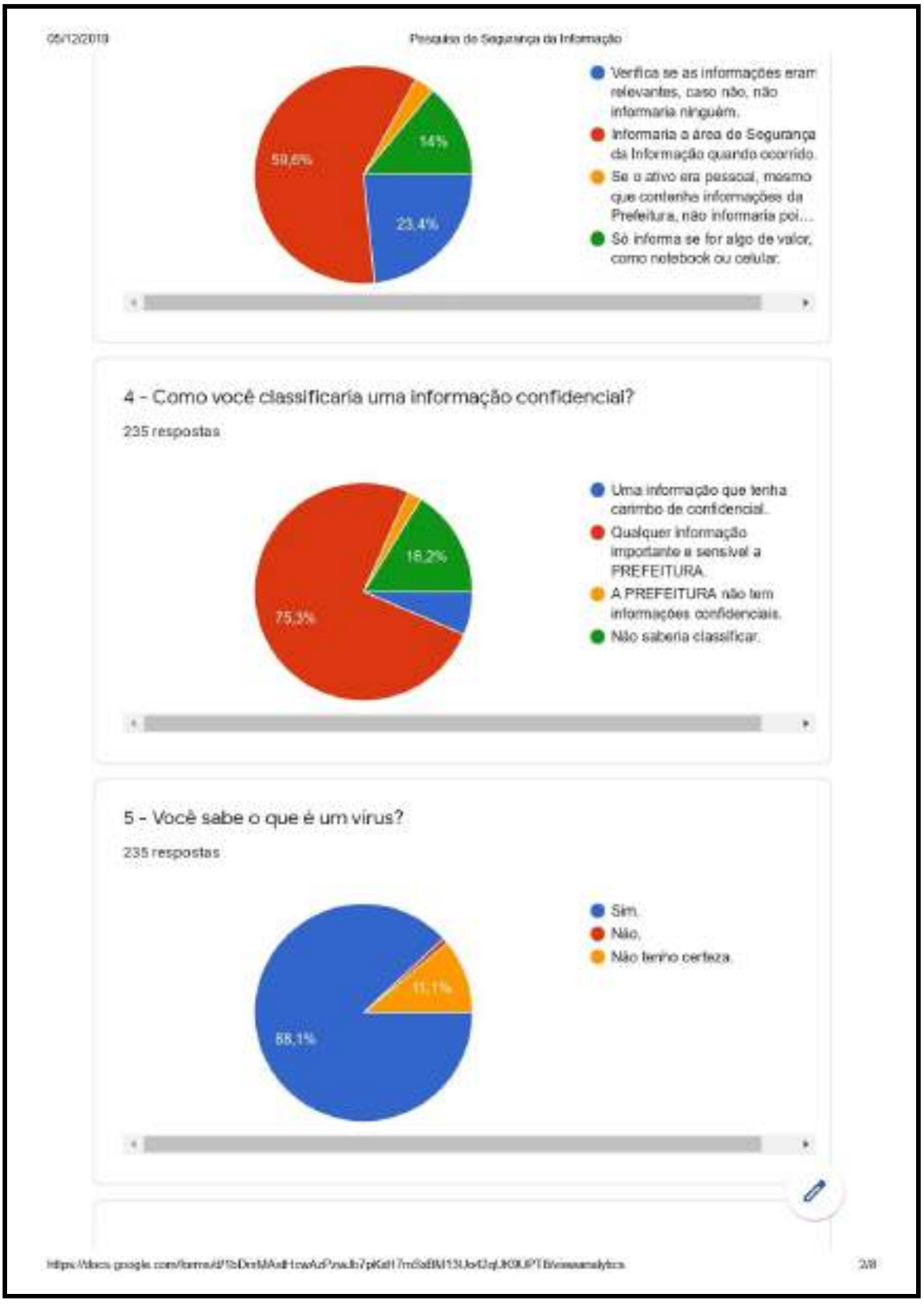
Fonte: Próprio autor

Fonte: Próprio autor

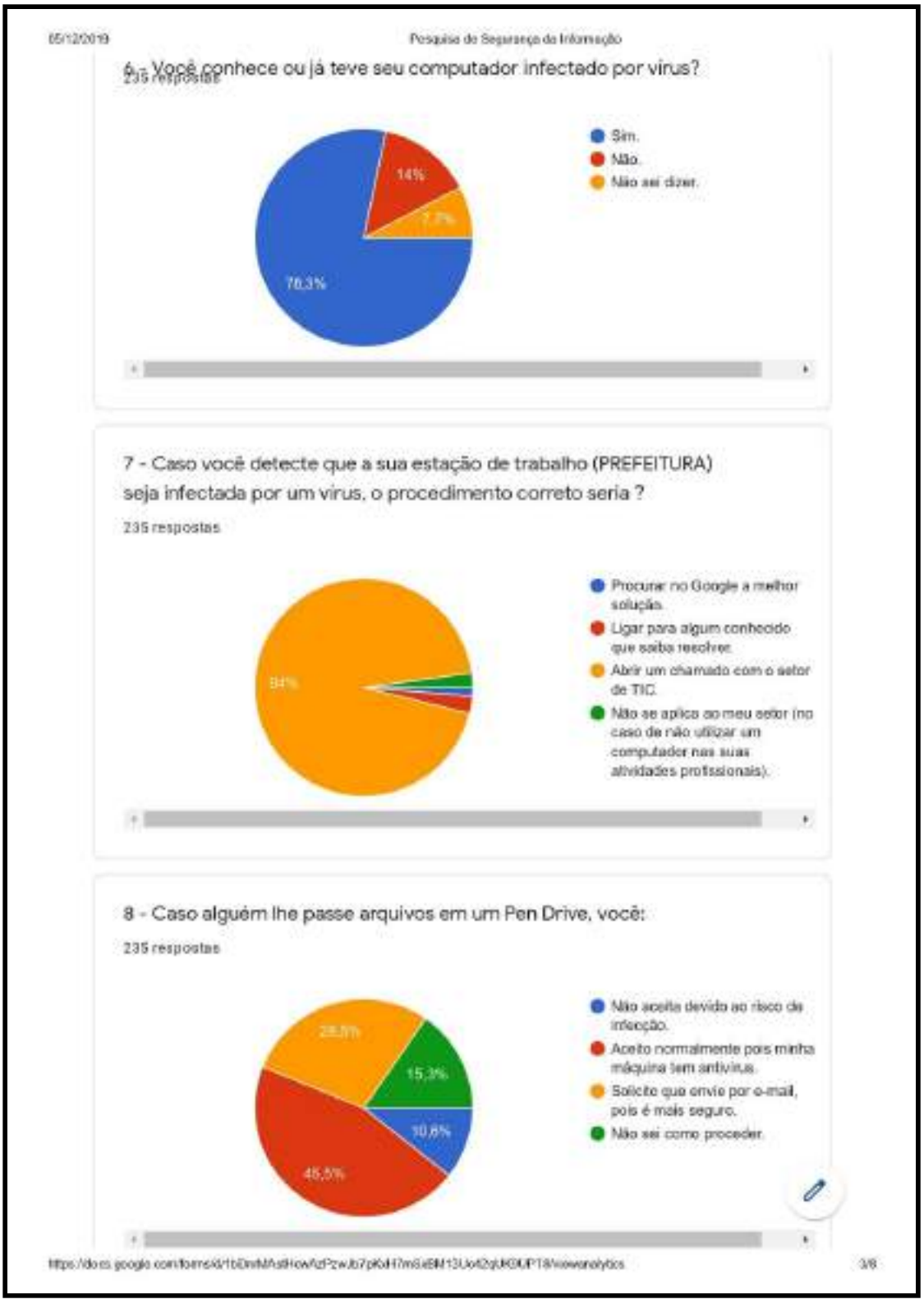
ANEXO C - PRIMEIRA PESQUISA DE SEGURANÇA



Fonte: Próprio autor



Fonte: Próprio autor

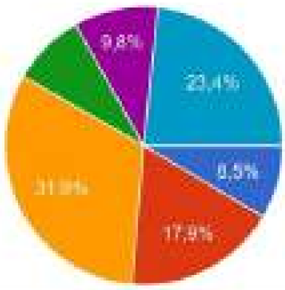


Fonte: Próprio autor

05/12/2019 Pesquisa de Segurança da Informação

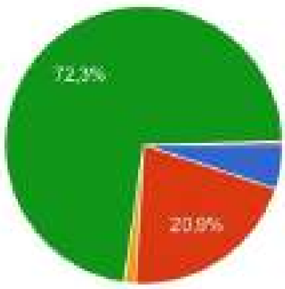
9 - Você está no seu intervalo e acessou o seu e-mail pessoal. Na sua caixa de entrada está o e-mail de um amigo com um link suspeito. Por curiosidade você clica no link e identifica que é um link malicioso. Que ação você tomaria?

235 respostas



10 - Posso considerar um e-mail suspeito:

235 respostas

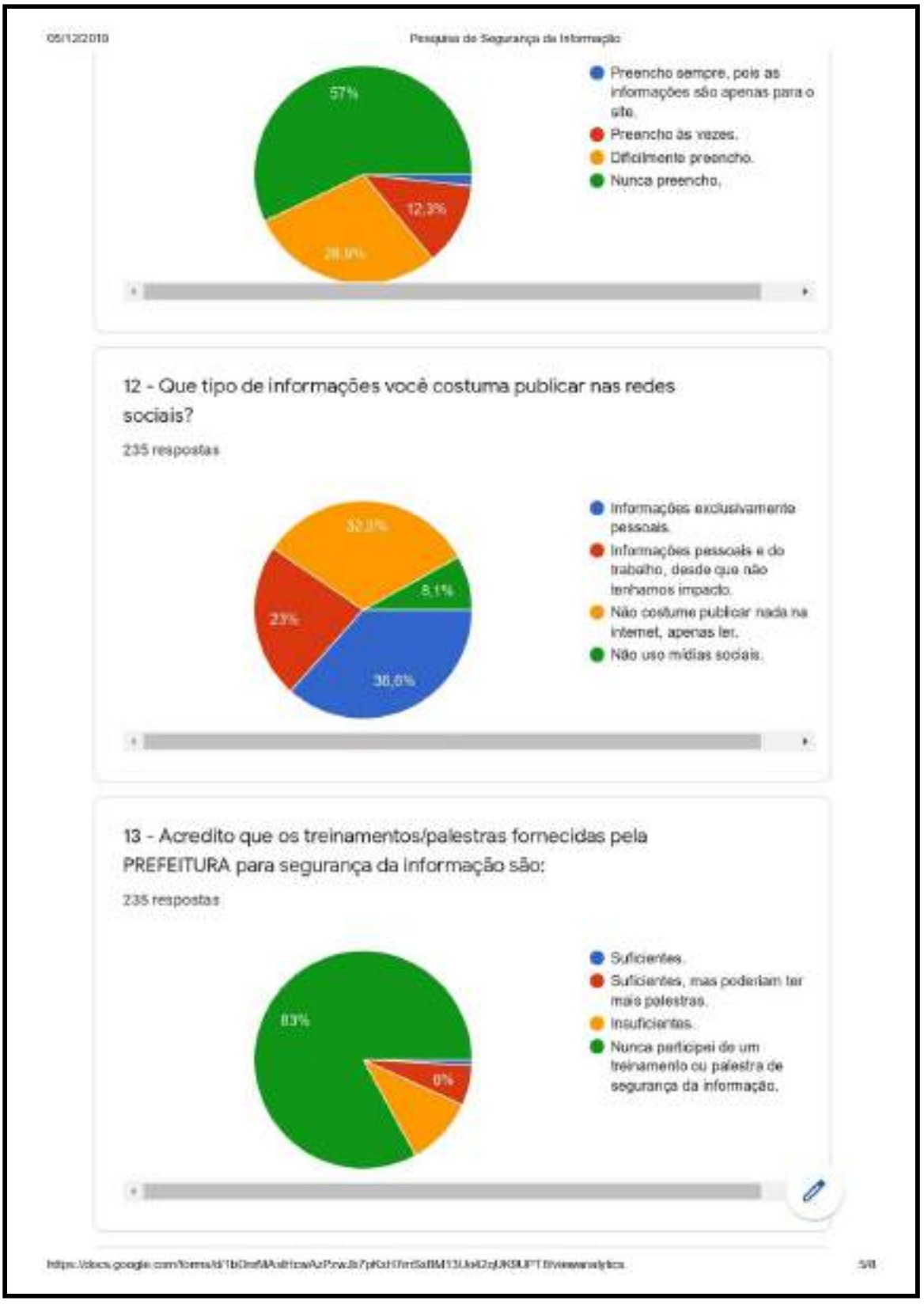


11 - Quando é solicitada a você informações de trabalho, pelas redes sociais [Ex: Linkedin,Facebook] como: local de trabalho, função, tempo de empresa, média salarial e etc., você:

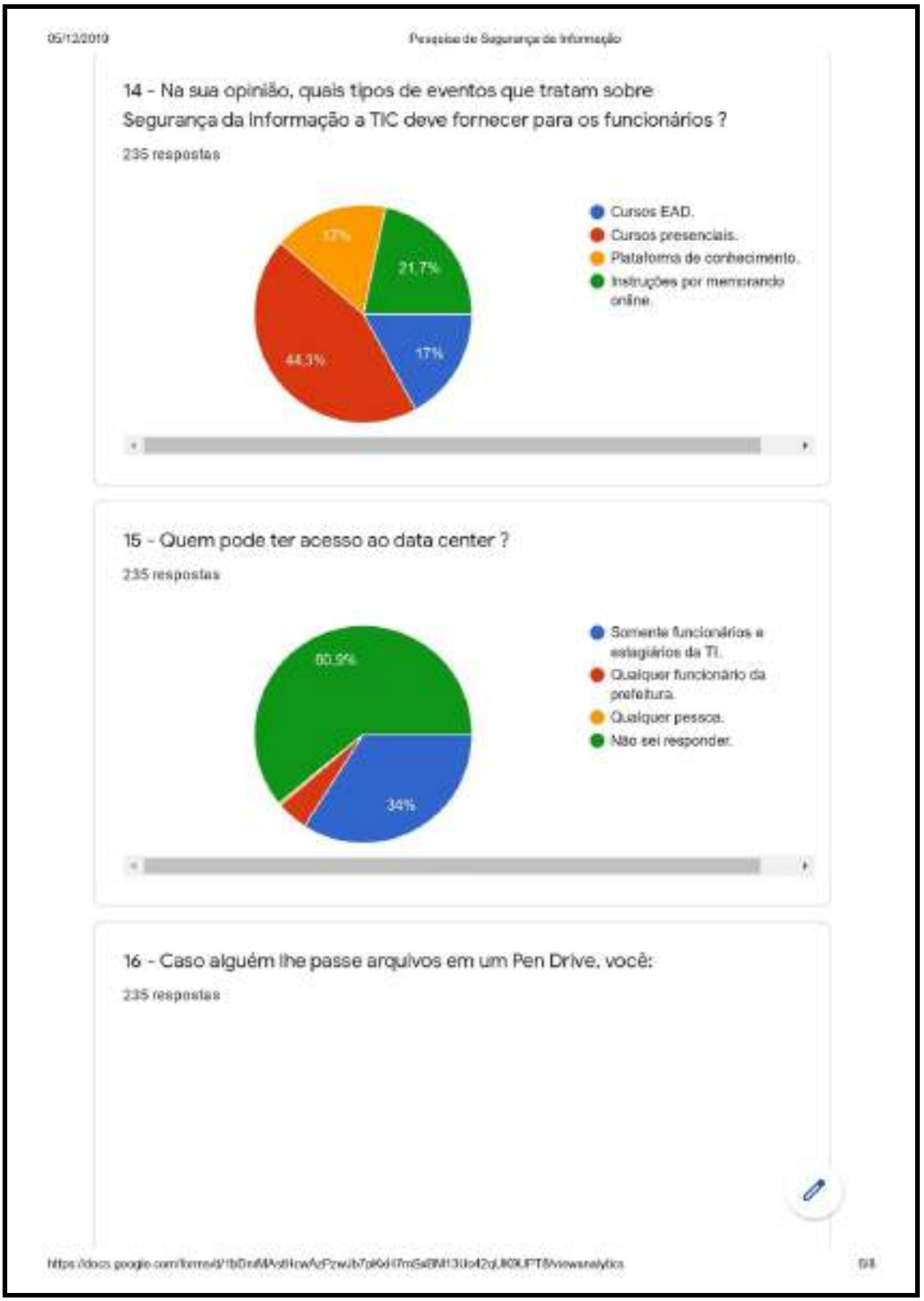
235 respostas

https://docs.google.com/forms/d/1bDnrMAatHowAzPcsuJb7pKsH7m6eBM13Uv42qUK9UPT8/viewanalytics 4/8

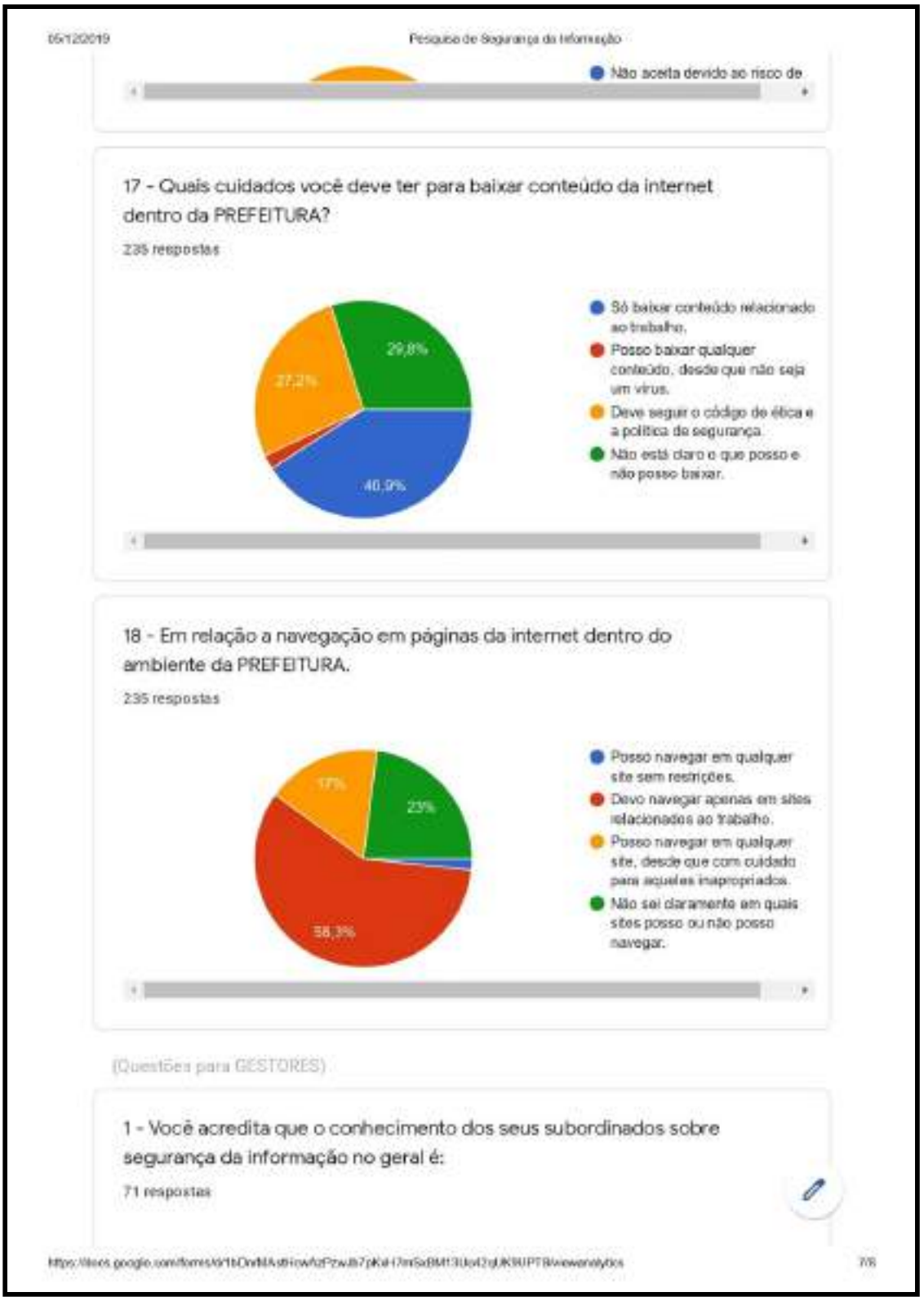
Fonte: Próprio autor



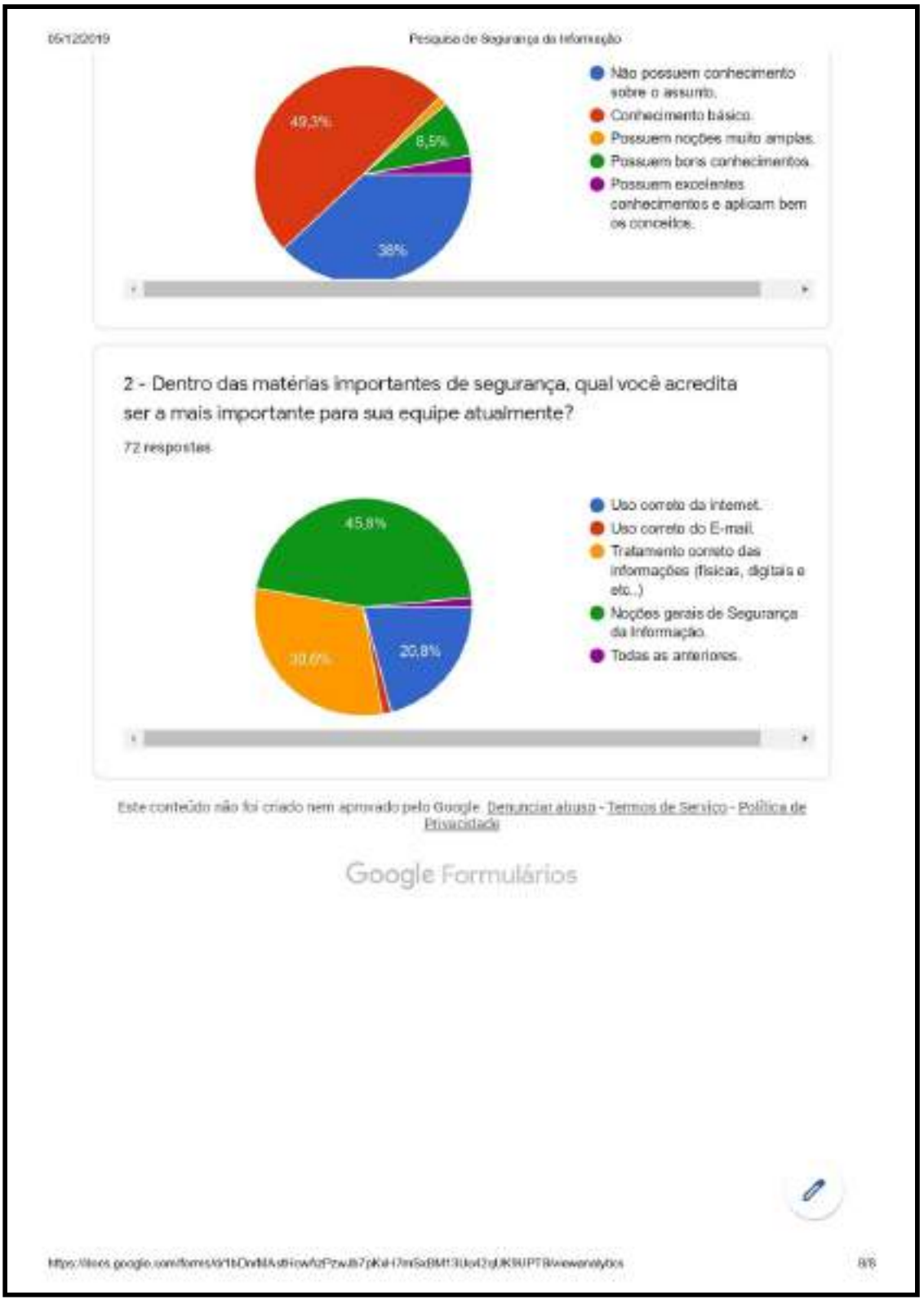
Fonte: Próprio autor



Fonte: Próprio autor

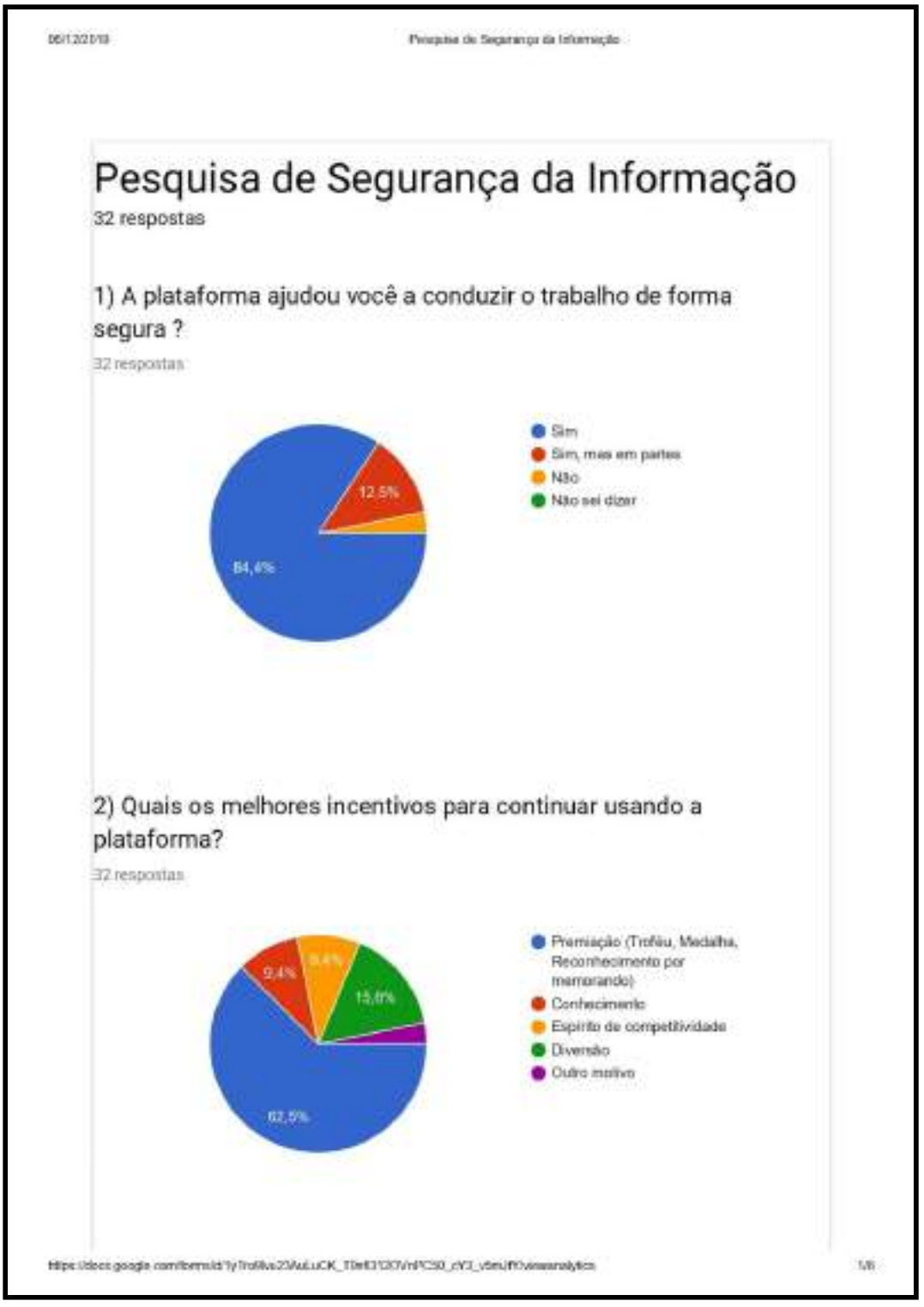


Fonte: Próprio autor



Fonte: Próprio autor

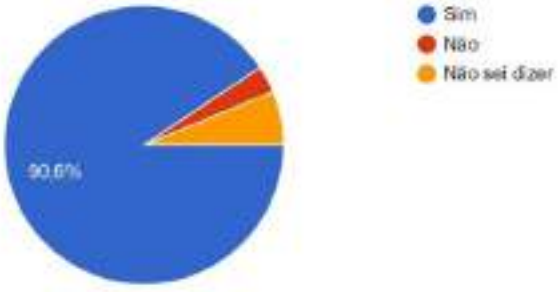
ANEXO D - SEGUNDA PESQUISA DE SEGURANÇA



Fonte: Próprio autor

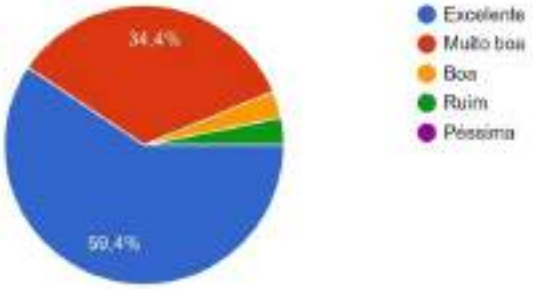
3) A prefeitura deve manter a plataforma ativa ?

32 respostas



4) Referente a aprendizagem, como foi sua experiência com a plataforma ?

32 respostas

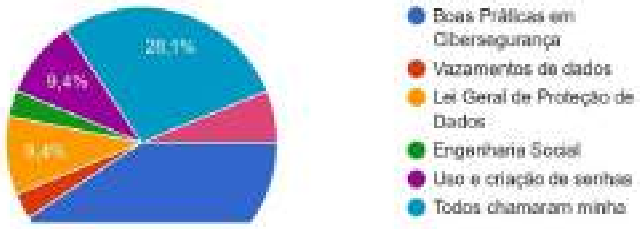


5) Qual assunto chamou mais a sua atenção ?

32 respostas

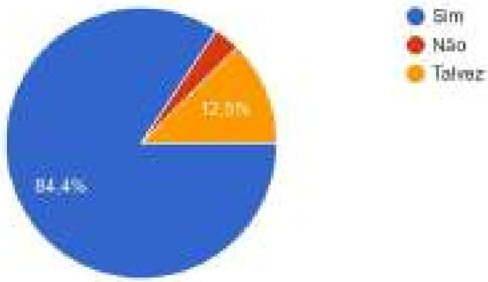
Fonte: Próprio autor

09/12/2019 Pesquisa de Segurança da Informação



6) Você repetiria esta experiência de participar de um Ambiente Virtual de Aprendizagem com técnicas de gamificação ?

32 respostas



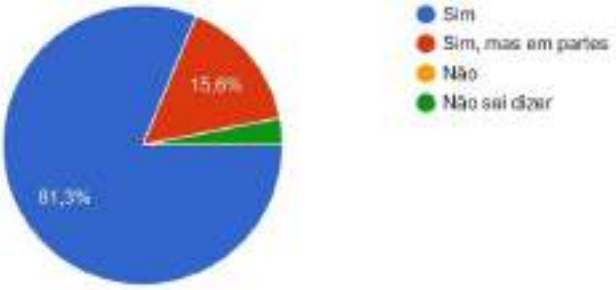
7) Quantas horas por semana você dedicou a plataforma ?

32 respostas

Fonte: Próprio autor

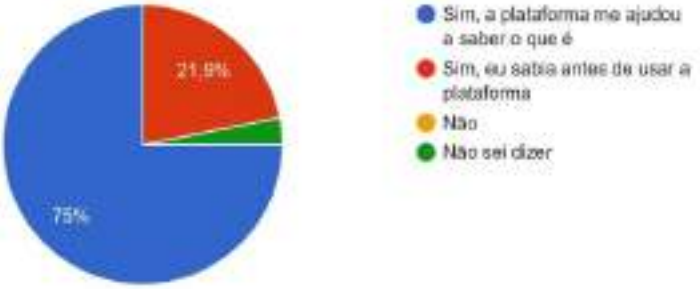
8) A plataforma foi intuitiva ?

32 respostas



9) Você sabe o que é um vírus?

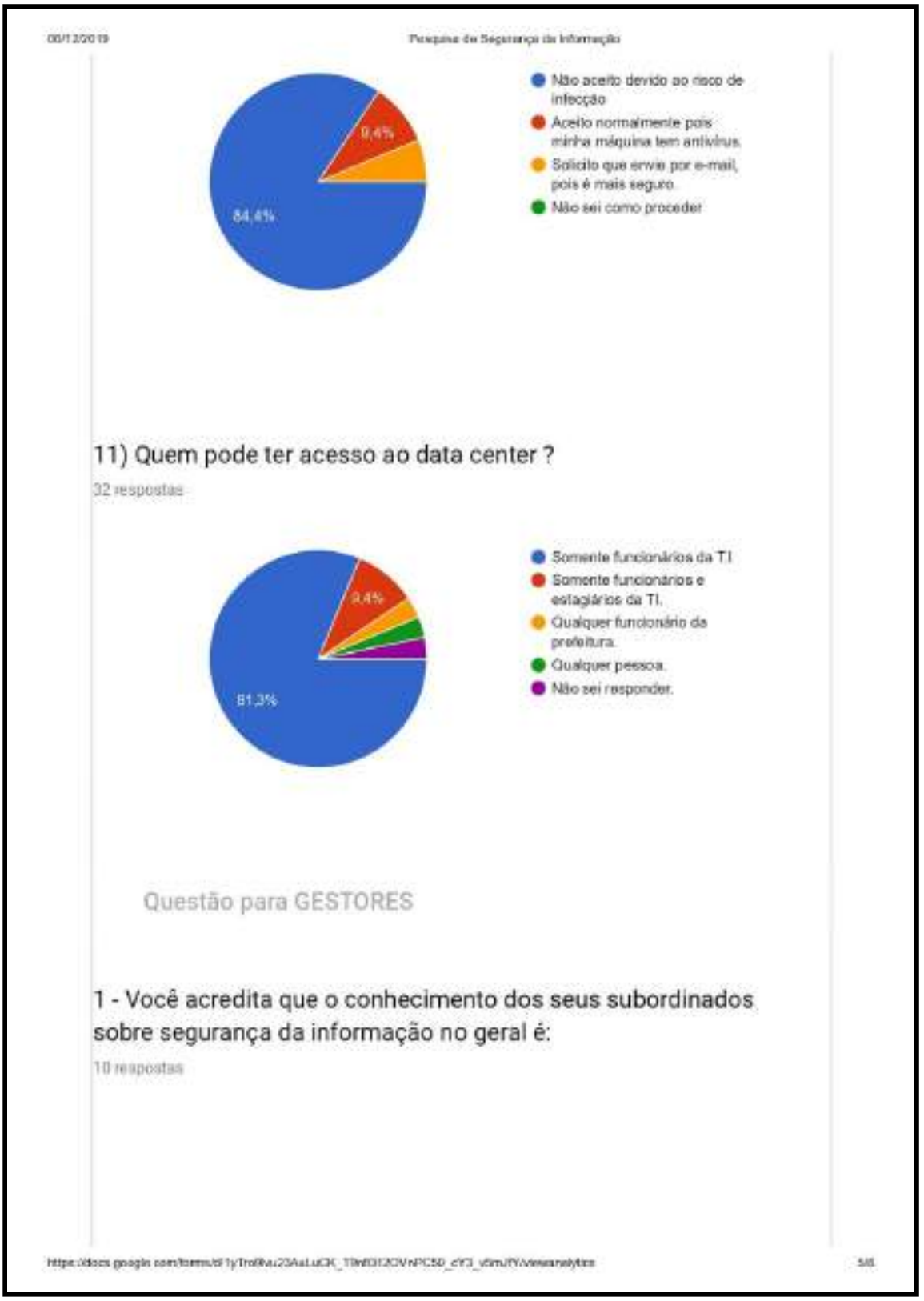
32 respostas



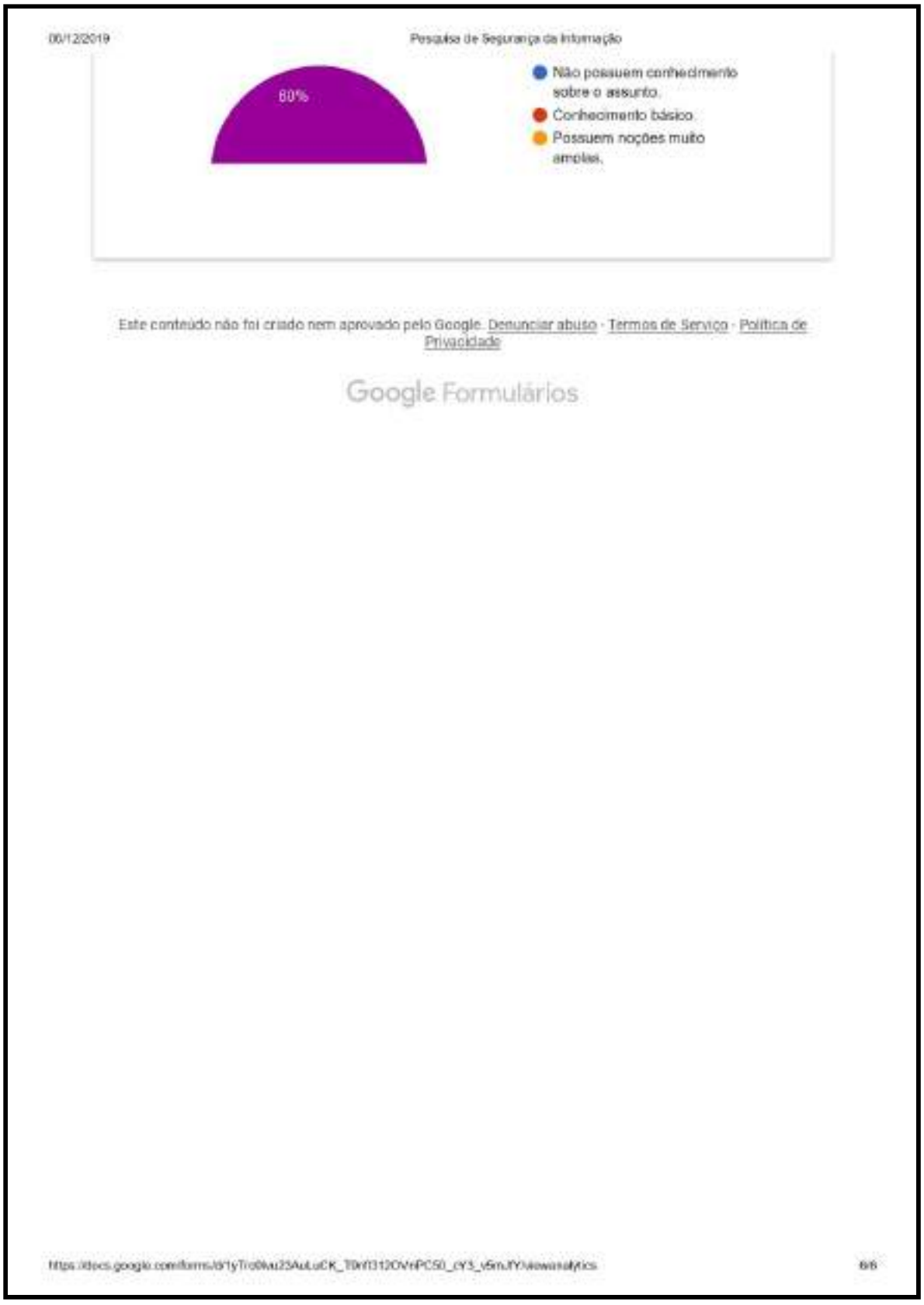
10) Caso alguém lhe passe arquivos em um Pen Drive, você:

32 respostas

Fonte: Próprio autor



Fonte: Próprio autor



Fonte: Próprio autor