FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Rita de Cássia Giusti Xavier

QR CODES CRIPTOGRAFADOS

Um estudo de caso de pingente para identificação animal

Americana, SP

2018

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Rita de Cássia Giusti Xavier

QR CODES CRIPTOGRAFADOS

Um estudo de caso de pingente para identificação animal

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof.ª Dr. Maria Cristina Aranda

Área de concentração: Segurança da Informação

Americana, SP.

2018

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

X23u XAVIER, Rita de Cássia Giusti

Um estudo de caso de pingente para identificação animal. / Rita de Cássia Giusti Xavier. – Americana, 2018.

71f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Dra. Maria Cristina Aranda

1 Reconhecimento óptico de caracteres 2. Criptografia I. ARANDA, Maria Cristina II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.6

Rita de Cássia Giusti Xavier

QR CODES CRIPTOGRAFADOS

Um estudo de caso de pingente para identificação animal

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof.ª Dr. Maria Cristina Aranda

Área de concentração: Segurança da Informação

Americana, 07 de dezembro de 2018.

Banca Examinadora:

Maria Cristina Aranda
Doutora
Faculdade de Tecnologia de Americana

Edson Roberto Gaseta
Especialista
Faculdade de Tecnologia de Americana

Maria Elizete Luz Saés
Mestre
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradeço aos meus pais, Selma e Jeferson, pela ajuda, paciência e compreensão nessa etapa. Ao Guilherme, por estar ao meu lado mesmo em tempos difíceis e estafantes. À minha orientadora Prof.ª Maria Cristina por toda compreensão e paciência. À Prof.ª Maria Elizete por toda ajuda e carinho.

E ao Deus e a Deusa, por me guiarem nesse novo caminho com sabedoria e harmonia.

DEDICATÓRIA

Aos mais de 30 milhões de animais abandonados que vivem nas ruas do Brasil, aos 23 milhões de animais silvestres mortos anualmente pelas mãos do homem e a todos os que, como eu, lutam para proteger o bem-estar e vida desses seres tão importantes e indefesos.

RESUMO

Esse trabalho teve grande motivação devido ao aumento significativo dos animais de estimação como alternativa aos filhos nos lares brasileiros, e ao seu *status* de membro da família, além de sua maior vulnerabilidade a desaparecimentos, abandonos, fugas e furtos. Apresentando uma contextualização histórica e tecnológica do QR Code seguro e sua utilidade e funcionalidade no pingente de identificação e localização de animais domésticos RegPet. Foram utilizados métodos de pesquisa pertinentes ao objetivo do trabalho, como pesquisa qualitativa e quantitativa, além do estudo de caso do RegPet. Assim, podendo apresentar a funcionalidade do QR Code seguro como alternativa às antigas tecnologias utilizadas em pingentes de identificação animal, mantendo a funcionalidade e aumentando a segurança das informações de tutores e animais.

Palavras Chave: QR Code; Criptografia; Animais de estimação.

ABSTRACT

This paper was motivated by the significant increase of pets as an alternative to children in Brazilian families, and at the same time due to their status as members of the family, and also to their greater vulnerability to disappearances, abandonments, escapes and thefts. Coming up with a historical and technological context of the QR secure Code, its utility and its functionality on the pet's identification and localization gadget called RegPet. Cientific relevant methods to the objective of the study were used, such as qualitative and quantitative researches, and also the RegPet case study. Thus, it can present the functionality of the secure QR Code as an alternative to old technologies used in pet identification pendants, maintaining the functionality and increasing the information security of tutors and pets.

Keywords: *QR Codes; Encryption; Pets.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS E GRÁFICOS

1 INTRODUÇÃO

A sociedade contemporânea está vivendo, conforme os pesquisadores, na chamada "Aldeia Global". E, Aldeia Global para Ianni (1996, p. 16) é uma comunidade mundial onde além de mercadorias, também se comercializa um novo produto: a informação. O planeta tornou-se um lugar onde praticamente tudo está conectado e a maioria dos dados pessoais trafega na rede mundial de computadores, assim, mais do que nunca é necessário zelar pela segurança dos dados disponíveis nos dispositivos usados, sejam eles conectados à *Internet* ou não.

Segundo a norma ABNT ISO/IEC 27002 (ABNT, 2013) segurança da informação é “proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou organização [...] o seu embasamento consiste em manter a integridade, disponibilidade, autenticidade e confidencialidade dos dados.”

Nessa sociedade, cada vez mais caótica e instável, as pessoas estão preferindo adotar animais a ter filhos. Segundo pesquisa publicada pelo jornal espanhol *El País*, feita pelo IBGE (Instituto Brasileiro de Geografia e Estatística), em 2015, de cada 100 famílias, 44 criam animais e somente 36 tiveram filhos biológicos ou adotaram crianças. As famílias brasileiras, em 2015, tinham cerca de 52 milhões de cães *versus* 45 milhões de crianças.

Os métodos de identificação de animais são usados há muito tempo por seus tutores para manter a segurança dos mesmos; são utilizados dispositivos como *chips* subcutâneos, também chamados de *transponders,* além de outros métodos, como anilhas, brincos, entre outros.

Nos dias de hoje os animais de estimação são tratados como verdadeiros membros da família: são levados com mais frequência para consultas veterinárias, opta-se pela castração, faz-se uso de serviços de banho e tosa, *spas*, creches, aulas de educação física e até consultas nutricionais. Então, percebe-se a necessidade do tutor querer identificar e ter controle sobre os dados do animal (data de nascimento, endereço, telefone dos tutores, além de dados sobre vacinas e doenças que ele já possuiu ou possui) e por onde ele anda, observando a demanda cada vez maior de cuidado e segurança dos dados, mantendo-os confiáveis e disponíveis para serem acessados pelas pessoas certas.

Foi pensando nesse novo público que esta autora estudou os QR Codes como opção para facilitar a utilização de dispositivos de identificação e localização de animais de estimação, já que com a evolução tecnológica, os QR Codes podem ser criptografados, mantendo a segurança dos dados do tutor e animal, e também podem oferecer localização geográfica. Com base nesse estudo, o RegPet foi desenvolvido e utilizado como estudo de caso no presente trabalho.

O **objetivo geral** era o estudo da funcionalidade dos QR Codes criptografados e sua utilização no dispositivo de identificação e localização animal RegPet e compreender a importância do pet como parte da família do tutor, e também a importância de manter a segurança dos dados tanto do tutor, quanto do próprio animal.

Como **objetivos específicos** destacam-se**:**

1. O estudo da história, tipificação e funcionalidade dos QR Codes, com objetivo de compreender por que eles podem ser utilizados no dispositivo sem perda de qualidade e com ganho em segurança;
2. Compreender o funcionamento dos QR Codes seguros e como a segurança é implementada nesses códigos, além de compreender os tipos de criptografia utilizados nos QR Codes seguros e seu funcionamento;
3. Demonstrar o dispositivo RegPet como um todo, englobando os QR Codes e protocolos de segurança utilizados.

O **método científico** de pesquisa utilizado foi o indutivo, que segundo Chalmers (1993),

> [...] é o raciocínio que, após considerar um número suficiente de casos particulares, conclui uma verdade geral. A indução, ao contrário da dedução, parte de dados particulares da experiência sensível. De acordo com o indutivista, a ciência começa com a observação. A observação, por sua vez, fornece uma base segura sobre a qual o conhecimento científico pode ser construído, e o conhecimento científico é obtido a partir de proposições de observação por indução.

Para o desenvolvimento da **pesquisa**, foram utilizados os métodos:

a) **Levantamento por pesquisa quantitativa**, nos questionários aplicados para compreender quais métodos e até quanto os tutores estariam dispostos a pagar pelo dispositivo estudado;
b) **Levantamento por pesquisa qualitativa**, nos questionários aplicados para melhor compreensão da importância dos animais para os tutores;
c) **Pesquisa bibliográfica**, para estudar a história, tipos de QR Codes, funcionalidades, criptografia, entre outros assuntos tratados neste trabalho;

d) **Estudo de caso** do RegPet e utilização do QR Code em seu dispositivo de localização e identificação animal.

O trabalho foi estruturado em seis capítulos, sendo o primeiro capítulo reservado para a introdução ao trabalho; o segundo capítulo trata do QR Code, sua história, funcionalidade e tipificação; no terceiro capítulo é feita a explicação sobre QR Codes seguros e métodos de segurança para o código; o quarto capítulo trata de criptografia em QR Codes, funcionamento dos algoritmos utilizados e uma pequena explicação sobre a ferramenta QRyptal, utilizada no RegPet; já no capítulo cinco é feito o estudo de caso do dispositivo RegPet, sua funcionalidade e como o QR Code seguro é aplicado nele.

Em posse das informações obtidas a partir dos estudos feitos nos capítulos anteriores, o capítulo seis reserva-se às considerações finais e sugestões de trabalhos futuros.

Nos apêndices também são apresentadas as pesquisas feitas pelo autor, além de prints do site e documentação sobre o aplicativo e dispositivo estudados.

Espera-se que o desenvolvimento dessa pesquisa possa contribuir com o avanço da tecnologia em dispositivos para identificação e localização de animais de estimação, mantendo a funcionalidade e aumentando a segurança dos dados armazenados.

2 O QUE É UM QR CODE

Os códigos de barras que estão impressos nos produtos que se encontram nos supermercados são códigos legíveis por máquinas produzidas especialmente para esse objetivo. Essas leitoras utilizam a luz infravermelha para fazer compreender os dados que estão contidos no mesmo, onde há um espaço escuro, a luz é absorvida, já onde há um espaço claro, a luz é refletida de volta para a leitora, que transmite esses dados para um processador (computador com um *software* instalado) que converterá as reflexões da luz em letras e números.

Os primeiros códigos de barras foram patenteados por Joseph Woodland e Bernard Silver em 1952, que consistia em um código de padrões circunferenciais e linhas de espessuras variáveis. Os códigos de Woodland-Silver só foram testados em 1969, pela cadeia de supermercados Kroger, nos EUA, por 18 meses. Porém, mesmo com o sucesso e a diminuição de custos operacionais, a universalização do sistema demorou mais de duas décadas para acontecer. No Brasil, ele foi introduzido formalmente, somente em 29 de novembro de 1984.

Na figura 1 é apresentado um exemplo de código de barras do padrão EAN-143, utilizado mundialmente (exceto nos EUA e Canadá), inclusive no Brasil, onde a barra preta significa números 1 e os espaços em branco significam números 0, utilizando o sistema de base decimal para converter os números binários (0 e 1) em números complexos e maiores.

Figura 1 - Código de barras

Fonte: GS1BR[1]

[1]Adaptado de GS1br. Disponível em <www.gs1br.com.br>. Acesso em: 18 ago. 2018.

Os códigos de barras ainda são utilizados, porém, em algum momento na década de 90 para algumas empresas eles se tornaram obsoletos, sendo necessária a criação de um código que suportasse o armazenamento de uma quantidade maior de dados, mais resistentes fisicamente e com a correção de erros mais eficiente. Assim, foram criados os QR Codes (*Quick Response Codes*, ou Códigos de Resposta Rápida, em tradução livre da autora) que são "códigos de barras modernizados" desenvolvidos e implementados pela empresa Denso Wave Incorporated (uma divisão da Denso Corporation) em 1994, para gerir e catalogar peças da linha de produção de suprimentos para automóveis.

QR Codes são códigos de barras bidimensionais, que podem ser lidos por equipamentos genéricos com um *software* de escaneamento instalado e que tenha uma câmera. Geralmente os QR Codes são lidos por *smartphones* com aplicativos de leitura instalados, que podem ser facilmente adquiridos em lojas digitais (App Store, Play Store, Windows Store) gratuitamente. Os códigos são convertidos em textos interativos como endereços de *URL*, endereços de *e-mail*, localização geográfica, contatos pessoais (números de telefone, endereços, dados importantes), entre outros.

2.1 A história do QR Code

Segundo pesquisas divulgadas pela Denso Wave Incorporated, na década de 60, durante o *boom* do comércio japonês na área de *commodities*, houve uma grande disseminação de pequenos comércios de bairro no país. O volume de compras era tanto e os funcionários dos caixas precisavam digitar manualmente os valores, que houve um aumento considerável de pessoas com doenças como tendinites e síndrome do túnel do carpo; com a implementação do código de barras, esse problema foi solucionado, porém o código só comportava vinte caracteres alfanuméricos em sua memória, o que passou a ser um problema para algumas empresas e lojas, já que o alfabeto japonês tem caracteres diferenciados, não só alfanuméricos.

Os usuários acabaram por contatar a Denso Wave para que desenvolvessem um código de barras que tivesse capacidade de codificar caracteres como *kanjis* e *kanas*, além dos alfanuméricos. Então, Masahiro Hara, contratado pela Denso Wave, ficou no comando da equipe (de duas pessoas) que desenvolveu o código bidimensional, com o foco em fazer uma leitura rápida e não somente em guardar

grandes quantidades de dados. Assim, depois de um ano e meio, os pesquisadores chegaram a um padrão de detecção composto de pequenos quadrados que disponibilizam a leitura vertical e horizontal, e com leitura em velocidade dez vezes maior e capacidade de codificar cerca de 7.000 caracteres, entre eles números, letras, *kanjis* e *kanas*.

O padrão quadrado foi escolhido para que a detecção seja mais rápida, já que ele seria menos provável de aparecer em impressões próximas ao código. Assim, para evitar que a leitura fosse errônea, foram analisadas as proporções de áreas pretas e brancas em vários tipos de materiais, criando então uma proporção de 1:1:3:1:1 de preto e branco. Então, foi criado um dispositivo através do qual a orientação de seu código poderia ser determinada independentemente do ângulo de varredura, que poderia ser qualquer ângulo fora de 360º, sempre procurando pela proporção de 1:1:3:1:1 única.

Figura 2 - Modelos de QR Code

Fonte: QRCode.com[2]

Em meados dos anos 2000 o QR Code já era amplamente divulgado no Japão, devido a incidentes com BSE (encefalopatia espongiforme bovina, conhecida como doença da vaca louca) no país, que fizeram as pessoas exigirem processos de produções mais transparentes e produtos rastreáveis para compreender o que teriam para oferecer para suas famílias, especialmente no caso de produtos farmacêuticos e alimentícios. Essa divulgação também foi facilitada pela tendência de telefones celulares com leitores de QR Codes, que possibilitam a pessoa acessar endereços *URL* e outros dados complexos simplesmente apontando suas câmeras para o código impresso em algum local visível.

O QR Code é um código aberto e apesar de ser patenteado pela Denso Wave Incorporated pode ser utilizado por pessoas de todo o mundo, com padrões

[2]Disponível em <www.qrcode.com>. Acesso em: 19 ago. 2018.

registrados para uso internacional pela ISO, como se pode observar na tabela 1, o que padroniza seu uso mundialmente.

Tabela 1 - Padronização dos QR Codes

Outubro de 1997	Aprovado como padrão AIM International (Identificação Automática de Fabricantes Internacionais) – Padrão ISS QR Code
Março de 1998	Aprovado como padrão na JEIDA (Associação Japonesa de Desenvolvimento da Indústria Eletrônica) – Padrão JEIDA-55
Janeiro de 1999	Aprovado como padrão JIS (Japanese Industrial Standards) – Padrão JIS X 0510
Junho de 2000	Aprovado como padrão internacional ISO – Padrão ISO / IEC18004
Novembro de 2004	Código QR Micro: Aprovado como padrão JIS (Padrões Industriais Japoneses) – JIS X 0510
Dezembro de 2011	Aprovado pela GS1, organização internacional de padronização, como padrão para telefones celulares

Fonte: Adaptado de QRCode.com

Com o avanço da tecnologia os QR Codes também evoluíram e se sofisticaram. Em 2004 foi criado o Micro QR Code, aprovado como padrão JIS X 0510, que pode ser impresso em superfícies pequenas sem o risco de erro de detecção. Já em 2008 um módulo que permite padrões retangulares foi criado, o iQR Code. Em 2014 foi introduzido no mercado o FrameQR, que combina *design* e funcionalidade, onde se pode combinar a arte da empresa ou objetivo e os dados necessários ou desejados. Além da melhora da funcionalidade e estética, também foram implementadas restrições de leitura e aprimoramento de graus de privacidade e confidencialidade para aumentar os níveis de segurança da informação, já que os dados contidos no código estão cada vez maiores, mais importantes e pessoais.

2.2 Tipos de QR Code

Os QR Codes sofreram modificações e avanços tecnológicos com o tempo e com a demanda. A seguir será feita uma explanação sobre cada um dos tipos, suas capacidades, forma de leitura, velocidade, entre outras características.

2.2.1 QR Code Original (QR Code Modelo 1 e Modelo 2)

O QR Code original, ou QR Code modelo 1 ou modelo 2, são os códigos originais desenvolvidos pela Denso Wave Incorporated na década de 1990.

O primeiro modelo QR Code é capaz de codificar (e armazenar) mais de 1.167 caracteres; com sua versão máxima sendo 14, ou seja, 73 x 73 módulos = 2.192 caracteres.

Figura 3 - QR Code Modelo 1

Fonte: QRCode.com

Na figura 3 pode-se ver um exemplo do QR Code do modelo 1, com 14 módulos e o padrão quadrado original.

Já o segundo modelo é capaz de armazenar mais de 7.089 caracteres (com sua versão máxima sendo 40, ou seja, 177 x 177 módulos = 23.648 caracteres); outra modificação feita do modelo 1 para o modelo 2 é a capacidade de fazer a impressão desse código em superfícies curvas sem risco de erro de leitura.

Na figura 4 observa-se um exemplo do QR Code do modelo 2, com 40 módulos e o padrão quadrado original.

Figura 4 - QR Code Modelo 2

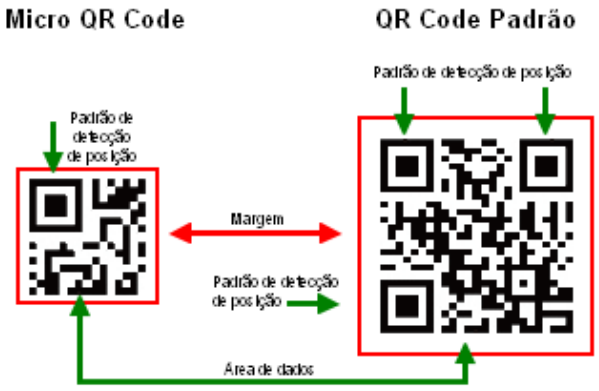
Fonte: QRCode.com

É possível notar que a diferença visual é quase imperceptível, porém a capacidade de armazenamento é extremamente diferenciada do padrão original, podendo conter até dez vezes mais caracteres.

2.2.2 Micro QR Code

A principal diferença entre o QR Code original e o Micro QR Code é a redução da área de detecção de posição: no Micro QR Code há somente uma área, enquanto no original são necessárias três áreas nos cantos do símbolo maior. Há também a diferença entre a margem nula de pelo menos quatro módulos que é necessária no código original; no Micro QR Code é necessária somente uma margem larga de dois módulos, sendo isso o suficiente para a detecção de erros e maior velocidade para a leitura. Assim, a área de impressão do Micro QR Code é menor. Essas diferenças podem ser observadas graficamente na figura 5.

Figura 5 – Diferenças entre QR Codes padrão e Micro QR Codes

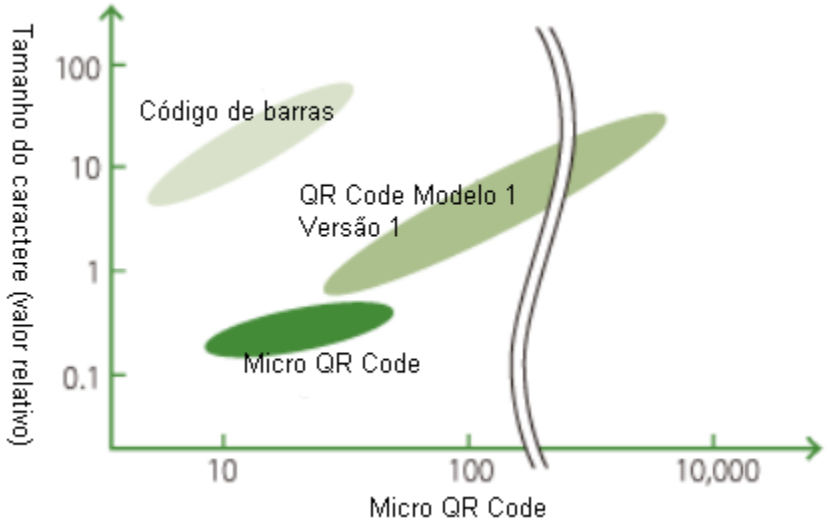


Fonte: Adaptado de QRCode.com

Por ter uma área menor de impressão, o Micro QR Code também tem uma capacidade menor de armazenamento de dados (cerca de 35 caracteres alfanuméricos), e apesar de ser um código com maior velocidade e eficiência que o QR Code original para codificação dos dados, ele não é indicado se a necessidade do usuário for de grande armazenamento.

Esse tipo de QR Code tem quatro variações: a menor delas armazena 5 caracteres e a maior até 41.

Gráfico 1 – Comparação de armazenamento entre QR Code Modelo 1 e Micro QR Code



Fonte: Adaptado de QRCode.com

No gráfico 1 pode-se observar a comparação de armazenamento entre os dois modelos de QR Code (Micro e Modelo 1 original, versão 1) e a diferença entre eles e o código de barras.

O padrão Micro QR Code foi aprovado em 2004 como JIS X 0510, pelos Padrões Industriais Japoneses.

2.2.3 iQR® Code

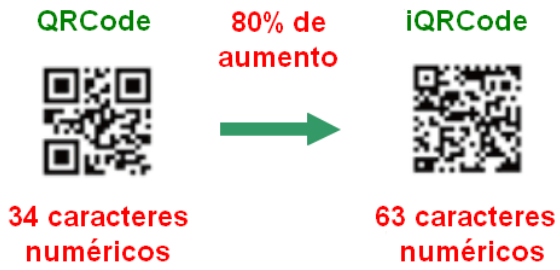
O iQR Code é um dos subtipos de QR Codes com patente exclusiva da Denso Wave Incorporated (Corporation), o que significa que não pode ser livremente usado sem o pagamento de *royalties* (direitos autorais) ou autorização da empresa.

Esse tipo de QR Code é uma matriz de leitura fácil permitindo ampla gama de códigos (menores que o QR Code tradicional e maiores que o Micro QR Code); seu

maior diferencial é poder ser impresso em formato retangular, em formato invertido, em cor invertida e também em padrões diferenciados de pontos, o que permite uma maior gama de aplicações desse código. Com essa diferenciação de formatos e padrões de pontos, há também a possibilidade de um código iQR ter o mesmo tamanho de um QR Code tradicional e comportar 80% a mais de dados, como pode ser visto nas figuras 6 e 7.

Figura 6 – Diferenças entre QR Codes Parão e iQR Codes

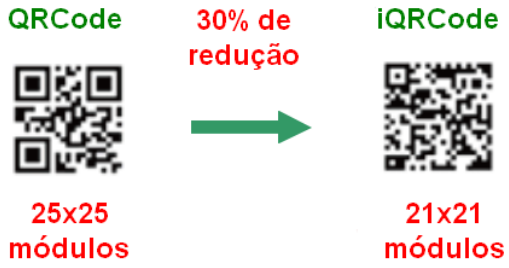
Aumento de capacidade de armazenamento de dados



Fonte: Adaptado de QRCode.com

Figura 7 - Diferenças entre QR Codes Parão e iQR Codes

Redução de área de impressão

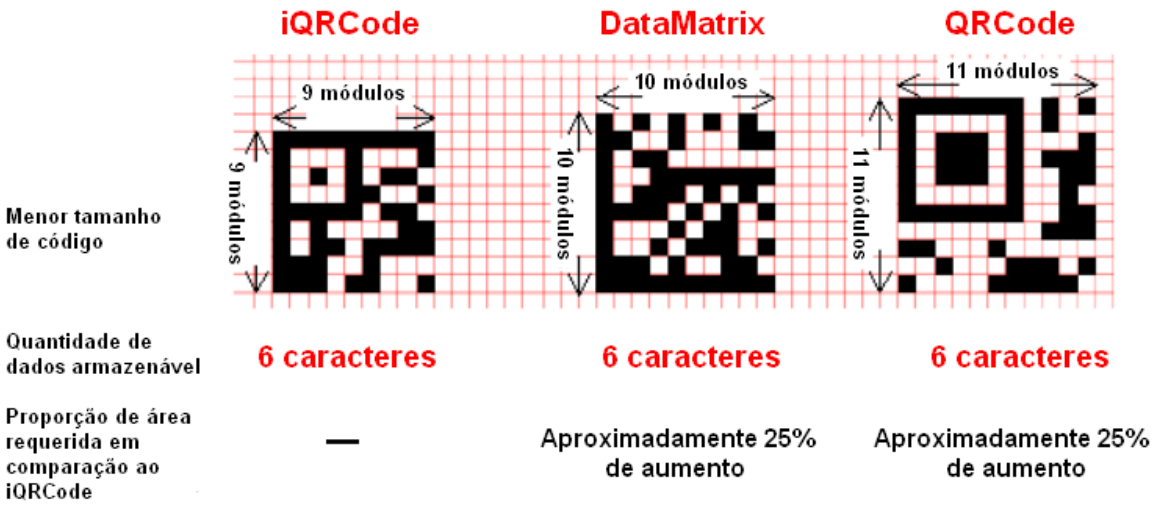


Fonte: Adaptado de QRCode.com

O iQR Code também pode comportar a mesma quantidade de dados de um QR Code tradicional e ter uma superfície de impressão 30% menor, como na figura acima, podendo chegar a uma redução de 60%.

Outra diferenciação do iQR Code é seu tamanho reduzido, como pode ser observado na figura 8.

Figura 8 – Comparação entre iQR Codes, Data Matrix e QR Codes padrão



Fonte: Adaptado de QRCode.com

A redução é visível, o que faz o iQR Code ser uma ferramenta interessante para empresas que necessitam armazenar dados gravados diretamente em seus produtos, tendo em vista esses dados são maiores do que os gravados em um código de barras convencional, e menores do que os que poderiam ser gravados em um QR Code tradicional. Em um formato quadrado, o iQR Code pode armazenar mais de 40.000 caracteres numéricos.

A impressão do iQR Code em formato retangular também é um grande diferencial, com esse recurso, pode-se imprimir um QR Code no local onde seria impresso um código de barras convencional, porém com uma capacidade de armazenamento muito maior. Também é possível imprimir esse código em produtos cilíndricos (arredondados, entre outros) mantendo sua capacidade e velocidade de leitura, o que não seria possível com um QR Code tradicional em impressão e módulos quadrados.

O iQR Code também tem uma capacidade de restauração (correção de erros) 20% maior que o de um QR Code tradicional. Em um QR Code tradicional essa correção de erros é de 20%, já no iQR Code ela pode chegar a 50%.

2.2.4 FrameQR® Code

O FrameQR Code é um QR Code também patenteado e de uso exclusivo pela Denso Wave, *royalties*.

O código FrameQR tem a mesma capacidade de um QR Code tradicional, porém pode conter uma ilustração no centro, ou alguma modificação gráfica: pode ser colorido, conter outras formas geométricas, entre outras.

2.2.5 SQRC® Code (Secure QR Code)

O SQRC Code também é um QR Code também patenteado e de uso exclusivo pela Denso Wave, devendo pagar *royalties* para uso externo.

O SQRC é um código QR com restrição de leitura, ou seja, só pode ser lido por aplicativos específicos. Em geral é usado em empresas para acesso restrito a informação secreta, porém sua arquitetura não assegura que o conteúdo armazenado no QR Code também seja criptografado, ou seja, é necessário tomar providências quanto a isso caso necessário.

O SQRC utiliza o sistema de *PKI* (infraestrutura de chaves públicas) para controlar o acesso, sendo possível guardar até dois níveis de informação no mesmo código.

Outros QR Codes seguros foram criados baseados no SQRC Code, e em sua maioria utilizam das mesmas infraestruturas de segurança e níveis de informação, porém com tecnologias mais avançadas. Como o caso do CRyptal, que foi estudado neste trabalho.

Em capítulo posterior será explicado em detalhes o funcionamento do QR Code seguro e sua infraestrutura de segurança.

2.3 Como funciona o QR Code

O QR Code, como dito anteriormente, é um código em duas dimensões, o que o diferencia grandemente do seu antecessor, o código de barras. O código de barras pode ter seus dados processados graças a um feixe de luz que sai das máquinas leitoras criadas especificamente para esse fim. Já o QR Code trabalha com a leitura digital, onde cada “quadradinho” de seu desenho é “montado” em um padrão que pode ser lido através da câmera de um celular (*smartphone*, tabletes, entre outros)

facilmente, apenas apontando-a para o código, visto que a maioria dos aparelhos já tem um leitor de QR Code nativo, ou seja, já vem com o leitor instalado em seu sistema.

O QR Code é composto de *pixels* pretos, sendo eles pequenos ou grandes, conforme sua funcionalidade. Esses *pixels* são chamados de módulos, e eles representam graficamente o conteúdo que está armazenado no código.

Percebe-se que o QR Code tem três grandes módulos que se destacam, um módulo um pouco menor em seu canto direito e pequenos módulos espalhados por toda sua extensão. Cada um têm sua funcionalidade específica, como pode-se observar na figura 9.

Figura 9 – Composição e funcionamento do QR Code

Fonte: Próprio autor

Nos quadrados destacados em vermelho observa-se o que é chamado de *fiding pattern*, ou seja, padrão de localização; eles ocupam três módulos cada um e permitem que o leitor do código identifique a posição dos módulos no QR Code e determinem a posição correta em que deveriam estar, assim, quando alguma modificação for detectada, o leitor não irá redirecionar o usuário para o conteúdo,

prevenindo ataques de códigos maliciosos. Os módulos em roxo são os chamados de *timing patterns*, os padrões de tempo, que são módulos alternadamente preto e brancos e determinam a coordenação do código, localizados sempre entre os padrões de localização. O que está destacado em azul é o *alingment pattern*, ou padrão de alinhamento, que são os módulos responsáveis por ajudar o leitor caso o código esteja distorcido ou impresso em alguma superfície irregular. O módulo destacado em bordô é o responsável por mostrar ao leitor qual a versão do código que está sendo processado e é chamado de *format information*, ou informação de formato. Em verde tem-se as *quiet zones*, ou zonas de margem, que delimitam o tamanho do código. Os módulos em amarelo representam os *pixels* de 8 *bits* onde os dados estão decodificados, ou seja, onde a informação do QR Code está armazenada. E por último, os módulos destacados em cinza, que são os corretores e detectores de erro.

Apesar de ser uma tecnologia relativamente nova, *o* QR Code já é amplamente utilizado, e teve um crescimento do seu uso, como divulgado em pesquisa da empresa de tecnologia Pitney Bowes,

> [...] os códigos de resposta rápida estão ganhando aceitação cada vez maior entre os consumidores da América do Norte e Europa, sendo os veículos impressos os que mais fomentam esta interação, alcançando 15% dos 3.000 entrevistados. Na sequência aparecem os Correios e embalagens, na casa dos 13%, seguido de cartazes, com 10%, *website* e *e-mail*, com 8% e 5%, respectivamente e por fim, TV, com 4% do uso. (PITNEY BOWES, 2016)

Assim, os QR Codes se modernizaram e contam com sistemas diferenciados e mais potentes de detecções e correções de erro e leitura.

Hoje em dia os códigos contam com o algoritmo Reed-Solomon de correção de erros, um conjunto de códigos de correção de erros cíclicos e não-binários criados por Irving S. Reed e Gustave Solomon em 1960, no qual descreveram sistematicamente, uma cadeia de códigos capazes de detectar erros aleatórios em símbolos diferenciados. Segundo Reed e Solomon (1960),

> [...] ao adicionar ***t*** símbolos de verificação aos dados, um código Reed-Solomon pode detectar qualquer combinação de até ***t*** símbolos errados, e corrigir até ***t / 2*** símbolos. Como *erasure code* consegue corrigir até t faltas conhecidas, ou pode detectar e corrigir uma combinação de erros e faltas. Além disso, os códigos RS são adequados como códigos de correção de *multiple-burst bit-error*, uma vez que uma sequência de ***b + 1*** erros consecutivos afeta no máximo dois símbolos de tamanho ***b***, onde a escolha de ***t*** é arbitrária sendo efetuada pelo criador do código, e podendo ser selecionada dentro de limites amplos.

Então, os códigos contam com quatro níveis conhecidos de detecção de erros, sendo eles observados na tabela 2.

Tabela 2 – Nível de correção de erros do Algoritmo Reed-Solomon em QR Codes

NÍVEL	SÍMBOLO	PODER DE CORREÇÃO (%)
Baixo	L	7%
Médio	M	15%
Quarto	Q	25%
Alto	H	30%

Fonte: Próprio autor

Nessa porcentagem de correção, é entendido que no nível baixo (L), 7% do que está contido na parte danificada do código pode ser restaurado, 15% no nível médio (M), e assim por diante.

Explanada a história, tipificação e funcionalidade dos QR Codes, o próximo capítulo será dedicado à proteção do código e a importância da segurança da informação de um QR Code.

3 QR CODE SEGURO

Um QR Code seguro pode ser um código criptografado em si ou também pode-se optar por encriptar seu conteúdo, ou seja, a informação contida no código. Também há a opção de assinar o código: imprimi-lo com a marca de um produto ou empresa, mas não seria uma opção totalmente segura, pois o código pode facilmente ser pirateado ou copiado. Outra opção para deixar um QR Code mais seguro seria criá-lo protegido por uma senha.

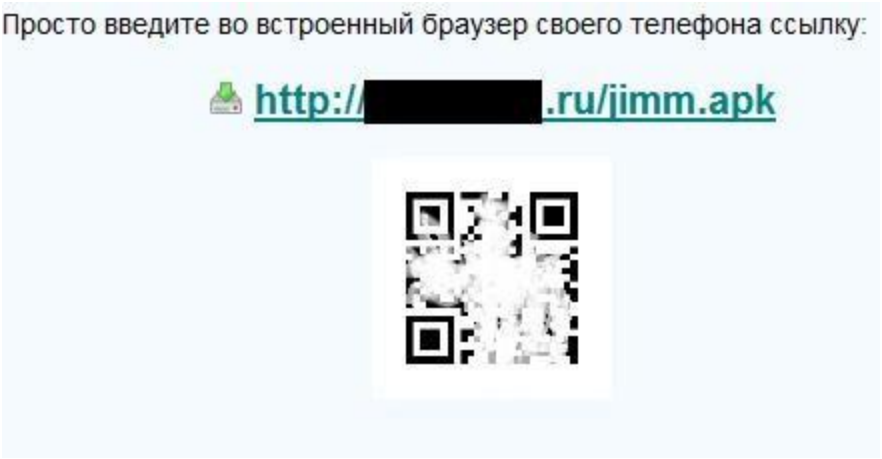
Nos tópicos a seguir será explicado mais sobre as vulnerabilidades de um QR Code, ataques maliciosos que podem usar o QR Code e como proteger o código para um uso seguro.

3.1 Por que proteger um QR Code

Em setembro do ano de 2011, a empresa de segurança da informação Kaspersky Lab, responsável pelo desenvolvimento do antivírus Kaspersky, detectou o primeiro QR Code malicioso. Ele direcionava o usuário que fazia a leitura do código para um site de conteúdo duvidoso e fazia *download* desse conteúdo no dispositivo que realizou a leitura, sem o conhecimento do usuário.

O QR Code pode ser usado como vetor, ou seja, como meio de disseminar vírus e *softwares* maliciosos, como Cavalos-de-Tróia que são capazes de mandar mensagens de aplicativos (WhatsApp, Telegram, entre outros) sem consentimento do usuário do dispositivo. Um exemplo desse tipo de ataque foi o acontecido em 2011 na Rússia, quando, após lido, o QR Code induzia o dispositivo a baixar um aplicativo chamado Jimm que enviava mensagens custando cerca de seis dólares cada, o que acarretava altas nas contas telefônicas e o usuário não sabia de onde vinha esse gasto extra. Na figura 10 observa-se como o Jimm era apresentado para os usuários.

Figura 10 – Apresentação do *Malware* Jimm



Fonte: Securelist[3]

O Jimm foi o precursor dos ataques de QR Code como vetor de *softwares* maliciosos. Hoje em dia muitas pessoas ainda se aproveitam da ingenuidade dos usuários para usar dos QR Codes como vetores de vírus e programas maliciosos, mas eles estão cada dia mais perigosos, já que o QR Code "infectado" não pode ser identificado a olho nu, por ser igual ao código sadio.

Dentre os ataques que usam o QR Code como vetor, estão os ataques automatizados, por *bots* ou por *scripts*. Um desses tipos de ataque são os ataques por injeção de SQL, ou seja,

> [...] Considere um cenário em que um scanner (software de decodificação de QR Code) é conectado a um banco de dados e as informações de QR Code são usadas para executar uma consulta no banco de dados de back-end. Nesse cenário, se o QR Code contiver uma consulta como "1 'OR' 1 '=' 1" (sem as aspas), o leitor poderá executar a consulta sem verificar se ela vem ou não de uma fonte autenticada. pode levar à exibição de informações para um hacker em potencial que é destinado a um usuário autorizado. (SHARMA, 2012)

Assim, com o avanço da tecnologia e os QR Codes sendo usados para acesso à *links* de *logins* em bancos de dados ou perfis privados, esses dados podem ser acessados por pessoas com intenções duvidosas.

Outro tipo de ataques são os de exploração baseada em navegadores conjuntos aos de *cross-site scripting* (também conhecido como XSS), que são vulnerabilidades de sistemas de segurança de computador ou em navegadores (ou

[3]Disponível em <https://securelist.com/en/blog/208193145/Its_time_for_malicious_QR_codes>. Acesso em: 10 out. 2018.

servidores *web*) que ativam ataques maliciosos dentro de páginas *web* (*sites*) por meio de pequenos *scripts* em JavaScript, já que essa linguagem costuma ser persistente na página. Já que um QR Code pode conter um *link* com uma *URL*, que pode redirecionar o usuário para um *site* que contenha um *script* malicioso, assim podendo causar danos ao navegador ou ao dispositivo do usuário quando acessado.

Outro tipo de ataque que utiliza o QR Code como vetor é o de injeção de comando, ou injeção de código.

> [...] Um invasor pode facilmente explorar a vulnerabilidade alterando o QR Code e, assim, executar comandos arbitrários no sistema. Desta forma, um invasor pode instalar *rootkits, spywares*, iniciar um ataque de negação de serviço (DoS) ou conectar um *shell* a um computador remoto e acessá-lo de onde estiver. (SHARMA, 2012)

Também existem os ataques baseados em interação humana, ou seja, ataques que dependem da interação ou de um *start* do usuário para que sejam ativados. Um deles é chamado de *phishing* (pescar, ou seja, fisgar o usuário) e é amplamente utilizado por usuários maliciosos em vários tipos de ataques, com ou sem QR Code. Com o QR Code o *phishing* pode ser utilizado como no ataque de XSS, onde quando o código é lido, o usuário é redirecionado para uma página falsa onde o atacante pode se apoderar de seus dados.

Outro ataque por interação humana é a fraude, e pelo QR Code ela funcionaria também redirecionando a *URL* do usuário, porém para páginas fraudulentas. Por exemplo, se uma empresa faz uma promoção e utiliza o QR Code para redirecionar o usuário para a página do produto promocional, o atacante pode utilizar esse código para, ao invés do usuário chegar na página desejada, acabar em uma página maliciosa ou falsificada.

O QR Code também pode ser utilizado para propagar *malwares* (vírus, *worms*, cavalos-de-tróia, *spywares*, entre outros), e o invasor pode utilizar o código para que, quando ele for lido, direcione o usuário para uma página onde esse *malware* será baixado automaticamente, infectando o dispositivo do usuário.

O Jimm se encaixa em dois tipos de ataques, de interação humana e código como vetor, sendo uma mistura de propagador de *malware* e injeção de comando.

3.2 Ferramentas para proteção do QR Code

O QR Code pode ser protegido de três formas, como já mencionado, criptografando o conteúdo do código, ou a própria imagem código usando aplicativos

e *softwares* específicos e também pode-se manter o código seguro com um usuário e senha.

3.2.1 Controle de acesso de conteúdo em *QR Codes*

Para proteger um QR Code e seu conteúdo pode-se criar o código já com um tipo de "controle de acesso", que segundo Stallings (2008) é,

> [...] Limitar e controlar o acesso a sistemas e aplicações hospedeiras (ou dados) mor meio de enlaces de comunicação. Para conseguir isso, cada entidade precisa ser identificada antes de obter acesso, ou autenticada, de modo que os direitos de acesso possam ser ajustados a cada indivíduo.

Assim, esse código será acessível somente a quem tenha esses dados, através da geração de um *login* de usuário e uma senha para cada QR Code gerado dessa maneira. Esse QR Code é gerado por aplicativos e softwares específicos, em geral são pagos.

Uma das soluções tecnológicas que oferecem QR Codes com controle de acesso, ou seja, com usuário e senha, é o Scanova, que oferece um aplicativo com etapas simplificadas e em poucos passos o usuário é capaz de distribuir QR Codes com controle de acesso somente à pessoal autorizado. Esse aplicativo armazena qualquer informação ou dado que um QR Code comum armazena: documentos, *links* e mensagens, porém, sendo um QR Code totalmente personalizado, esses documentos podem ser confidenciais, os *links* podem ser de produtos personalizados a um cliente ou usuário específico e as mensagens podem também ser de conteúdo confidencial ou personalizado. Outra vantagem dessa solução é que o aplicativo oferece a opção de mudar nome de usuário e senha ou alterar o conteúdo do código para os administradores.

3.2.2 Criptografia de conteúdo em *QR Codes*

O método mais utilizado é o de criptografar o conteúdo do código, isto é, implementar um algoritmo criptográfico para encriptar, ou "esconder", o que está dentro do QR Code e somente o usuário em posse da chave desse algoritmo seria possibilitado de ler esse conteúdo.

3.2.3 Criptografia de *QR Codes*

O método de criptografar o próprio QR Code é o que demanda mais tecnologia, porém é o mais seguro. No capítulo 4 e em seus subcapítulos será explicado em detalhes como funcionam os QR Codes de chave simétrica, ou de chave privada e os QR Codes de chave assimétrica, ou de chave pública e como essas criptografias funcionam.

4 CRIPTOGRAFIA E QR CODES

Criptografia é, sem dúvida, um dos maiores meios de proteção para dados que trafegam numa rede compartilhada ou que estão armazenados em mídias tecnológicas conectadas à essas redes, como computadores, tabletes e *smartphones*.

A criptografia é, "o estudo e prática de princípios e técnicas para comunicação segura na presença de terceiros" (RIVEST, 1984). Assim, ela é a forma de segurança de informação automatizada mais importante e mais utilizada em redes de computadores, o que faz pesquisadores trabalharem arduamente para seu desenvolvimento tecnológico.

Atualmente existem dois tipos importantes (e usuais) de criptografia computacional: a criptografia tradicional, também chamada de criptografia simétrica ou de chave privada, e a criptografia assimétrica, também chamada de criptografia de chave pública.

Para a melhor compreensão de todo o assunto que será tratado nos tópicos subsequentes é necessária a explanação do funcionamento das tecnologias usadas em criptografia.

A criptografia assimétrica, ou de chave pública é,

> [...] uma forma de criptossistemas em que a criptografia e a decriptografia são realizadas usando diferentes chaves – uma chave pública e uma chave privada. Ela transforma o texto claro em um texto cifrado usando uma de duas chaves e um algoritmo de criptografia. Usando a outra chave associada e um algoritmo de decriptografia, o texto claro é recuperado a partir do texto cifrado. (STALLINGS, 2008)

Um dos algoritmos de chave pública mais conhecidos é o RSA, desenvolvido por três pesquisadores do MIT (Instituto de Tecnologia de Massachusetts) e até a data de conclusão deste trabalho ele não foi quebrado por nenhum pesquisador, estudioso ou curioso. As chaves do RSA são geradas com iterações matemáticas de alta complexidade utilizando números primos e funções específicas, como a de *totiene*.

Na figura 11 pode-se observar o funcionamento da criptografia de chave assimétrica com mais detalhes.

Figura 11 – Exemplo de criptografia de chave assimétrica

Fonte: Adaptado de Digicert[4]

Observa-se que os algoritmos de chave pública não precisam de um canal seguro para que a chave seja transmitida, já que eles transmitem somente uma chave (a pública) e a privada não é transmitida em hipótese alguma, assim, trazendo maior segurança à mensagem e aos envolvidos.

Já o outro tipo de criptografia, a simétrica, ou de chave privada é,

> [...] uma forma de sistemas em que a criptografia e a decriptografia são realizadas usando a mesma chave. Ela transforma o texto claro em texto cifrado, usando uma chave secreta e um algoritmo de criptografia, essa mesma chave e um algoritmo de decriptografia são utilizados para recuperar o texto claro a partir do texto cifrado. (STALLINGS, 2008)

Antes da utilização das cifras lógicas as técnicas usadas eram de transposição e de substituição. A técnica de transposição troca automaticamente as posições do texto claro, gerando assim um texto cifrado, já a técnica de substituição mapeia os elementos do texto em claro e gera um texto cifrado.

Com o avanço da tecnologia foram inventadas as máquinas à rotor, dispositivos que, apesar de serem anteriores aos computadores, eram sofisticados e extremamente úteis; a máquina mais conhecida foi a Enigma, que pode ser vista na figura 12, criada por Alan Turing durante a Segunda Guerra Mundial, que utilizava técnicas de substituição automatizadas, facilitando o trabalho do encriptador.

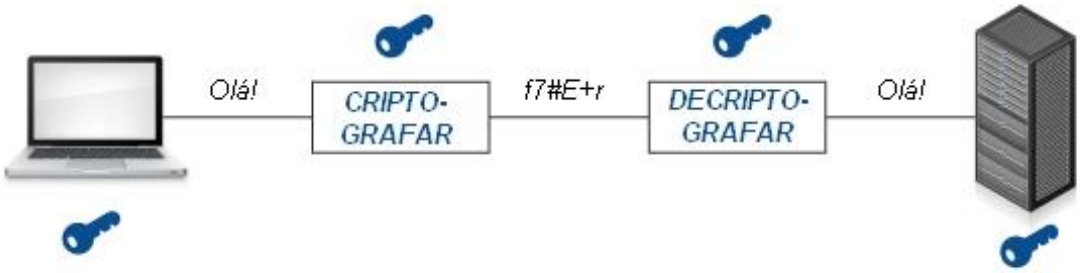
[4]Disponível em <https://www.digicert.com/ssl-cryptography.htm>. Acesso em 13 out. 2018.

Figura 12 – Máquina Enigma

Fonte: Il Galileo[5]

O algoritmo de criptografia simétrica mais utilizado é o AES, que é baseado em redes de permutação-substituição e utiliza chaves privadas. Apesar de ser mais simples que os algoritmos de chave privada, atende perfeitamente todas as necessidades da criptografia de QR Codes.

Figura 13 – Exemplo de criptografia de chave simétrica



Fonte: Adaptado de Digicert

Na figura 13 observa-se o funcionamento de uma chave simétrica em criptografia. Na criptografia de chave privada deve existir um meio seguro para que os

[5]Disponível em <http://www.il-galileo.eu/archivio/1002-turing.html>. Acesso em 13 out. 2018.

envolvidos a troquem e para que a mensagem seja criptografada e decriptografada, diferente do que foi dito sobre a criptografia de chave assimétrica, cujo meio seguro não é necessário.

No próximo tópico será abordada a criptografia em QR Codes, os algoritmos utilizados, suas iterações e utilização no software QRyptal.

4.1 Introdução ao *QRyptal* e funcionamento

A criptografia em QR Codes é, em sua maioria, feita utilizando algoritmos de chave privada, ou de chave simétrica. Esses QR Codes são chamados de SEQRs (*Symmetric Encrypted* QR Codes), e conforme descrito,

> [...] Nos SEQRs usamos um esquema de criptografia simétrica onde tanto o leitor quanto o gerador do QR Code criptografado compartilham uma chave secreta. O esquema de criptografia é extremamente simples: criptografar os bits da mensagem usando cifra de bloco AES com a chave secreta compartilhada (...) A única coisa a notar com esses métodos é que os *bits* de correção de erro devem corrigir erros na mensagem criptografada, não a própria mensagem, a fim de evitar vazamento de informações da mensagem original. (PENG; *et al*, 2014)

O sistema QRyptal foi criado por três engenheiros de software especializados em segurança da informação: Nikhill Jhingan, Vinod Vasnani e Rahul Sinha. A empresa tem sua sede em Cingapura e lançou o QRyptal em 2011, software que usa QR Codes como veículo de armazenamento e compartilhamento de documentos e informação, sempre prezando pela segurança do ativo do contratante.

O QRyptal é um *software*, ou solução, que se conecta aos sistemas de criação de documentos nas empresas contratantes e gera assinaturas digitais de alta segurança como um código de barras ou QR Code nesses documentos. Este software conta com um sistema de criação de QR Code seguro e criptografado, que foi o foco da pesquisa deste trabalho. Para a implementação do QRyptal como gerador e leitor de QR Code criptografado, é necessária a implantação de um *software* chamado QRyptal Generator e também o QRyptal Validator.

Na figura 14 pode-se observar o esquema de funcionamento da API do QRyptal em todas as suas fases, tanto a de geração da assinatura ou do código QR, tanto na fase de validação do documento e acesso ao mesmo.

Figura 14 – Esquema de funcionamento do QRyptal

Fonte: Adaptado de QRyptal[6]

Na fase de geração, como visto na primeira parte da figura 13, utiliza-se o aplicativo QRyptal Generator (ou Gerador do QRyptal), que pode ser utilizado tanto *online* quanto localmente na empresa. Esse aplicativo assina o documento digitalmente com a assinatura da própria contratante, devolvendo documentos seguramente assinados. Já no processo de validação, pode-se utilizar o aplicativo móvel (para leitura de QR Codes) para acessar os documentos e também é possível fazer uso de um leitor local, quando será validado o documento no servidor, assim, conseguindo acessar os documentos sem alterações e com mínimas chances de acesso malicioso.

Para melhor entender a assinatura digital utilizada por esse *software*, pode-se dizer que,

> [...] o código é assinado digitalmente pela chave privada da organização. As chaves são geradas inicialmente como parte da configuração. O aplicativo para dispositivos móveis usa a chave pública da organização para validar a assinatura digital. Além disso, todo o código é compactado especificamente para criar o menor tamanho de QR Code possível. (QRYPTAL, 2011)

[6]Disponível em <https://www.qryptal.com/technology/overview/>. Acesso em 24 out. 2018. Tradução: Autora

Tanto o gerador quanto o validador são servidores sem dependências de bancos de dados, o que possibilita um grande e robusto volume de operações escaláveis. O que também faz o software ser mais versátil, é que pode ser desenvolvido qualquer linguagem de programação ou sistema operacional.

No QRyptal o QR Code gerado pode ser de dois tipos, o EDC (Extended Data Codes, ou Códigos de Dados Estendidos) ou PDC (Primary Data Codes, ou Códigos de Dados Primários) como pode ser observado na figura 15.

Figura 15 – Tipos de QR Codes gerados pelo QRyptal

Fonte: Adaptado de QRyptal

O código de tipo EDC podem conter anexos, imagens, arquivos PDF, entre outros tipos de arquivos. Os anexos no código são criptografados e armazenados como BLOBs (Binary Large OBject, ou seja, Objetos Grandes Binários ou Objetos Grandes Básicos), que são,

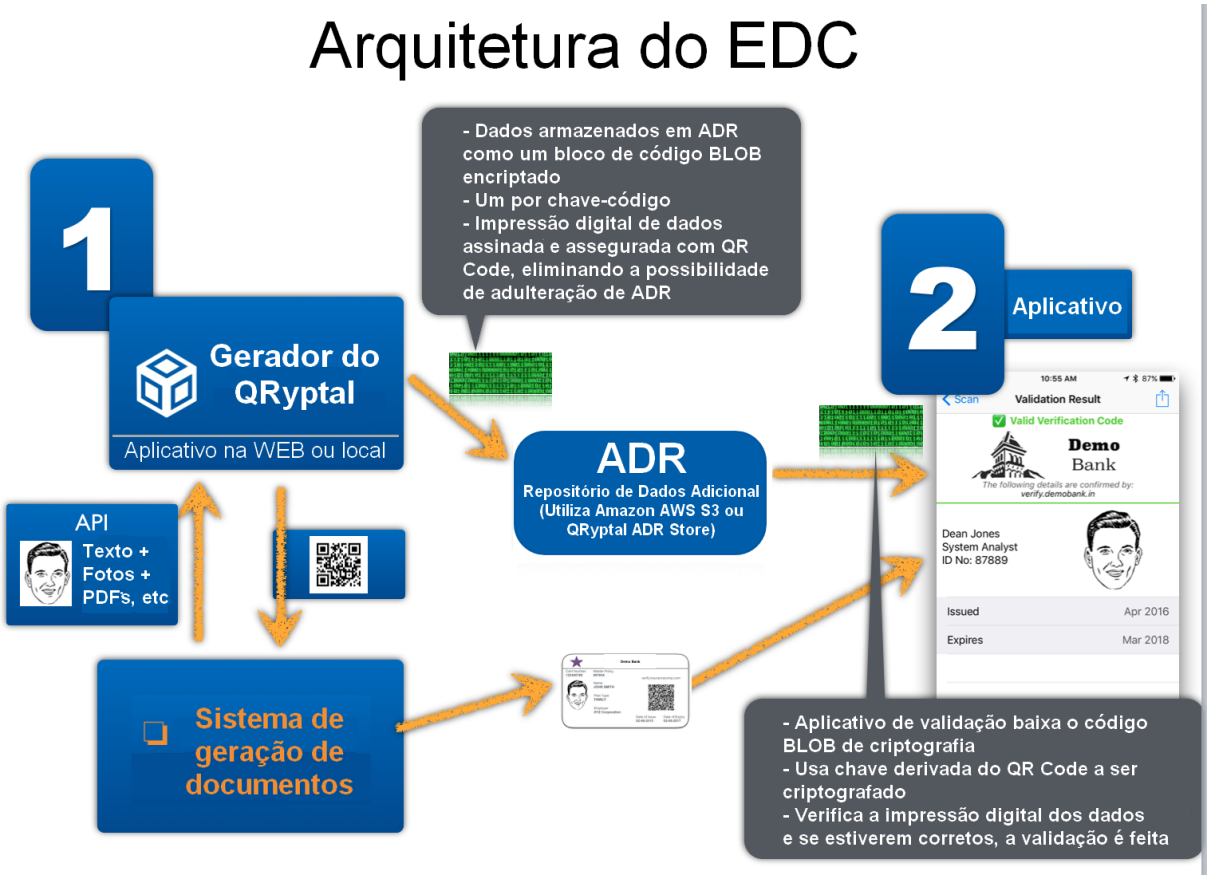
> [...] uma coleção de dados binários armazenados como uma única entidade em um sistema de gerenciamento de banco de dados. BLOBs geralmente são objetos de imagem, áudio ou outro objeto multimídia, apesar de algumas vezes código binário executável ser armazenado como um BLOB. (STARKEY, 2011)

Com o documento armazenado em BLOB não é necessária a utilização de um banco de dados para armazenar os documentos, o que aumenta a segurança da

informação sensivelmente. Então, as chaves de decodificação e as impressões digitais do documento e da empresa são armazenados no QR Code.

Já o QR Code do tipo PDC são códigos autossuficientes que armazenam todas as informações necessárias dentro deles mesmos e têm capacidade de cerca de 2.000 caracteres, podendo armazenar, por exemplo, um extrato bancário ou relatórios confidenciais.

Figura 16 – Arquitetura do QR Code tipo EDC gerado pelo QRyptal



Fonte: Adaptado de QRyptal

Na figura 16 pode-se observar melhor o esquema de arquitetura do código EDC, que armazena documentos, textos e fotos diversas, além de simples caracteres.

Com essas medidas, o QRyptal assegura que os documentos da contratante estejam sempre seguros e acessíveis a quem for necessário e a quem puder ter acesso aos mesmos.

O QRyptal utiliza dois algoritmos de criptografia para manter a segurança dos dados de seus clientes, no próximo item será exposta a teoria, iterações e exemplos

de como esses algoritmos funcionam e como são aplicados no software e em sua respectiva API.

4.1.1 Algoritmos de criptografia utilizados em QR Codes

No objeto estudado, no QRyptal, são utilizados dois algoritmos de criptografia: AES e RSA. A encriptação das assinaturas digitais é feita com o algoritmo RSA, que é um algoritmo de criptografia de chave assimétrica. Segundo Stallings (2008) o algoritmo RSA é,

> [...] um esquema que utiliza uma expressão com exponenciais, onde o texto claro é criptografado em blocos, com cada bloco tendo um valor binário menor que algum número n; ou seja, o tamanho do bloco precisa ser menor ou igual a log2(n).

Sendo um algoritmo criptográfico de alto processamento, é utilizado para encriptação de documentos que necessitam de segurança em grau mais alto.

O algoritmo RSA foi idealizado por três professores pesquisadores do MIT (Massachusetts Institute of Technology, ou Instituto de Tecnologia de Massachusetts) que nos dias atuais trabalham em sua própria empresa, a RSA Data Security Incorporated. O RSA foi o algoritmo de chave assimétrica com maior aceitação e mais ampla utilização, já que ainda não foi descoberto como quebrar a sua segurança.

A geração das chaves do RSA é feita com um conjunto de iterações da seguinte maneira:

Faz-se a escolha aleatória de dois números primos grandes, que serão chamados de *p* e *q*, e são números da ordem de, pelo menos 100^{10}. O número n é dado pelo cálculo de *p.q*. Com a função de *totiene* faz-se o cálculo: **n = Ø(n) = (p1).(q-1)**. Escolhe-se um número inteiro e tal que $1 < e < Ø(n)$, de forma que *e* e $Ø(n)$ sejam primos entre si. Calcule *d* para que seja o inverso multiplicativo de *e* em $(mod\ Ø(n))$.

Assim tem-se um par de chaves públicas **(n, e)** e um trio de chaves privadas **(p, q, d)** – na qual, para fazer a decriptação é necessário somente guardar *d*, já *p* e *q* são usadas somente para acelerar os cálculos.

A encriptação é feita transformando uma mensagem clara *m*, onde $1 < m < n - 1$ numa mensagem *c* cifrada usando essa chave pública gerada pelo destinatário *n* e *e* com 2^2 e uma potenciação modular do tipo: **c = me mod n**. A mensagem é transmitida cifrada ao destinatário. Já na decriptação, essa mensagem *m* para a

mensagem *c*, faz-se a operação modular inversa usando a chave do receptor: **m = cd mod n**.

No QRyptal, no entanto, as chaves não precisam ser calculadas a cada geração de assinatura, já que cada organização contratante tem seu par de chaves personalizado que é utilizado para criptografar e decriptografar os documentos no QR Code. Essa assinatura é baseada em uma chave RSA de 3072 bits de acordo com o NIST (Instituto Nacional de Padrões e Tecnologia.) O que garante a segurança nesse método é justamente o fato da assinatura somente poder ser gerada com a chave personalizada de cada organização, então outra chave, com assinaturas diferentes, não poderá acessar os documentos aleatoriamente.

Já o algoritmo AES, um algoritmo criptográfico de chave simétrica, é utilizado na geração dos QR Codes do tipo EDC no QRyptal. Os anexos nesse código são armazenados criptografados em AES no ADR (*Action Domain Responder*, ou ajuste de usuário natural do código, norma que garante uma arquitetura limpa num código) de objetos. A chave, diferente do explicado anteriormente, é armazenada dentro do próprio QR Code, garantindo acesso seguro às informações que estão armazenadas no mesmo.

O algoritmo AES (Advanced Encription Standard, ou Padrão Avançado de Criptografia), também conhecido como Rjindael, foi escolhido num concurso de algoritmos de criptografia e foi adotado em 2001 como padrão de algoritmo simétrico nos EUA. Trata-se de um algoritmo simétrico, razoavelmente mais simples que os algoritmos assimétricos como o RSA, e também menos seguro, já que necessita de um canal seguro para armazenar e transmitir a chave até o destinatário, correndo riscos de ataques de homem do meio, entre outros.

O AES ou Rijndael é baseado em redes de permutação-substituição, diferente do seu precursor DES. Apesar de ser tratado como o mesmo algoritmo, o AES e o Rijndael têm suas diferenças. Assim, pode-se dizer que,

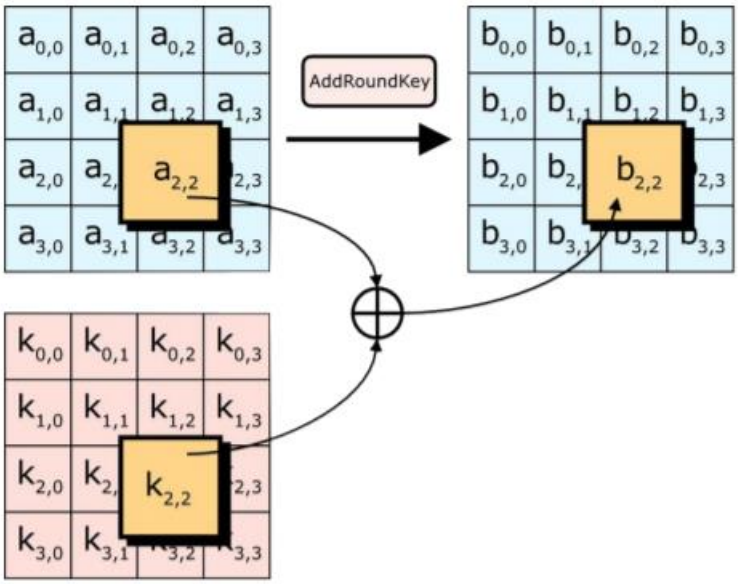
> [...] o AES não é exatamente o Rijndael (embora na prática possam ser permutados) já que o Rijndael suporta uma maior gama de tamanhos do bloco e da chave. O AES tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 *bits*, enquanto o Rijndael pode ser especificado com chaves e tamanhos de bloco de qualquer múltiplo de 32 *bits*, com um mínimo de 128 *bits* e um máximo de 256 *bits*. A chave é expandida usando-se o escalonamento de chaves do Rijndael. A maioria dos cálculos do AES é feita em um corpo finito próprio. (NIST, 2000)

O algoritmo sempre será tratado como AES neste trabalho, já que serão utilizadas as iterações do mesmo para a exemplificação e explicação.

A chave do AES é calculada sobre uma matriz bidimensional de *bytes* com 4x4 posições, chamado de estado, e para criptografar, cada turno (*round*) do AES tem quatro estágios: *AddRoundKey, SubBytes, ShiftRows, MixColumns*.

Como pode ser visto na figura 17, a primeira etapa, chamada *AddRoundKey*, a subchave gerada é combinada com o estado do algoritmo. Para cada *round*, uma subchave é "retirada" da chave principal, usando o escalonamento de chaves proveniente do Rijndael. Cada subchave é do mesmo tamanho que o estado do algoritmo. Essa subchave é somada com cada *byte* do estado e o seu correspondente na mesma subchave. Para isso é usada a operação **XOR** (ou exclusivo).

Figura 17 – Etapa de *AddRoundKey* do AES

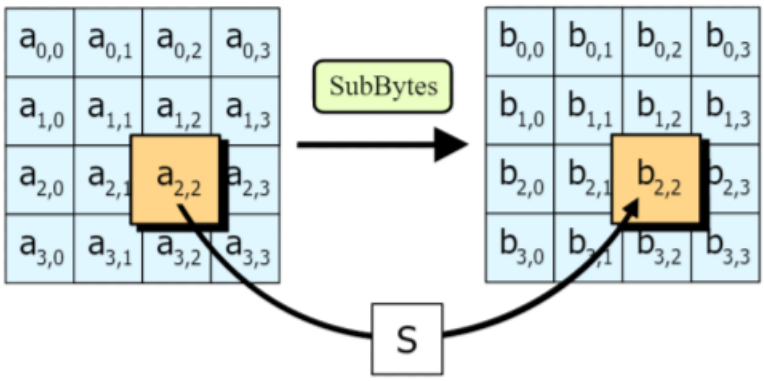


Fonte: NIST[7]

Já na figura 18 observa-se a etapa de *SubBytes*. Nela, cada *byte* na matriz da subchave é atualizado usando uma caixa de oito *bits*. A caixa é construída combinando uma função inversora com uma transformação afim invertível, assim, podem-se evitar ataques de operações algébricas simples ao algoritmo. E também se usa a caixa para evitar pontos fixos durante as iterações do algoritmo.

[7]Disponível em <https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development>. Acesso em 25 out. 2018.

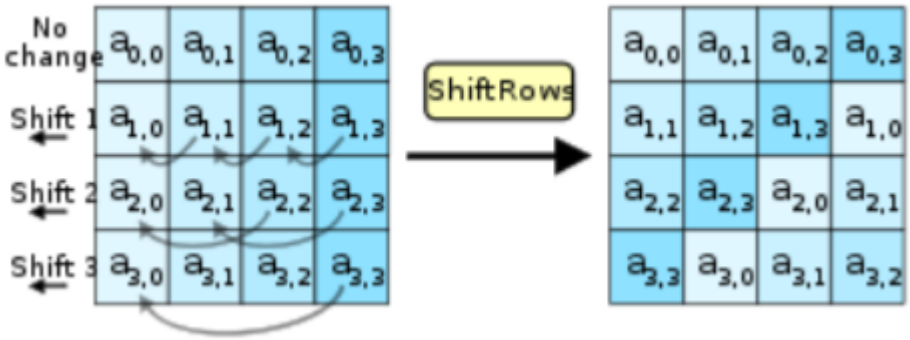
Figura 18 – Etapa de *SubBytes* do AES



Fonte: NIST

Na figura 19 pode ser observada a terceira etapa do AES, de nome *ShiftRows.* Ela opera sobre as linhas do estado, deslocando os *bytes* em cada linha de um número determinado de posições no mesmo, sempre sem alterar a primeira fila. Assim, na segunda linha, cada *byte* é deslocado para a esquerda da sua posição. Da mesma maneira, a terceira linha é deslocada em duas posições, e a terceira em três posições. O padrão de deslocamento é o mesmo para chaves de 128 e 192 *bits*, porém, em chaves de 256 *bits* o deslocamento é feito em 1 *byte* na segunda coluna, 2 *bytes* na terceira coluna e 4 *bytes* na quarta coluna, sempre deixando a primeira linha inalterada. Desta forma, toda coluna do estado fica composta por *bytes* de todas as colunas do estado de entrada, ao final.

Figura 19 – Etapa de *ShiftRows* do AES

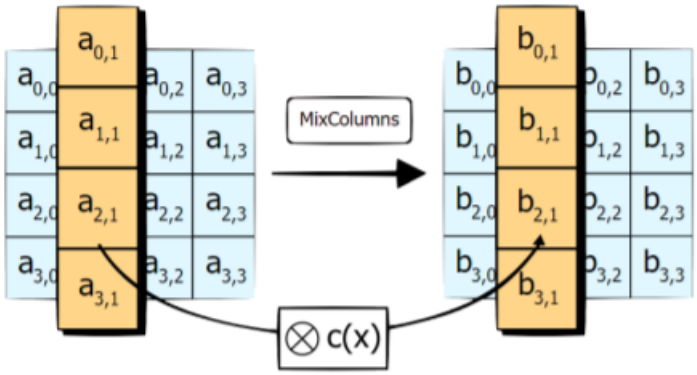


Fonte: NIST

Já na figura 20 pode-se ver o esquema da quarta e última etapa do AES, a *MixColumns*, onde os quatro bytes de cada coluna do estado do algoritmo são combinados usando uma transformação denominada linear invertível, que oferece

difusão à cifra, juntamente com o *ShiftRows*, assim podendo diminuir a chance de choques do texto cifrado com outros textos cifrados. No *MixColumns*, cada coluna é tratada como um polinômio com coeficiente em $\boldsymbol{GF(2^8)}$ e é, então, multiplicado em módulo com $\mathbf{x^4 + 1}$ com um polinômio fixo de valor $\boldsymbol{c(x) = 3x^3 + x^2 + x + 2}$, formando, assim, uma função para o algoritmo. Essa etapa também é chamada de *multiplicação matricial de corpo finito*.

Figura 20 – Etapa de *MixColumns* do AES



Fonte: NIST

Depois dessa última etapa serão feitas mais quatro vezes cada uma das etapas de iterações, gerando uma chave para a encriptação e decriptação do texto, já que o AES, como dito anteriormente, é um algoritmo de chave privada, cuja mesma chave criptografa e decriptografa o texto desejado.

Entendendo melhor como funciona o QR Code criptografado e como ele funciona, no próximo capítulo será apresentado um exemplo de implementação do mesmo, no estudo de caso do pingente de identificação animal RegPet.

5 ESTUDO DE CASO: REGPET – PINGENTE DE IDENTIFICAÇÃO ANIMAL

A sociedade contemporânea está vivendo, conforme os pesquisadores, na chamada "Aldeia Global". E, Aldeia Global para Ianni (1996, p. 16) é uma comunidade mundial onde além de mercadorias, também se comercializa um novo produto: a informação. O planeta tornou-se um lugar onde praticamente tudo está conectado e a maioria dos dados pessoais trafega na rede mundial de computadores, assim, mais do que nunca é necessário zelar pela segurança dos dados disponíveis nos dispositivos usados, sejam eles conectados à *Internet* ou não.

Segundo a norma ABNT ISO/IEC 27002 (ABNT, 2013) segurança da informação é “proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou organização [...] o seu embasamento consiste em manter a integridade, disponibilidade, autenticidade e confidencialidade dos dados.”

Nessa sociedade cada vez mais caótica e instável, as pessoas estão preferindo adotar animais a ter filhos. Segundo pesquisa publicada pelo jornal espanhol *El País*, feita pelo IBGE (Instituto Brasileiro de Geografia e Estatística), em 2015, de cada 100 famílias, 44 criam animais e somente 36 tiveram filhos biológicos ou adotaram crianças. As famílias brasileiras, em 2015, tinham cerca de 52 milhões de cães *versus* 45 milhões de crianças.

Sabe-se que métodos de identificação de animais são usados há muito tempo por seus tutores para manter a segurança dos mesmos; não somente em casos de animais domésticos, mas também no caso de criação de animais para abate e também para controle e identificação de animais selvagens. Como o caso dos *chips* subcutâneos, também chamados de *transponders,* usados em criações de gado e animais de grande porte; as etiquetas de identificação, também conhecidas como brincos de identificação, também usadas em animais de grande porte, mas também em criações de animais que vivem em grandes áreas, como ovinos e caprinos; e as anilhas de identificação, no caso de aves e animais de pequeno porte, como pequenos roedores exóticos.

Nos dias de hoje os animais de estimação são tratados como verdadeiros membros da família: são levados com mais frequência para consultas veterinárias, opta-se pela castração, faz-se uso de serviços de banho e tosa, *spas*, creches, aulas de educação física e até consultas nutricionais. Então, percebe-se a necessidade do

tutor querer identificar e ter controle sobre os dados do animal (data de nascimento, endereço, telefone dos tutores, além de dados sobre vacinas e doenças que ele já possuiu ou possui) e por onde ele anda, observando a demanda cada vez maior de cuidado e segurança dos dados, mantendo-os confiáveis e disponíveis para serem acessados pelas pessoas certas.

Então, pensando nesse grande trânsito ao qual os animais estão sendo expostos a criação e implementação de um sistema diferenciado de identificação, manutenção de dados e informações, além de possível rastreamento, que seja de fácil manuseio ao tutor do animal é de suma importância para a boa manutenção dos animais como os novos membros da família.

Em pesquisa feita por esta autora (Apêndice A), considerou-se nas respostas (Apêndice B) que 82,5% dos tutores de animais acham importante e necessário o uso de algum tipo de identificação em seu *pet*, porém 54% deles tem medo de fazer a implantação de *microchips* em animais pelo fato do *transponder* ser subcutâneo; outros 30% tem problemas com o preço da aplicação do *microchip*, que flutua entre R$ 160,00 e R$ 250,00 (conforme tabela 3), pois por ser um procedimento médico, deve ser aplicado por um veterinário.

Tabela 3 – Comparações de preços de marcas e aplicações de *microchips* para animais

MARCA	TAMANHO	PREÇO
Faripet	14mm x 8mm	R$ 22,00
Microchips Brasil	12mm x 2mm	R$ 9,50
Abrachip	12mm x 2mm	R$ 14,00
APLICAÇÃO	**PREÇO**	
Animaltag	R$ 250,00	
Prevet	R$ 160,00	

Fonte: Próprio autor

Também existem outros métodos de identificação, como já citado ~~pelo autor~~ anteriormente, porém observa-se que eles têm funcionalidade limitada comparada ao proposto neste trabalho, como apresentado na tabela 4. Assim, apesar de serem

dispositivos já tradicionais no mercado, existe a possibilidade de modernizar a identificação dos animais de estimação com a implantação do RegPet.

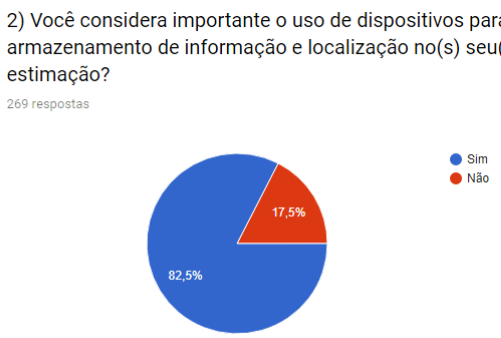
Tabela 4 – Comparações de preços de dispositivos de identificação para animais

DISPOSITIVO	OBJETIVO	PREÇO/PRODUTO	PREÇO/IMPLANTAÇÃO
Microchip Subcutâneo	Identificação com leitura eletrônica	R$ 9,50 – R$ 22,00	R$ 160,00 – R$ 250,00
Etiqueta (brinco) de Identificação	Identificação com leitura eletrônica	R$ 1,10	R$ 40,00 – R$ 60,00
Anilha de Identificação	Identificação sem leitura eletrônica	R$ 0,20 - 3,00	-

Fonte: Próprio autor

Baseando-se na pesquisa elaborada neste trabalho, a criação e implantação do RegPet pode representar o futuro para quem necessita de maior segurança no controle de seus animais, e, posteriormente, para cadastramento e manutenção de animais em canis e gatis ou centros de zoonoses e Organizações Não-Governamentais (ONGs) de proteção animal, já que, conforme gráfico 2, 82,5% dos pesquisados acham de extrema importância o uso de dispositivos de identificação em seus animais; além de 71,4% dos tutores afirmarem que usariam este dispositivo e 86,6% demonstrarem total segurança em usá-lo.

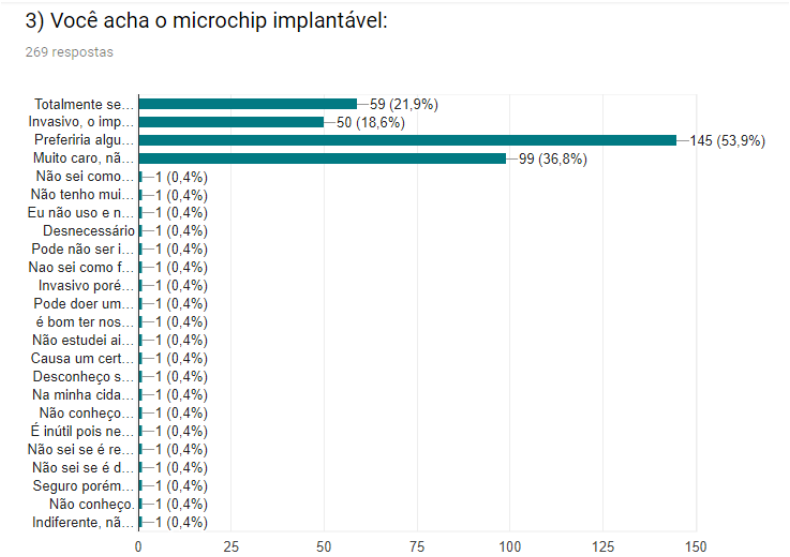
Gráfico 2 – Pesquisa



Fonte: Próprio autor

Outro ponto importante da implementação do dispositivo proposto é a questão do valor. Como observado na tabela 4, os preços dos *transponders* não são altos, porém a implantação, por ser um procedimento médico, não é acessível para a maioria da população. Conforme gráfico 3, a segunda maior motivação para o tutor não fazer o uso do *microchip* implantável é justamente o preço, seguida somente de a preocupação do método de implantação ser muito invasivo e talvez doloroso ao animal.

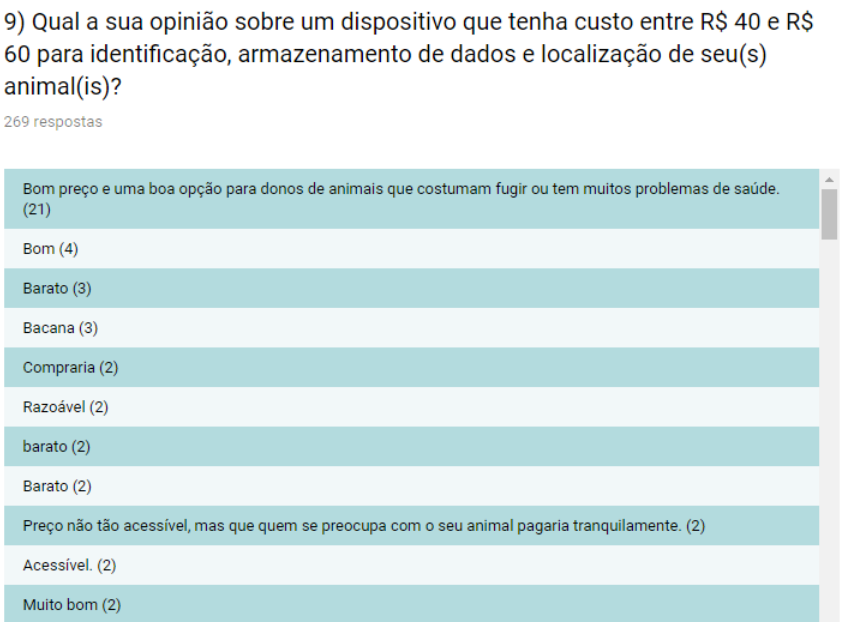
Gráfico 3 – Pesquisa



Fonte: Próprio autor

Assim, com base em estudos primários e orçamentos feitos pela autora deste trabalho, o dispositivo custaria entre R$ 40,00 e R$ 60,00 – podendo ter menor preço com maior tiragem do produto, o que foi bem aceito pelos pesquisados, conforme figura 21.

Figura 21 – Pesquisa



Fonte: Próprio autor

Pode-se pensar também na leitura do dispositivo, enquanto os tradicionais necessitam de equipamentos especiais para fazer a mesma, e o dispositivo proposto terá a leitura feita por meio de um aplicativo gratuito distribuído via lojas de aplicativos como *Google Play* e *App Store*, além de poder ter seu banco de dados acessado via *web* (por *site*), somente com *login* e senha do próprio tutor ou *login* especial de médico veterinário. Isso tornaria o dispositivo acessível, já que, conforme dados da PNAD divulgados pelo IBGE em 2017, 92% dos lares brasileiros tem *smartphones*. E nesta mesma pesquisa, foi concluído que mais de 60% da população tem acesso à *Internet* em casa, e mais de 80% da população faz uso da mesma em algum local que frequenta, como escolas, *shoppings* ou local de trabalho.

5.1 Introdução ao RegPet e funcionamento

O RegPet é um dispositivo de identificação e localização animal baseado em QR Code. Ele é um pingente colocado na coleira, roupa, bolsa de transporte ou carteira de vacinação/documentação do animal que contém dados do seu tutor, do próprio *pet*, entre outras informações com controle de acesso restrito aos tutores do animal, ONGs ou veterinários. Na figura 22 pode-se ver o dispositivo, tanto na versão para felinos, quanto para caninos.

Figura 22 – Dispositivo pingente RegPet

Fonte: Próprio autor

O dispositivo conta com um site interativo e um vasto banco de dados protegido por HTTPS[8], que mantém os dados do tutor e animal seguros.

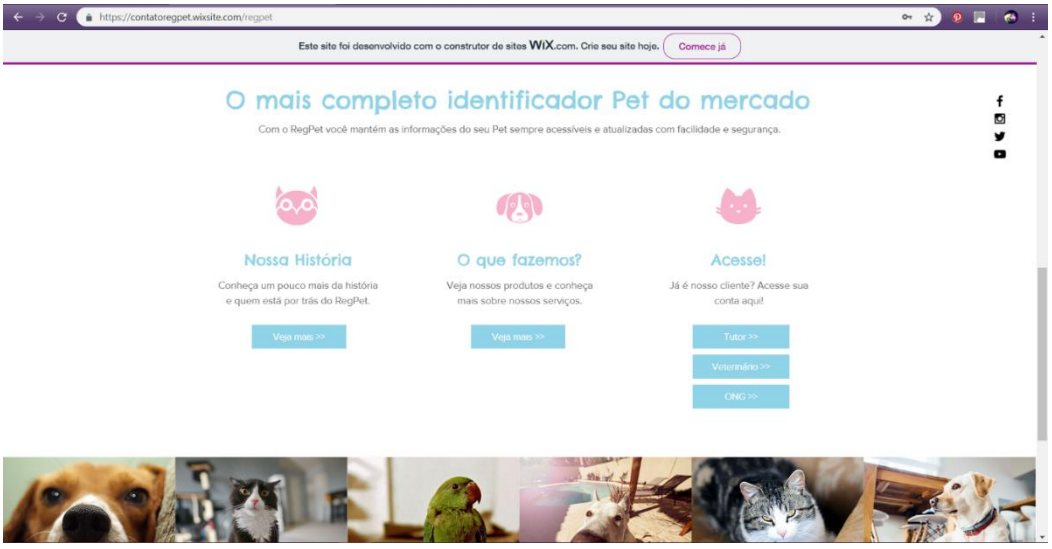
[8] Também chamado de Protocolo de Transferência de Hipertexto Seguro (HTTPS) é uma extensão do Protocolo de Transferência de Hipertexto (HTTP, Hypertext Transfer Protocol) para comunicação segura em uma rede de computadores e é amplamente usado na Internet. No HTTPS, o protocolo de comunicação é criptografado usando TLS (Transport Layer Security) ou, antes das atualizações, o Secure Sockets Layer (SSL). O protocolo é, portanto, também conhecido como HTTP por TLS ou HTTP por SSL. (COMODO C.A. LTD., 2017)

Nas figuras 23 e 24 pode-se observar um pouco melhor a página principal do site do RegPet, ao qual o tutor terá acesso ao cadastro e também ao registro dos dados do seu animal de estimação.

Figura 23 – Site RegPet

Fonte: Próprio autor[9]

Figura 24 – Site RegPet



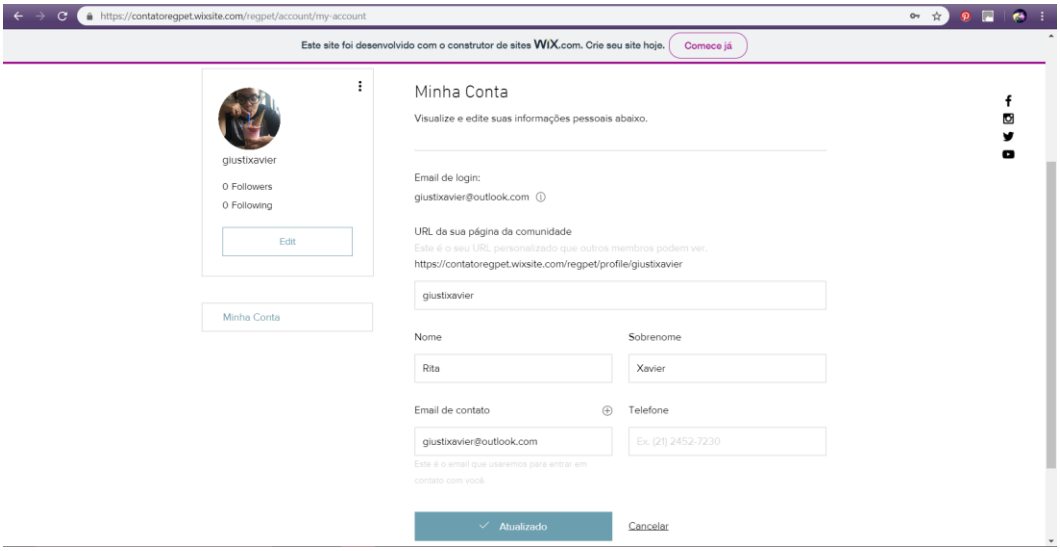
Fonte: Próprio autor

Para hospedar o *site* foi usado o Wix, que é um servidor de *sites* que oferece amplas funcionalidades e várias ferramentas que facilitam a utilização pelo cliente

[9]Disponível em <contatoregpet.wixsite.com/regpet>. Acesso em 29 de out. 2018.

(tutor do animal, veterinário, participante de ONGs) e também a gerência de dados pelo administrador do *site*. Além de oferecer HTTPS e ambiente seguro de banco de dados.

Figura 25 – Perfil do tutor no RegPet



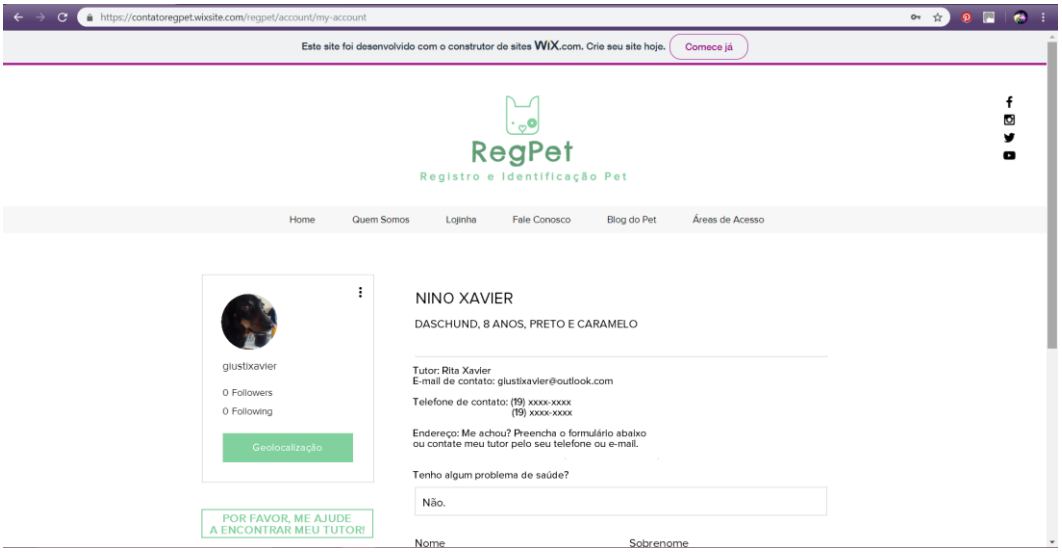
Fonte: Próprio autor

Apenas o tutor poderá ter acesso ao perfil, onde ele poderá atualizar seus dados e os dados do animal de estimação. Cada tutor pode ter vários animais de estimação, *linkados* por vários dispositivos em somente uma conta, podendo centralizar a gerência dos pingentes e dos dados de seus *pets*. Essa conta é protegida por uma senha que deve ser forte (caracteres maiúsculos e minúsculos, caracteres especiais e mínimo de 8 caracteres obrigatórios) e deve ser modificada a cada três meses, quando o RegPet se responsabiliza por mandar um *e-mail* para o tutor com uma mensagem e *link* para modificação da mesma. O perfil é único e só pode ser acessado pela pessoa com seu *e-mail* e senha. Pode-se observar o perfil na figura 25.

O perfil de participante de ONG segue o mesmo *layout* e tem as mesmas funcionalidades, porém ele poderá centralizar seus animais num banco de dados e perfil da própria ONG. Já o perfil do veterinário, apesar de seguir o mesmo *layout*, não terá a funcionalidade de administrar os dados dos animais, somente caso o tutor autorize o veterinário a fazer alterações no perfil do animal, porém ele terá acesso

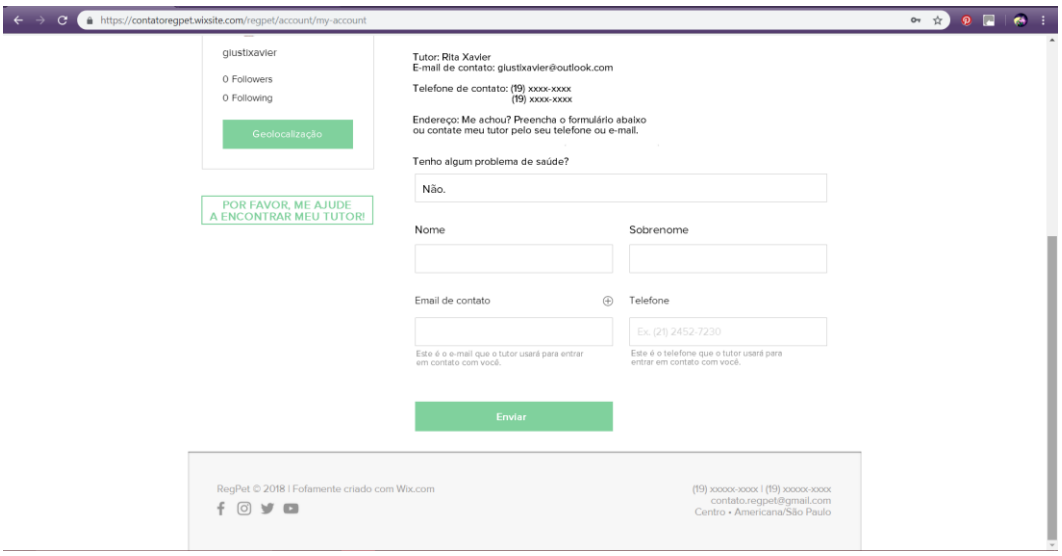
somente ao campo “Tenho algum problema de saúde?” e ao campo para preencher os problemas de saúde do animal.

Figura 26 – Perfil do *pet* no RegPet



Fonte: Próprio autor

Figura 27 – Perfil do *pet* no RegPet



Fonte: Próprio autor

Nas figuras 26 e 27 pode-se observar o perfil do *pet* no RegPet. Nele a pessoa que fez a leitura do QR Code, acessará os principais dados sobre o animal, como seu nome, raça, cor da pelagem, se tem algum tipo de problema de saúde ou condição especial e se é idoso. Também haverá o acesso ao telefone e *e-mail* do tutor do

animal, e também um formulário para ser preenchido para entrar em contato com o tutor do *pet*, caso a pessoa que fez a leitura do QR Code não queira entrar em contato direto com o tutor. Nas figuras 26 e 27 observa-se o perfil na tela do computador ou *notebook,* acessado pelo *site*. O tutor também poderá ver o perfil como ele ficará para quem fizer a leitura do QR Code, e também controlará o que poderá ser visto: telefone, *e-mail*, endereço, somente formulário, entre outros. O que é obrigatório ser mostrado no perfil é o nome do animal, sua raça, cor de pelagem e se ele tem algum tipo de doença ou necessidade especial.

Figura 28 – Aplicativo RegPet

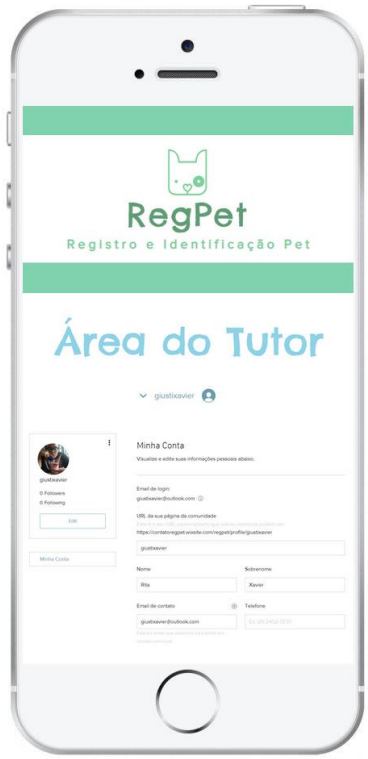
Fonte: Próprio autor

A figura 28 apresenta o aplicativo RegPet, seu ícone na página inicial do *smartphone* e a página inicial do aplicativo. Na página inicial do aplicativo o usuário pode escolher se quer entrar com seu usuário e senha e acessar algumas funcionalidades do RegPet, ou se quer ler o QR Code de um pingente.

O mesmo que se vê e se acessa no *site*, pode-se ver e acessar pelo aplicativo, com algumas funcionalidades diminuídas. Na figura 29 observa-se o perfil do tutor, e

o acesso de seus dados e do seu *pet*, assim como no *site*, porém no aplicativo ele não poderá adquirir novos dispositivos, nem contratar novos serviços, como poderia fazer no *site*.

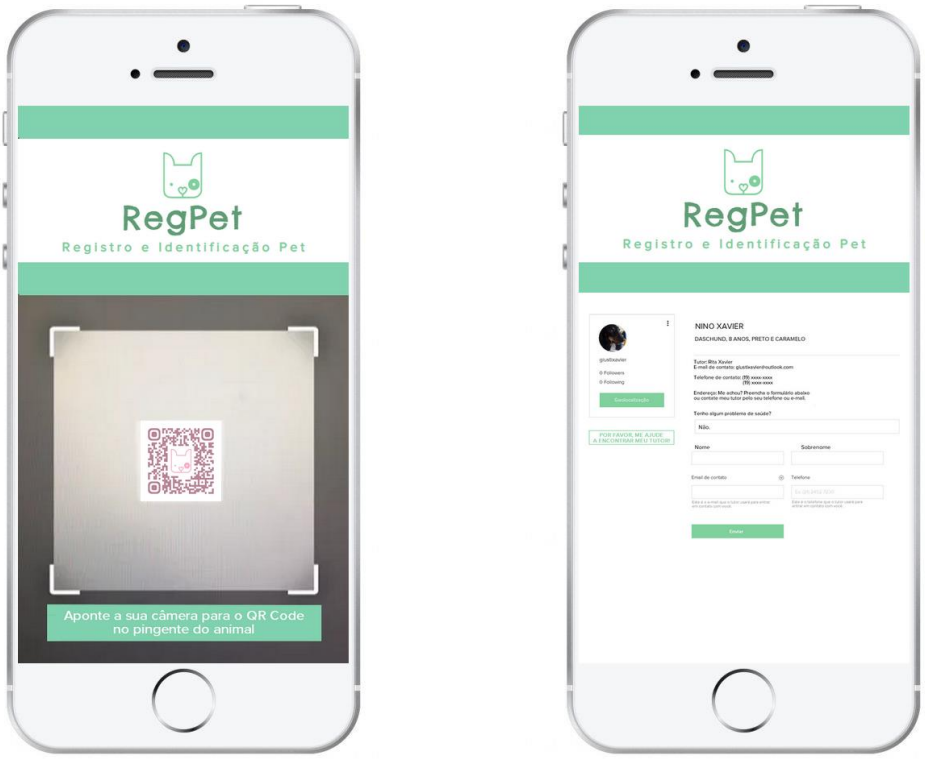
Figura 29 – Aplicativo RegPet



Fonte: Próprio autor

Caso a pessoa tenha achado o animal perdido e opte somente por ler o QR Code, poderá escolher a opção “Ler QR Code” na página inicial do aplicativo, e como observa-se na figura 30, ele abrirá um leitor de QR Code utilizando a câmera do *smartphone* e poderá escanear o pingente do animal que foi encontrado. Também na figura 30 pode-se ver como o perfil do *pet* aparecerá depois de ser escaneado no leitor de QR Code do aplicativo. Nesse caso observa-se um perfil de um animal saudável, sem nenhum tipo de necessidade especial ou doença, assim quem achou o animal deve entrar em contato com o tutor, porém não é necessária a urgência, podendo utilizar o formulário do aplicativo para fazer esse contato.

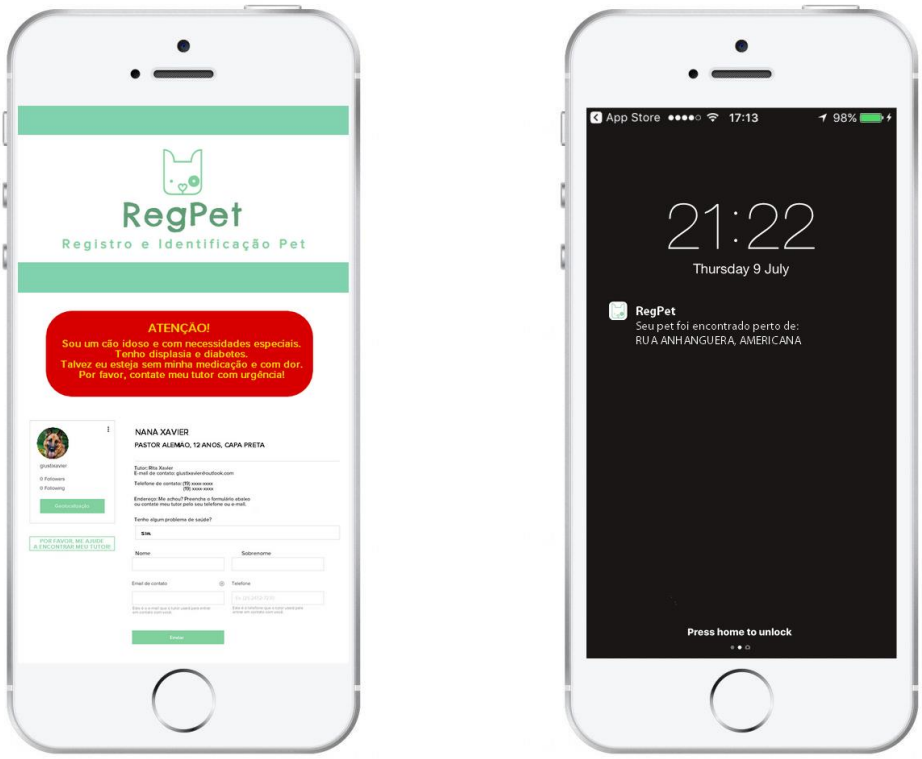
Figura 30 – Aplicativo RegPet



Fonte: Próprio autor

Porém, caso o animal tenha algum tipo de problema de saúde, ou seja um animal idoso, após o escaneamento do QR Code, haverá um aviso de alerta acima do perfil do *pet*, como pode-se observar na figura 31. Assim, sabendo da necessidade de cuidados do animal, quem o encontrou deverá entrar em contato urgentemente com o tutor.

Figura 31 – Aplicativo RegPet



Fonte: Próprio autor

Como a pessoa que encontrar o animal talvez tenha intenções maliciosas, o QR Code também manda uma mensagem de geolocalização para o tutor do animal, caso ele seja escaneado, como também pode ser visto na figura 31.

No item abaixo serão explicadas com mais detalhes as funcionalidades do QR Code no dispositivo RegPet.

5.2 Funcionalidade do QR Code no RegPet

No RegPet o QR Code tem suma importância, já que o dispositivo e *site* são baseados em QR Code seguro e criptografia.

Para se diferenciar dos outros dispositivos de identificação animal baseados em QR Code, o RegPet utiliza o QRyptal como leitor dentro de seu aplicativo. Os QR Codes seguros são gerados no *site* da QRyptal e impressos em papel de alta qualidade com impermeabilização, para que o erro de leitura seja mínimo. Apesar de serem gerados pela QRyptal, utiliza-se a tecnologia de SQRC e Frame QR Code, da Denso Wave.

Os QR Codes disponíveis para o dispositivo são oferecidos em três modelos, como pode-se observar na figura 32, seguindo o *design* da RegPet e cores claras e agradáveis aos animais, porém que não dificultam o escaneamento pelo leitor de QR Code, nem aumentam a taxa de erro.

Figura 32 – QR Codes RegPet

Fonte: Próprio autor

Além de oferecerem um design agradável, os QR Codes contam com tecnologia de geolocalização, isto é,

> [...] a identificação ou estimativa da localização geográfica de um objeto em tempo real, podendo ter como fonte um radar, telefone celular ou computador conectado à Internet. Em sua forma mais simples, a geolocalização envolve a geração de um conjunto de coordenadas geográficas e está relacionada ao uso de sistemas de posicionamento, como GPS, mas sua utilidade é aprimorada pelo uso dessas coordenadas para determinar um local mais específico, como um endereço [...] também se refere às coordenadas de latitude e longitude de um determinado local. O termo e a definição foram padronizados pelo padrão de sistema de localização em tempo real com a ISO/IEC 19762-5:2008. No campo da biologia animal e ecologia, a palavra geolocalização também é usada para se referir ao processo de localização de um animal rastreado baseado em algum instrumento ou dispositivo ligado ao animal. Tais instrumentos são comumente chamados de *tags* ou *transponders* (incluindo implantes de *microchip*) ou *dataloggers*, como QR Codes. (IONESCU, 2010)

Assim, quando um animal perdido é encontrado e a pessoa que o localizou faz o escaneamento do QR Code no pingente, é feito o envio de uma mensagem pelo aplicativo do RegPet para o tutor com a localidade próxima de onde essa leitura foi realizada, como pode ser visto na figura 31 do item anterior. Além de manter o tutor informado, mantém o banco de dados do sistema alimentado com as coordenadas da geolocalização do animal toda vez que o QR Code é escaneado.

O QR Code mantém os dados seguros, pois conta com criptografia, e como ele é *linkado* diretamente ao banco de dados com os perfis dos animais, os dados que o tutor não autorizar que sejam vistos, não poderão ser acessados por esse método. Outra ferramenta de segurança utilizada é o HTTPS no site e banco de dados, o que aumenta a confiabilidade do dispositivo.

O RegPet é um dispositivo diferenciado, porém essa diferenciação não faz dele um dispositivo difícil de ser utilizado pelos tutores, nem pelas pessoas que encontrarem o animal perdido. No pingente, como pode ser visto na figura 33, existem as instruções de como deve ser procedida a utilização do mesmo, caso o animal seja encontrado.

Figura 33 – Embalagem frente e verso e pingente RegPet

Fonte: Próprio autor

Já na embalagem do dispositivo e também no site, existem todos os passos de como o tutor proceder para fazer o cadastro do seu perfil e do seu *pet*, como pode ser visto na figura 34.

Figura 34 – Interior e instruções da embalagem do RegPet

Fonte: Próprio autor

Assim, o RegPet é um identificador e localizador *pet* baseado em QR Code seguro com todas as funcionalidades necessárias para o bem-estar do animal e tranquilidade do tutor.

6 CONSIDERAÇÕES FINAIS

O uso de dispositivos de localização e identificação de animais se popularizou, já que com o decorrer do tempo muitas pessoas começaram a optar pelos animais de estimação em alternativa aos filhos, assim necessitando de dispositivos que ajudem em sua segurança e bem-estar, pois esses estão mais vulneráveis à furtos, acidentes, fugas e desaparecimentos.

Com a análise primária dos dados das pesquisas feitas pelo autor antes do início do desenvolvimento deste trabalho, pode-se entender melhor as necessidades dos tutores de animais de estimação e quais as funcionalidades eles esperam de um dispositivo como o RegPet.

O desenvolvimento deste estudo possibilitou uma ampla análise de como QR Codes podem otimizar a utilização de dispositivos de identificação e localização de animais, sem diminuir a segurança dos dados armazenados nele ou que são acessados por meio do código.

O **objetivo geral** de estudar a funcionalidade do QR Code criptografado dentro do dispositivo RegPet foi concluído, mostrando que o QR Code pode ser utilizado para o fim proposto sem nenhuma perda de qualidade para o tutor e sem perda de segurança nos dados, pelo contrário, fazendo o tutor ganhar tempo e segurança utilizando criptografia no QR Code e nos dados, e também o HTTPS no *site* e banco de dados.

Os **objetivos específicos** foram analisados da seguinte forma:

a) **O estudo da história, tipificação e funcionalidade dos QR Codes, com objetivo de compreender por que eles podem ser utilizados no dispositivo sem perda de qualidade e com ganho em segurança:** foi alcançado, utilizando a pesquisa bibliográfica, e demonstrando que o QR Code é uma tecnologia que pode ser utilizada sem danos à segurança do tutor e do animal;

b) **Compreender o funcionamento dos QR Codes seguros e como a segurança é implementada nesses códigos, além de compreender os tipos de criptografia utilizados nos QR Codes seguros e como elas funcionam:** foi alcançada, demonstrando que os códigos são utilizados com segurança, já que os algoritmos de criptografia utilizados neles, e também outros métodos de garantir a segurança, são confiáveis;

c) **Demonstrar o dispositivo RegPet como um todo, englobando os QR Codes e protocolos de segurança utilizados nele:** como o objetivo geral, este também foi alcançado, demonstrando que o QR Code pode facilitar a utilização do pingente de identificação, mantendo a segurança dos dados do tutor e animal.

Apesar dos resultados serem animadores, ainda é necessária a melhoria da tecnologia de QR Code criptografado, já que este só pode ser gerado e escaneado por um *software* específico, o que pode tornar o processo de leitura do código dificultado, apesar de estar explicado no pingente de identificação.

Para estudos futuros, o autor sugere que os futuros estudantes pensem em tecnologias que incluam QR Codes criptografados e seguros em leitores e geradores de códigos convencionais, sem a necessidade de despendimento financeiro ou de *download* de *softwares* ou aplicativos específicos. Assim, a leitura do QR Code seria ainda mais facilitada seu uso se tornaria ainda mais popular.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - Associação Brasileira de Normas Técnicas. **ISO/IEC 27002:2013**. São Paulo: ABNT. 2013.

ANDA - Agência de Notícias de Direitos de Animais. **Brasil tem 30 milhões de animais abandonados**. São Paulo, 2013. Disponível em <https://anda.jusbrasil.com.br/noticias/100681698/brasil-tem-30-milhoes-de-animais-abandonados>. Acesso em: 4 out. 2018.

ARIAS, Juan. Lares brasileiros já têm mais animais do que crianças, *In* Coluna Opinião, . Madri, Espanha. Disponível em: <https://brasil.elpais.com/brasil/2015/06/09/opinion/1433885904_043289.html>. Acessado em: 24 de agosto de 2017.

CIPRA, Barry A. **The ubiquitous Reed–Solomon codes**. 1993.

COMODO C.A. LTD. **What is HTTPS?** EUA, 2017. Disponível em < https://www.instantssl.com/ssl-certificate-products/https.html>. Acesso em: 29 de out. De 2018.

DENSO WAVE Corporated. **QR Code® Essentials**. Japão, 2011. Disponível em <http://www.nacs.org/LinkClick.aspx?fileticket=D1FpVAvvJuo%3D&tabid=1426&mid%20=4802>. Acesso em: 16 ago. 2018.

DENSO WAVE Corporated. **QRCode.com**. Japão, 2018. Disponível em <www.qrcode.com>. Acesso em: 19 de ago. 2018.

DIGICERT Incorporated. **Digicert.com**. EUA, 2018. Disponível em <https://www.digicert.com/ssl-cryptography.htm>. Acesso em 13 out. 2018.

GS1 BRASIL. **GS1BR.com.br**. São Paulo, 2018. Disponível em <www.gs1br.com.br>. Acesso em: 18 ago. 2018.

IBGE - Instituto Brasileiro de Geografia e Estatística. Brasília. **PNAD 2017.** IBGE, 2017.

IONESCU, Daniel. **Geolocation 101: How It Works, the Apps, and Your Privacy.** EUA, 2010. Disponível em <https://www.pcworld.com/article/192803/geolo.html>. Acesso em: 29 de out. de 2018.

KASPERSKY LAB. AO. **Securelist.com**. EUA, 2018. Disponível em <https://securelist.com/en/blog/208193145/Its_time_for_malicious_QR_codes>. Acesso em: 10 out. 2018.

LAMBERT, Sam. **QR codes demonstrate considerable success in Pitney Bowes research**. EUA, 2013. Disponível em < https://www.qrcodepress.com/qr-codes-demonstrate-considerable-success-in-pitney-bowes-research/8516378/>. Acesso em: 20 set. 2018.

MATSUURA, Sérgio. **Estudo revela que 23 milhões de animais foram mortos na Amazônia**. Rio de Janeiro, 2016. Disponível em <https://oglobo.globo.com/sociedade/sustentabilidade/estudo-revela-que-23-milhoes-de-animais-foram-mortos-na-amazonia-20280141>. Acesso em: 4 out. 2018.

NIST – National Institute of Standards and Technology. **Cryptographic standards and guidelines**. EUA, 2016. Disponível em <https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development>. Acesso em 25 out. 2018.

PENG, Kevin; SANABRIA, Harry; WU Derek; ZHU, Charlotte. **Security overview of QR codes**. 2014.

POPPER, Karl R. **A lógica da pesquisa científica**. São Paulo:Cultrix, 2004.

REED, Irving S.;SOLOMON, Gustave. Polynomial codes over certain finite fields. **Journal of the Society for Industrial and Applied Mathematics** (SIAM, 1960). pp. 300–304.

PRUNAI, Giuseppe. **Turing, il padre del computer**. Itália, 2016. Disponível em <http://www.il-galileo.eu/archivio/1002-turing.html>. Acesso em 13 out. 2018.

QRYPTAL Pte. Ltd. **Technology Overview**. Cingapura, 2018. Disponível em <https://www.qryptal.com/technology/overview/>. Acesso em 24 out. 2018.

RIVEST, Ronald L. Cryptography. In: **Handbook of theoretical computer science**. Amsterdam: J. Van Leeuwen. 1990.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. São Paulo:Cortez, 2007.

SHARMA, Vishrut. **A study of malicious QR Codes**. 2012.

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. São Paulo:Pearson, 2014. Ed. 6.

APÊNDICES

APÊNDICE A – QUESTIONÁRIO APLICADO

RFPid - DISPOSITIVO DE IDENTIFICAÇÃO, INFORMAÇÃO E CONTROLE DE ANIMAIS DOMÉSTICOS E SILVESTRES

Atualmente os animais de estimação são verdadeiros membros da família, com direito ao respeito que um ser com essa nomenclatura necessita. São levados com mais frequência para consultas veterinárias, opta-se pela castração, faz-se uso de serviços de banho e tosa, spas, creches, aulas de educação física e até consultas nutricionais. Assim, ao grande trânsito que os animais estão sendo expostos hoje em dia, a criação e implementação de um sistema diferenciado de identificação, manutenção de dados e informações, além de possível rastreamento, que seja de fácil manuseio ao tutor do animal é de suma importância para a boa manutenção dos animais como os novos membros da família. Este questionário visa entender melhor as necessidades dos tutores em questões de dispositivos de identificação, informação e rastreamento de animais domésticos e silvestres.

1) Você tem quais animais de estimação? *

- [ ] Cachorro(s)
- [ ] Gato(s)
- [ ] Roedor(es)
- [ ] Ave(s)
- [ ] Réptil(eis), quelônio(s), peixe(s), inseto(s), etc
- [ ] Silvestre(s), exótico(s), etc
- [ ] Outro: _____

2) Você considera importante o uso de dispositivos para identificação, armazenamento de informação e localização no(s) seu(s) animal(is) de estimação? *

- ( ) Sim
- ( ) Não

3) Você acha o microchip implantável: *

- [ ] Totalmente seguro e indolor
- [ ] Invasivo, o implante pode ser doloroso ao(s) animal(is)
- [ ] Preferiria algum dispositivo não tão invasivo
- [ ] Muito caro, não tenho condições
- [ ] Outro: _____

4) Você usaria um microchip implantável em seu(s) animal(is)? *

- ( ) Sim
- ( ) Não

5) Com base na questão anterior (4), justifique os motivos de sua resposta. *

Sua resposta

6) Você usaria um dispositivo não implantável em seu(s) animal(is) como método de identificação, rastreio ou armazenamento de dados importantes (doenças prévias, congênitas, situações, entre outros)? *

- ◯ Sim
- ◯ Não
- ◯ Talvez

7) Com base na questão anterior (6), justifique os motivos de sua resposta. *

Sua resposta

8) Você se sentiria seguro com seu(s) animal(is) usando um dispositivo não implantável de identificação, armazenamento de dados e localização? *

- ◯ Sim
- ◯ Não

9) Qual a sua opinião sobre um dispositivo que tenha custo entre R$ 40 e R$ 60 para identificação, armazenamento de dados e localização de seu(s) animal(is)? *

Sua resposta

10) Cadastre seu e-mail caso tenha interesse em saber mais sobre o projeto.

Sua resposta

ENVIAR

Página 1 de 1

Nunca envie senhas pelo Formulários Google.

APÊNDICE B – RESUMO DAS RESPOSTAS DO QUESTIONÁRIO APLICADO (APÊNDICE A)

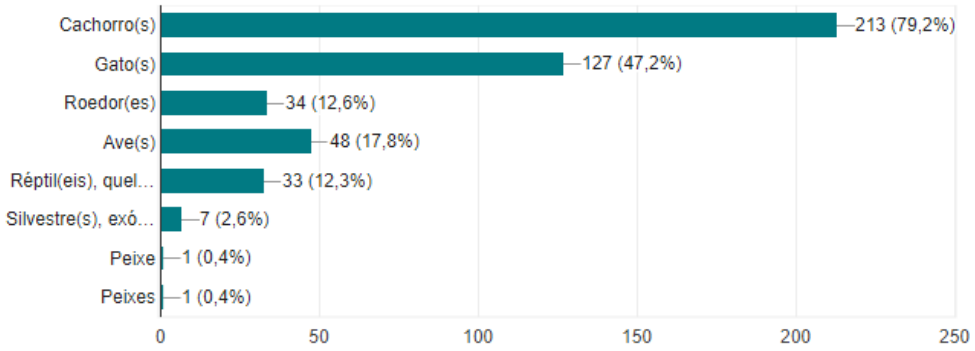
269 respostas

RESUMO | INDIVIDUAL

Aceitando respostas

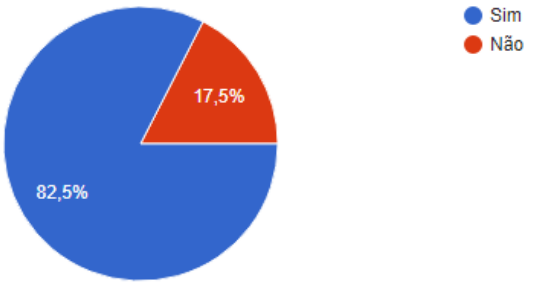
1) Você tem quais animais de estimação?

269 respostas



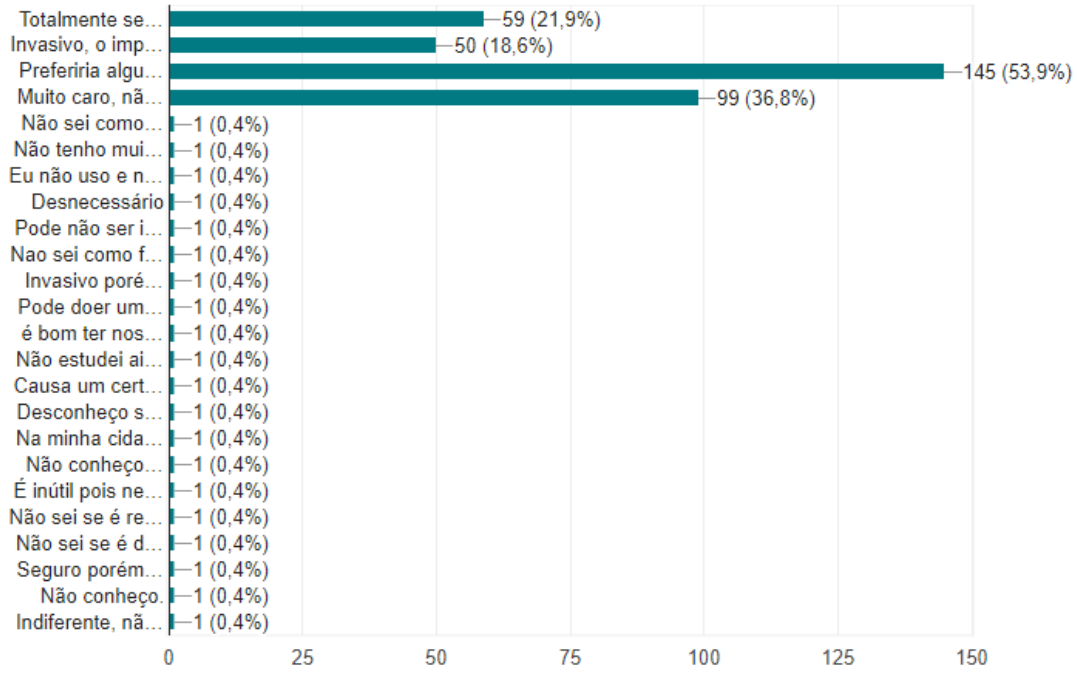
2) Você considera importante o uso de dispositivos para identificação, armazenamento de informação e localização no(s) seu(s) animal(is) de estimação?

269 respostas



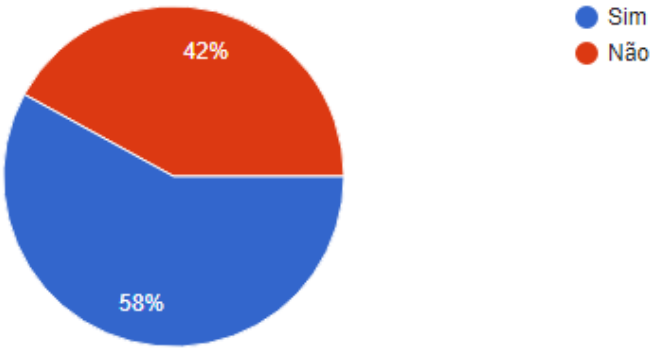
3) Você acha o microchip implantável:

269 respostas



4) Você usaria um microchip implantável em seu(s) animal(is)?

269 respostas



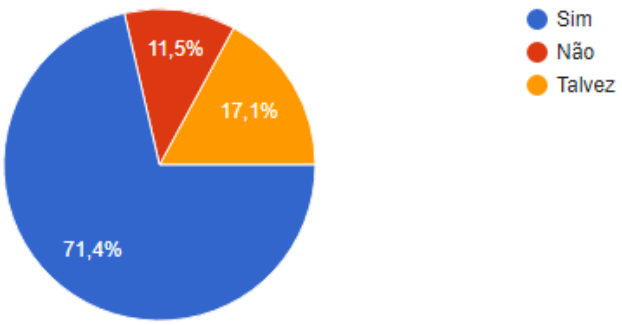
5) Com base na questão anterior (4), justifique os motivos de sua resposta.

269 respostas

Não acho necessário. (21)
Por segurança (2)
Por segurança (2)
Traria maior segurança ao meu animal. (2)
Gostaria de mante-los sempre dentro de casa. (2)
Acho seguro (2)
Para rastrear (2)
Garante uma maior segurança, para localizar o bicho.
Não acho necessário por enquanto.
Seguro e fácil
Porque tenho medo que ele se perca
Para sua segurança e rastreabilidade.

6) Você usaria um dispositivo não implantável em seu(s) animal(is) como método de identificação, rastreio ou armazenamento de dados importantes (doenças prévias, congênitas, situações, entre outros)?

269 respostas



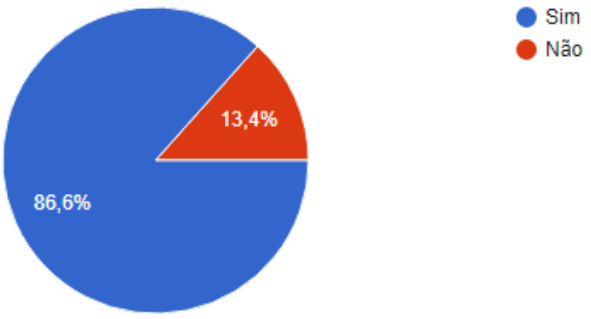
7) Com base na questão anterior (6), justifique os motivos de sua resposta.

269 respostas

Não acho necessário. (21)
Menos invasivo (3)
Menos invasivo (2)
. (2)
É importante. (2)
Segurança (2)
Dependeria do preço e da adaptação do gato ao dispositivo. (2)
Com toda a certeza, todo e qualquer dado que puder preservar o bem estar do bicho é muito importante.
seria legal um dispositivo não invasivo armazenar todas essas informações, que poderão ser de grande importância em certos casos.
Prevenção
Porque me preocupo muito com ele
Se for seguro e não for fácil perder ou ser removido, usaria sim.

8) Você se sentiria seguro com seu(s) animal(is) usando um dispositivo não implantável de identificação, armazenamento de dados e localização?

269 respostas

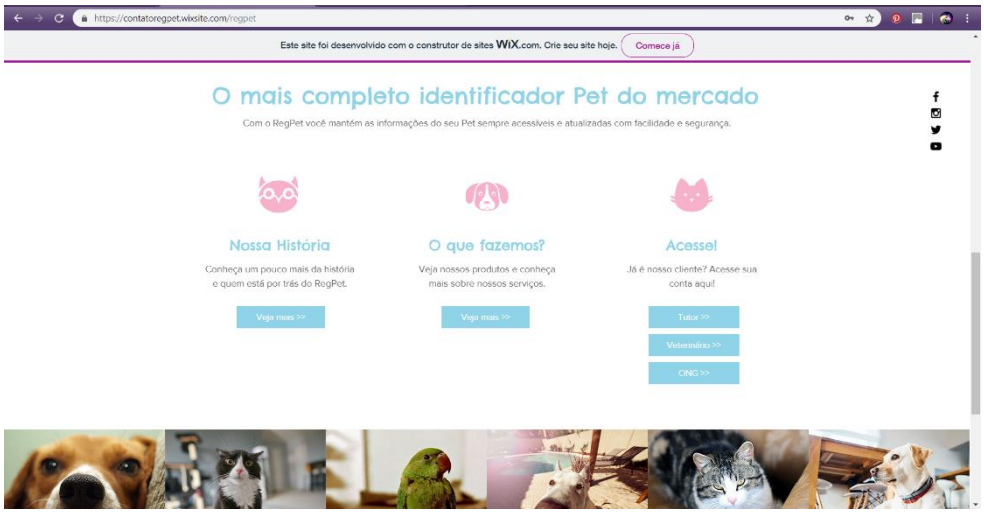


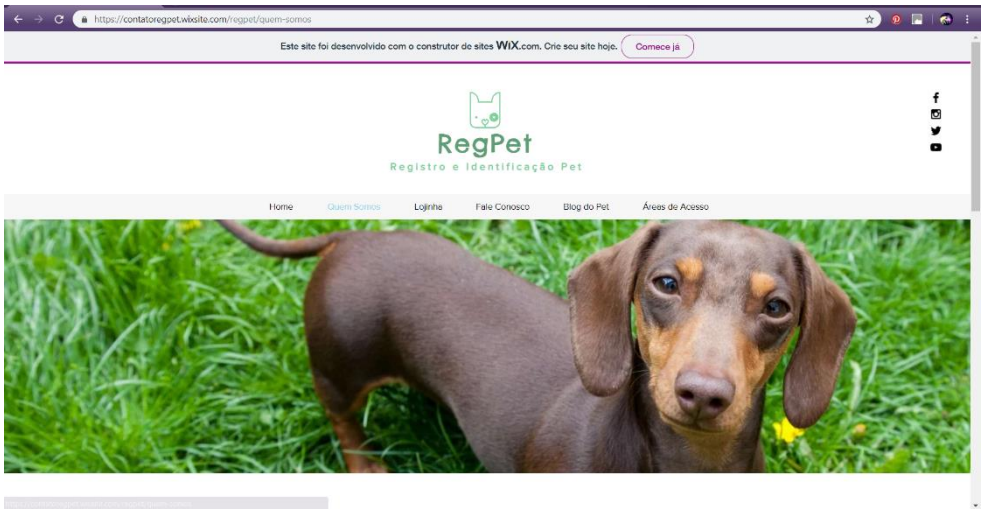
9) Qual a sua opinião sobre um dispositivo que tenha custo entre R$ 40 e R$ 60 para identificação, armazenamento de dados e localização de seu(s) animal(is)?

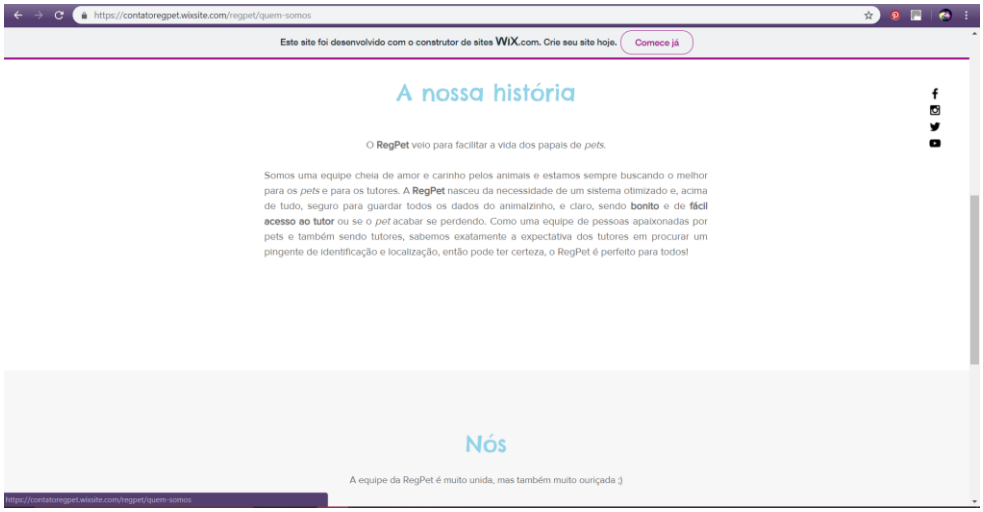
269 respostas

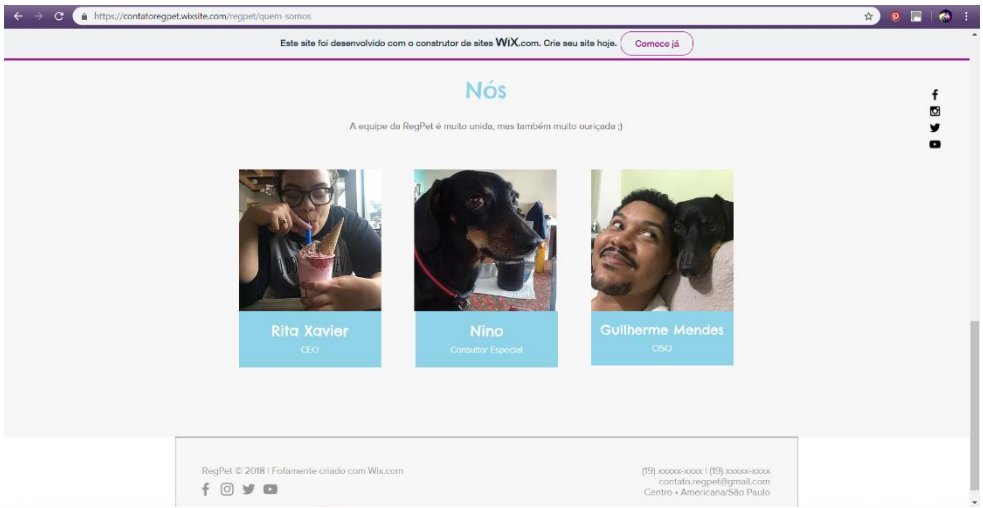
Bom preço e uma boa opção para donos de animais que costumam fugir ou tem muitos problemas de saúde. (21)
Bom (4)
Barato (3)
Bacana (3)
Compraria (2)
Razoável (2)
barato (2)
Barato (2)
Preço não tão acessível, mas que quem se preocupa com o seu animal pagaria tranquilamente. (2)
Acessível. (2)
Muito bom (2)

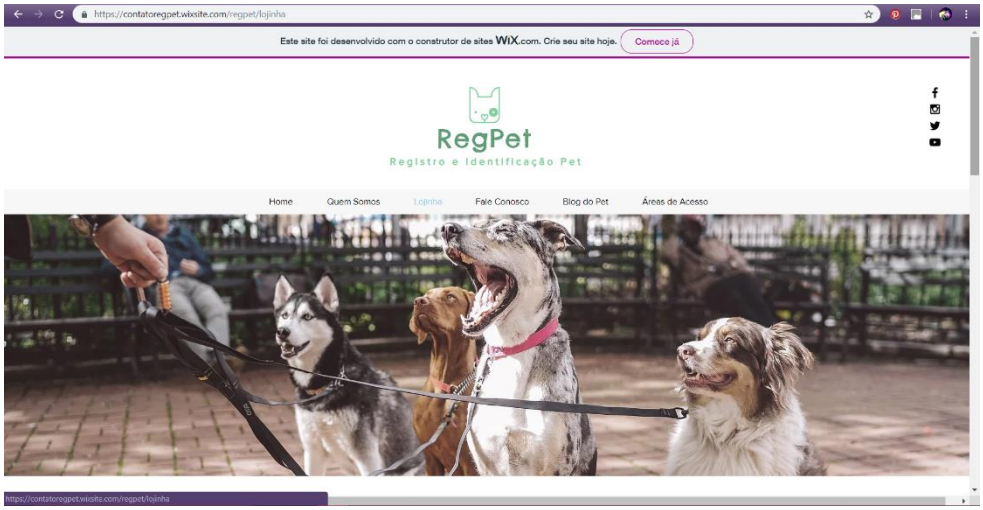
APÊNDICE C – PRINTS DO SITE REGPET



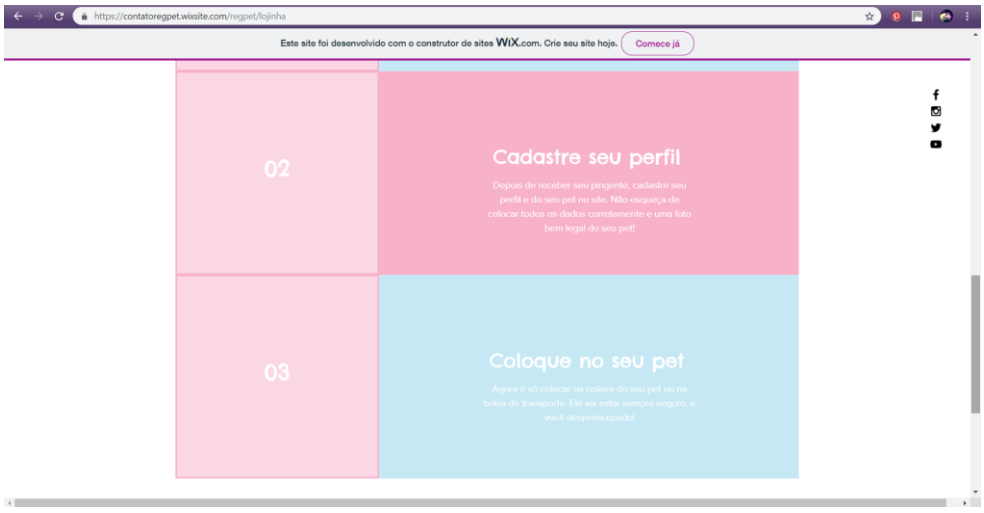


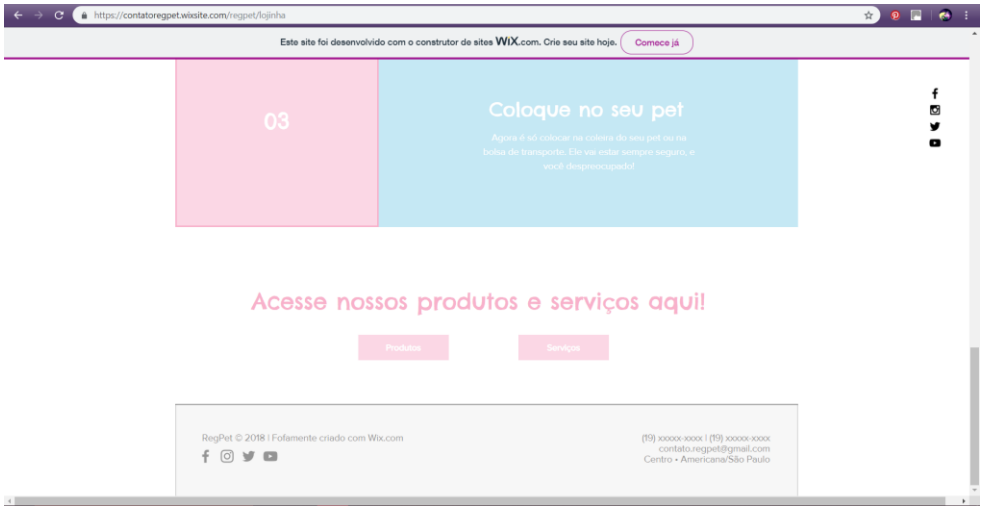

https://contatoregpet.wixsite.com/regpet/quem-somos
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
A nossa história
O RegPet veio para facilitar a vida dos papais de pets.
Somos uma equipe cheia de amor e carinho pelos animais e estamos sempre buscando o melhor para os pets e para os tutores. A RegPet nasceu da necessidade de um sistema otimizado e, acima de tudo, seguro para guardar todos os dados do animalzinho, e claro, sendo bonito e de fácil acesso ao tutor ou se o pet acabar se perdendo. Como uma equipe de pessoas apaixonadas por pets e também sendo tutores, sabemos exatamente a expectativa dos tutores em procurar um pingente de identificação e localização, então pode ter certeza, o RegPet é perfeito para todos!
Nós
A equipe da RegPet é muito unida, mas também muito ouriçada :)

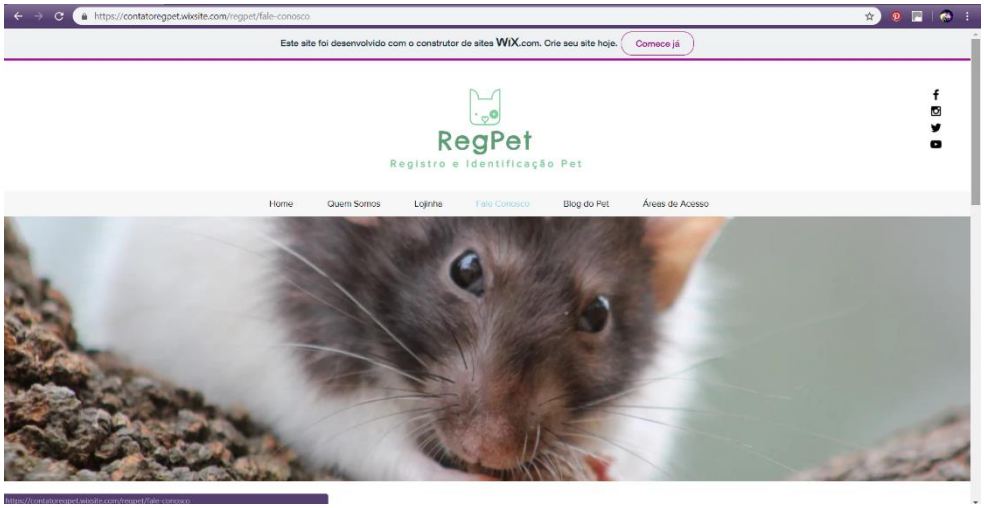

https://contatoregpet.wixsite.com/regpet/quem-somos
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
Nós
A equipe da RegPet é muito unida, mas também muito ouriçada :)
Rita Xavier
CEO
Nino
Consultor Especial
Guilherme Mendes
CISO
RegPet © 2018 | Folhamente criado com Wix.com
(19) xxxxx-xxxx | (19) xxxxx-xxxx
contato.regpet@gmail.com
Centro • Americana/São Paulo

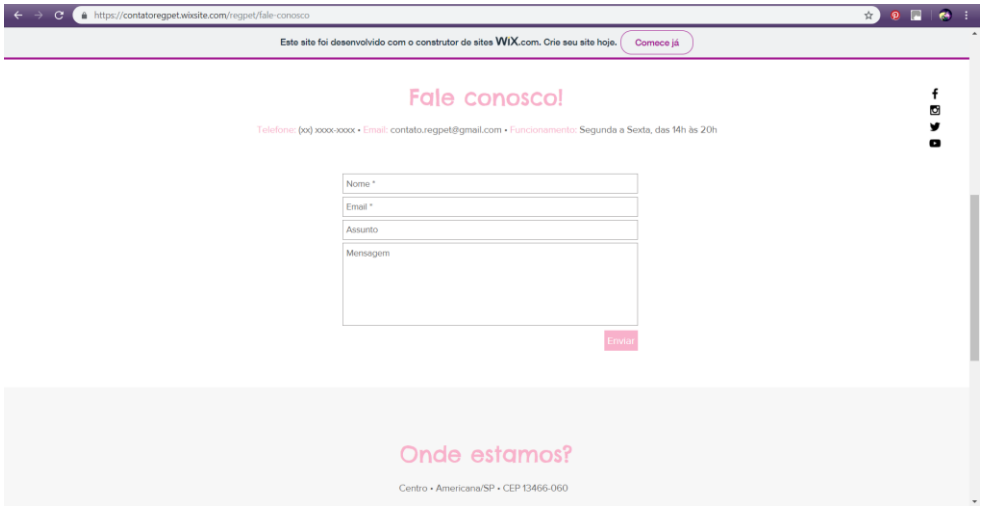

https://contatoregpet.wixsite.com/regpet/lojinha
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
RegPet
Registro e Identificação Pet
Home
Quem Somos
Lojinha
Fale Conosco
Blog do Pet
Áreas de Acesso

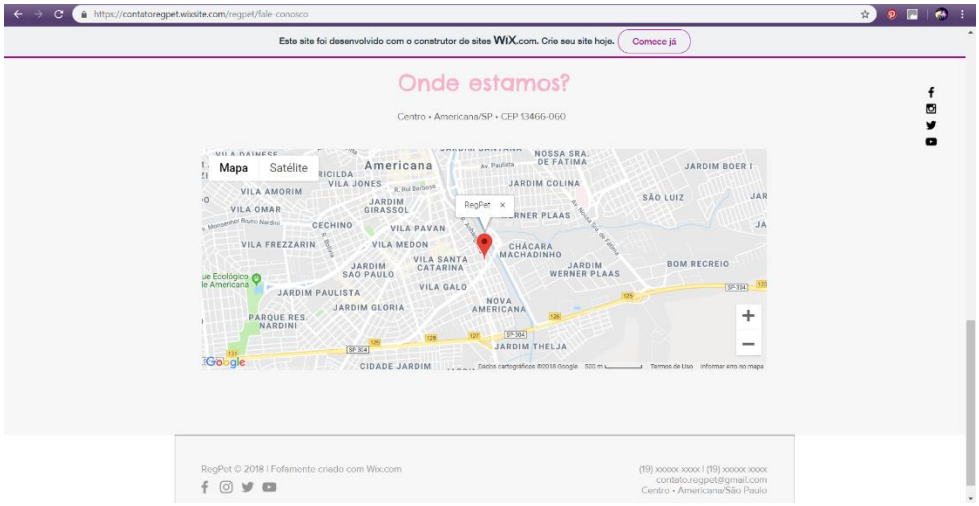

https://contatoregpet.wixsite.com/regpet/lojinha
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
Amamos o que fazemos!
Não produzimos somente um pingente de identificação animal, oferecemos um sistema seguro e otimizado para cadastro e atualização de todas as informações importantes sobre seu melhor amigo. Assim, caso ele se perca ou necessite de cuidados especiais, com uma simples fotografia no código QR impresso no pingente o tutor será notificado sobre a geolocalização do seu pet e quem o encontrou terá acesso as informações necessárias para devolver o bichinho para seu tutor. Também oferecemos um perfil privado, onde o veterinário do pet terá acesso a todos os dados médicos, caso ele necessite mudar de cidade, ou até de país.
01
Escolha seu pingente
Escolha seu pingente em nosso site na aba "lojinha". Lá teremos pingentes de vários preços e modelos. Escolha o que mais te agrada e faça sua compra!

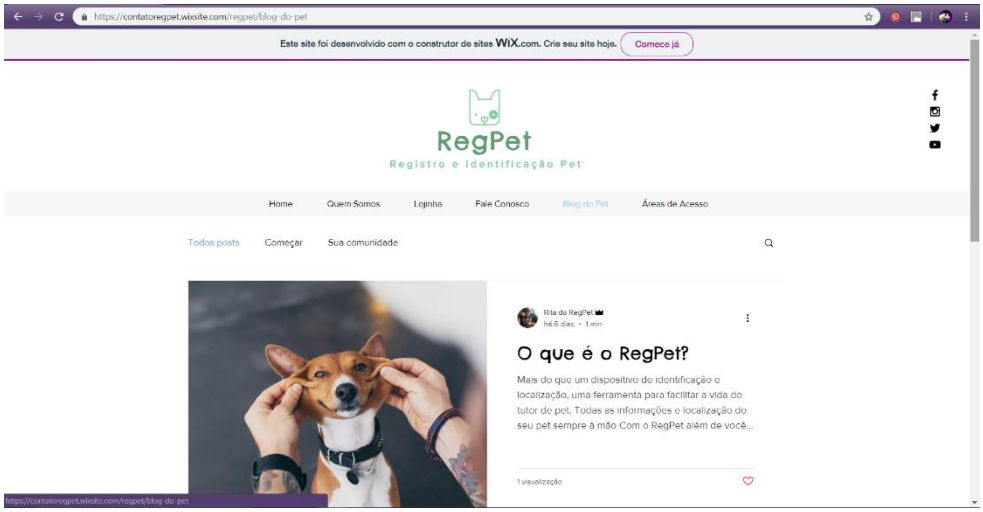

https://contatoregpet.wixsite.com/regpet/lojinha
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
02
Cadastre seu perfil
Depois de receber seu pingente, cadastre seu perfil e do seu pet no site. Não esqueça de colocar todos os dados corretamente e uma foto bem legal do seu pet!
03
Coloque no seu pet
Agora é só colocar na coleira do seu pet ou na bolsa de transporte. Ele vai estar sempre seguro, e você despreocupado!

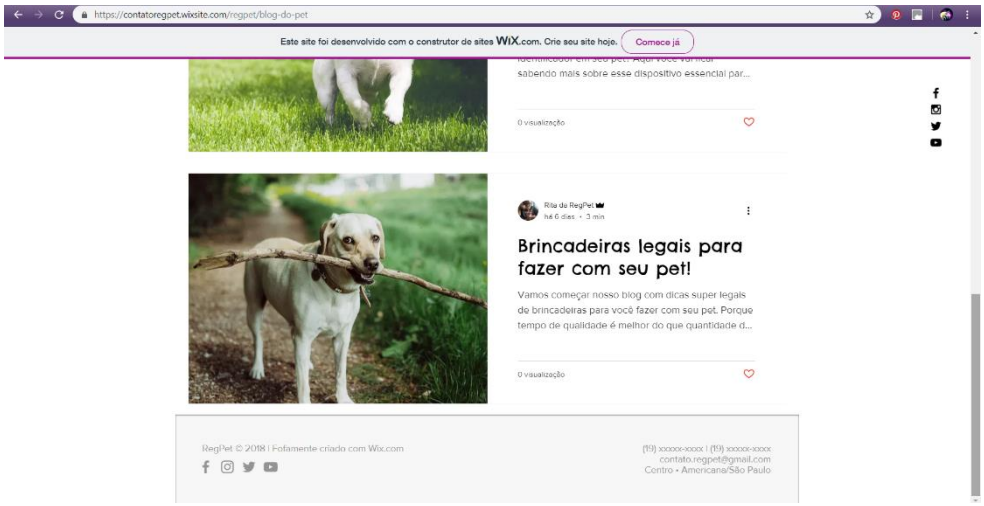

https://contatoregpet.wixsite.com/regpet/lojinha
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
03
Coloque no seu pet
Agora é só colocar na coleira do seu pet ou na bolsa de transporte. Ele vai estar sempre seguro, e você despreocupado!
Acesse nossos produtos e serviços aqui!
Produtos
Serviços
RegPet © 2018 | Fofamente criado com Wix.com
(19) xxxxx-xxxx | (19) xxxxx-xxxx
contato.regpet@gmail.com
Centro • Americana/São Paulo

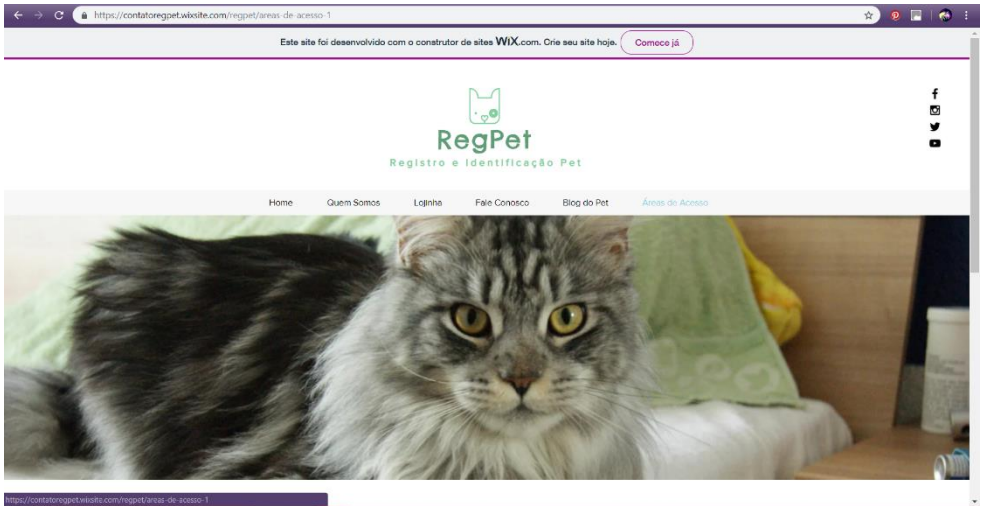

https://contatoregpet.wixsite.com/regpet/fale-conosco
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
RegPet
Registro e Identificação Pet
Home
Quem Somos
Lojinha
Fale Conosco
Blog do Pet
Áreas de Acesso

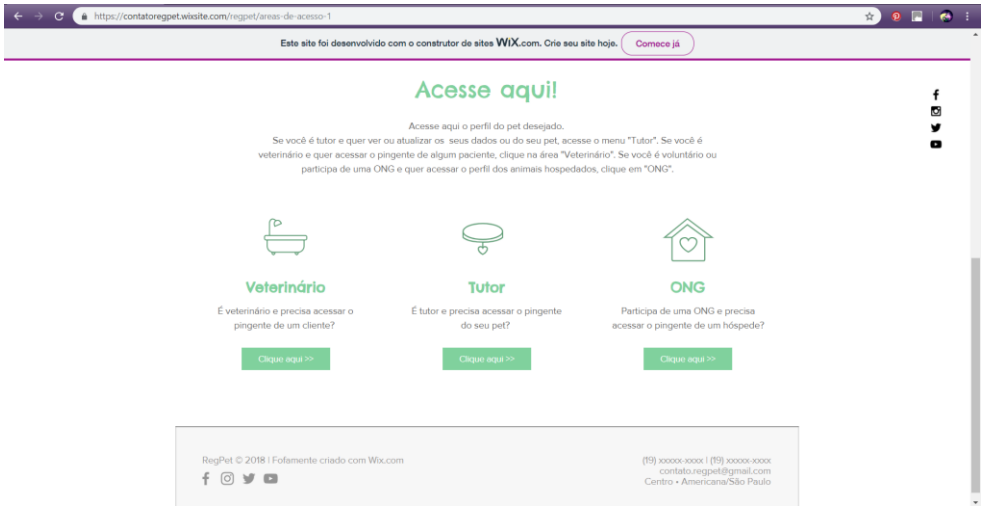

https://contatoregpet.wixsite.com/regpet/fale-conosco
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
Fale conosco!
Telefone: (xx) xxxx-xxxx • Email: contato.regpet@gmail.com • Funcionamento: Segunda a Sexta, das 14h às 20h
Nome *
Email *
Assunto
Mensagem
Enviar
Onde estamos?
Centro • Americana/SP • CEP 13466-060

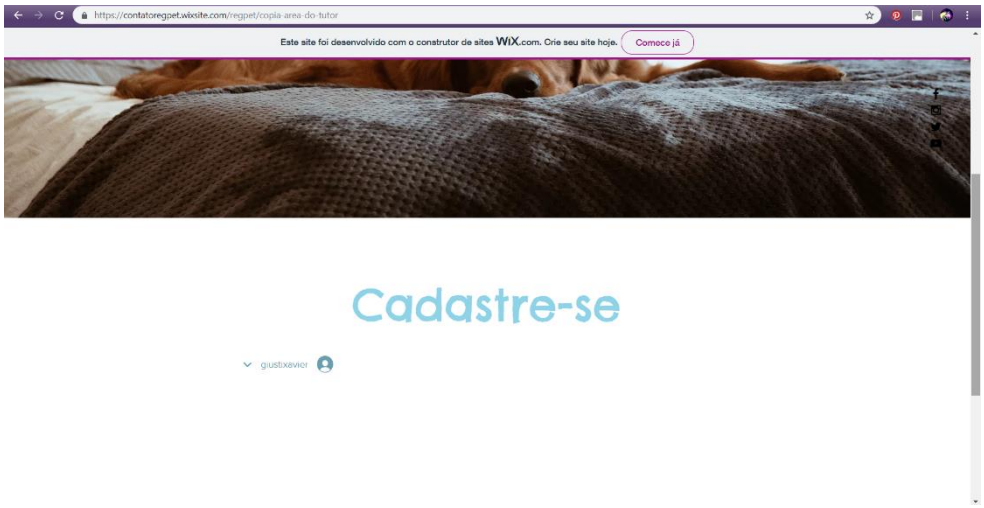

https://contatoregpet.wixsite.com/regpet/fale-conosco
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
Onde estamos?
Centro • Americana/SP • CEP 13466-060
Mapa
Satélite
Americana
RegPet
RegPet © 2018 | Fofamente criado com Wix.com
(19) xxxxx-xxxx | (19) xxxxx-xxxx
contato.regpet@gmail.com
Centro • Americana/São Paulo

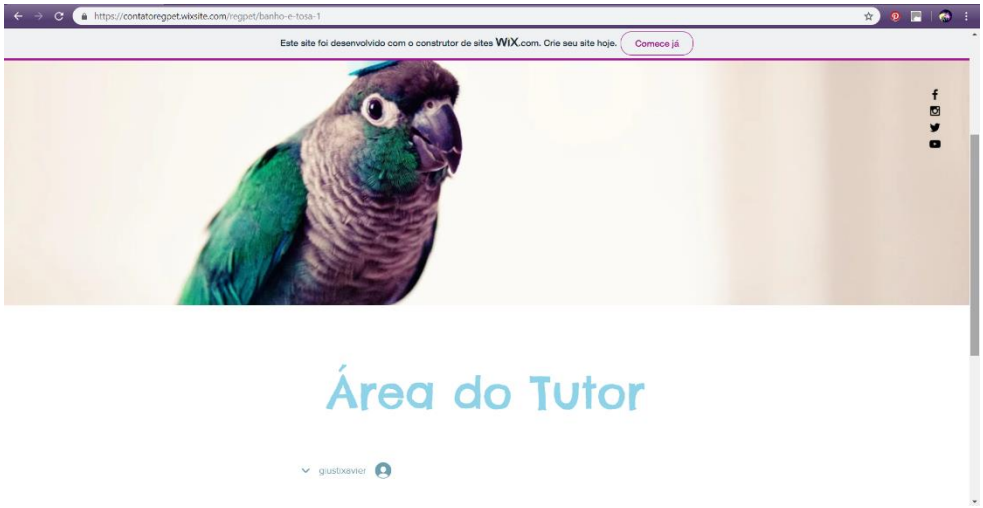

https://contatoregpet.wixsite.com/regpet/blog-do-pet
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
RegPet
Registro e Identificação Pet
Home
Quem Somos
Loja
Fale Conosco
Blog do Pet
Áreas de Acesso
Todos posts
Começar
Sua comunidade
Rita do RegPet
há 6 dias • 1 min
O que é o RegPet?
Mais do que um dispositivo de identificação e localização, uma ferramenta para facilitar a vida do tutor de pet. Todas as informações e localização do seu pet sempre à mão Com o RegPet além de você...
1 visualização

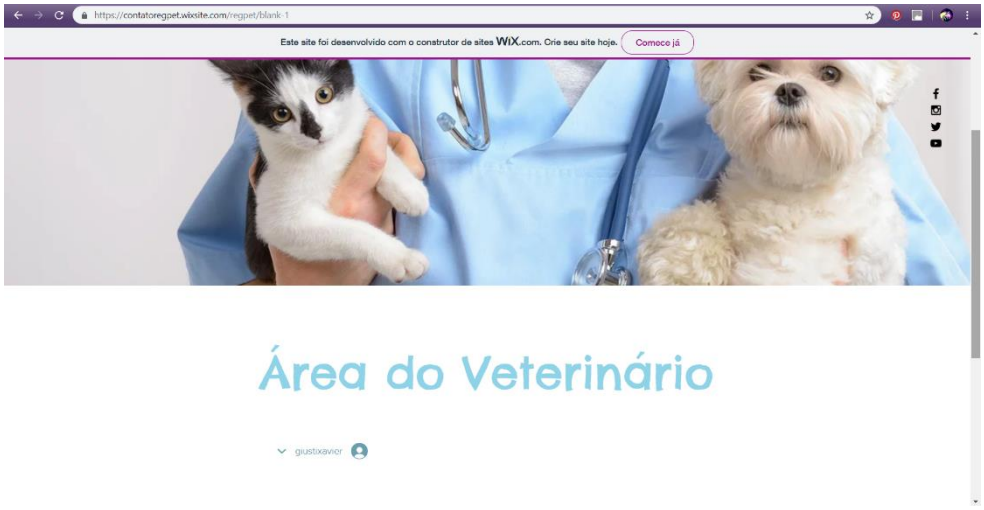

https://contatoregpet.wixsite.com/regpet/blog-do-pet
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
0 visualização
Rita do RegPet
há 6 dias • 3 min
Brincadeiras legais para fazer com seu pet!
Vamos começar nosso blog com dicas super legais de brincadeiras para você fazer com seu pet. Porque tempo de qualidade é melhor do que quantidade d...
0 visualização
RegPet © 2018 | Fofamente criado com Wix.com
(19) xxxxx-xxxx | (19) xxxxx-xxxx
contato.regpet@gmail.com
Centro • Americana/São Paulo

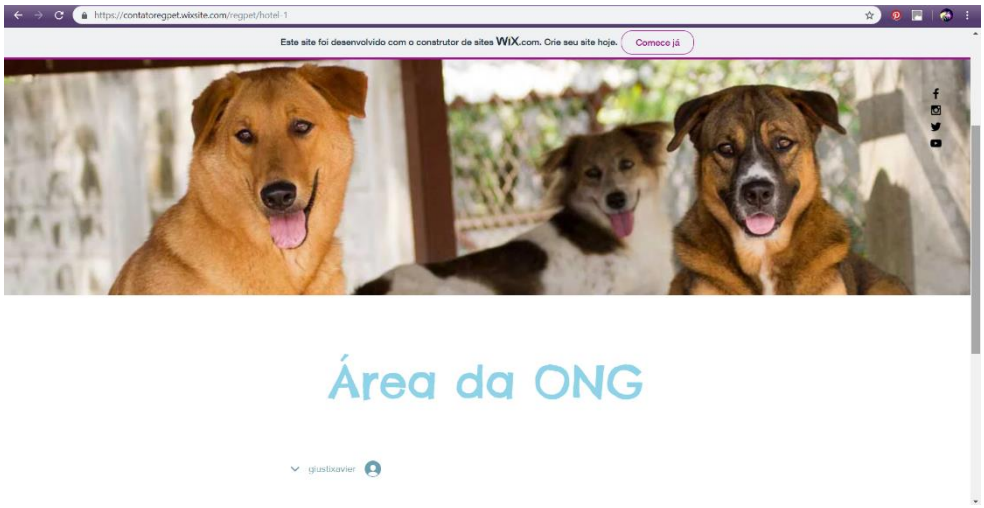

https://contatoregpet.wixsite.com/regpet/areas-de-acesso-1
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
RegPet
Registro e Identificação Pet
Home
Quem Somos
Loja
Fale Conosco
Blog do Pet
Áreas de Acesso

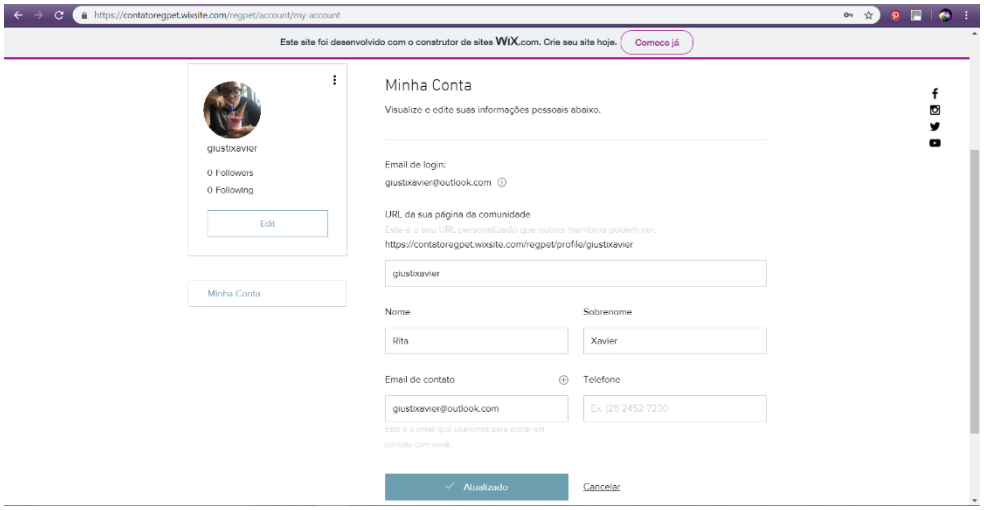

https://contatoregpet.wixsite.com/regpet/areas-de-acesso-1
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
Acesse aqui!
Acesse aqui o perfil do pet desejado.
Se você é tutor e quer ver ou atualizar os seus dados ou do seu pet, acesse o menu "Tutor". Se você é veterinário e quer acessar o pingente de algum paciente, clique na área "Veterinário". Se você é voluntário ou participa de uma ONG e quer acessar o perfil dos animais hospedados, clique em "ONG".
Veterinário
É veterinário e precisa acessar o pingente de um cliente?
Clique aqui >>
Tutor
É tutor e precisa acessar o pingente do seu pet?
Clique aqui >>
ONG
Participa de uma ONG e precisa acessar o pingente de um hóspede?
Clique aqui >>
RegPet © 2018 | Fofamente criado com Wix.com
(19) xxxxx-xxxx | (19) xxxxx-xxxx
contato.regpet@gmail.com
Centro • Americana/São Paulo

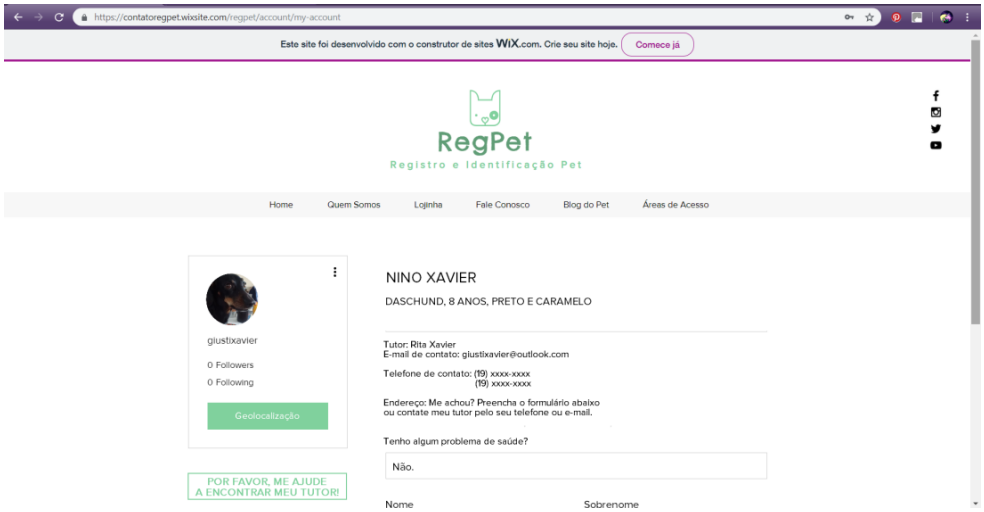

https://contatoregpet.wixsite.com/regpet/copia-area-do-tutor
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
Cadastre-se
giustixavier

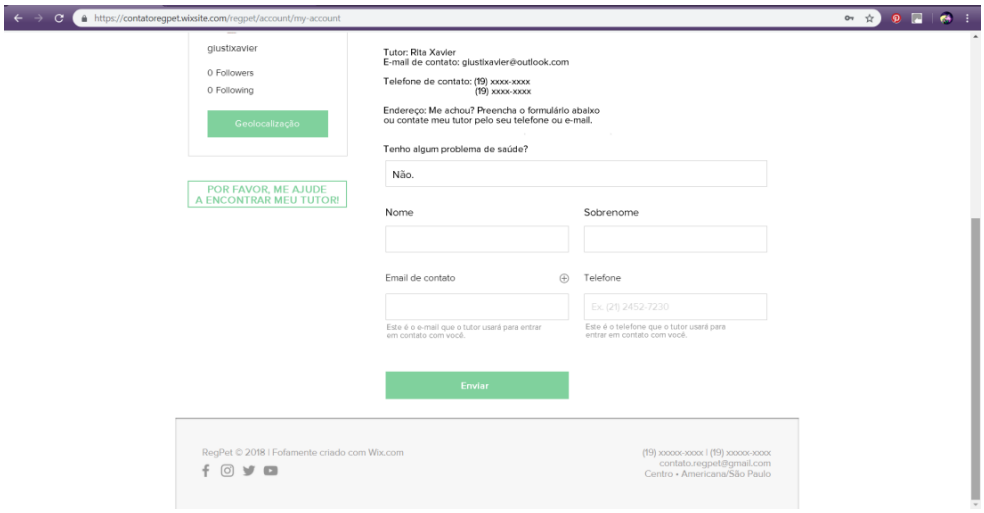

https://contatoregpet.wixsite.com/regpet/banho-e-tosa-1
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
Área do Tutor
giustixavier


https://contatoregpet.wixsite.com/regpet/blank-1
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
Área do Veterinário
giustixavier

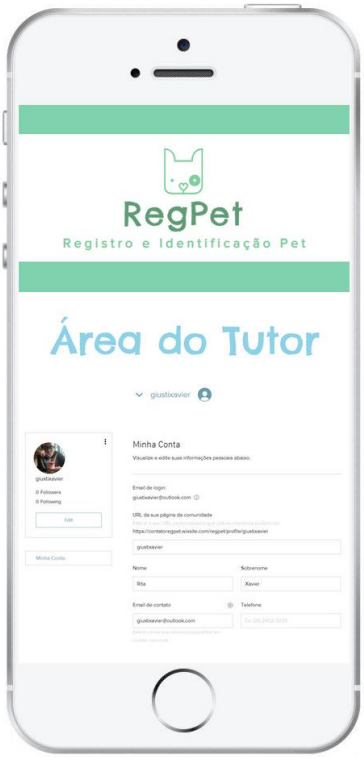

https://contatoregpet.wixsite.com/regpet/hotel-1
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
Área da ONG
giustixavier

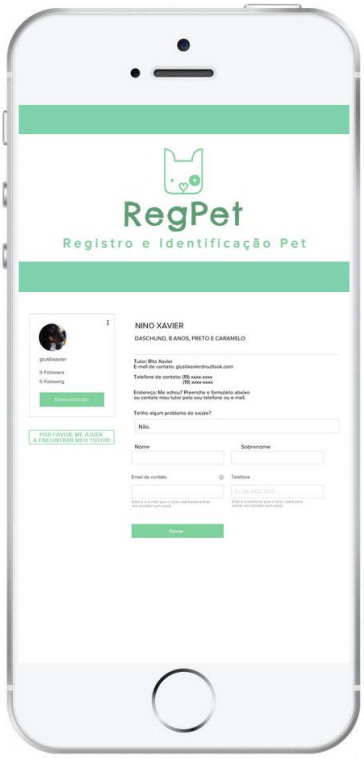

https://contatoregpet.wixsite.com/regpet/account/my-account
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
giustixavier
0 Followers
0 Following
Edit
Minha Conta
Minha Conta
Visualize e edite suas informações pessoais abaixo.
Email de login:
giustixavier@outlook.com
URL da sua página da comunidade
https://contatoregpet.wixsite.com/regpet/profile/giustixavier
giustixavier
Nome
Rita
Sobrenome
Xavier
Email de contato
giustixavier@outlook.com
Telefone
Ex. (21) 2452-7230
Atualizado
Cancelar


https://contatoregpet.wixsite.com/regpet/account/my-account
Este site foi desenvolvido com o construtor de sites WiX.com. Crie seu site hoje.
Comece já
RegPet
Registro e Identificação Pet
Home
Quem Somos
Lojinha
Fale Conosco
Blog do Pet
Áreas de Acesso
giustixavier
0 Followers
0 Following
Geolocalização
POR FAVOR, ME AJUDE A ENCONTRAR MEU TUTOR!
NINO XAVIER
DASCHUND, 8 ANOS, PRETO E CARAMELO
Tutor: Rita Xavier
E-mail de contato: giustixavier@outlook.com
Telefone de contato: (19) xxxx-xxxx
(19) xxxx-xxxx
Endereço: Me achou? Preencha o formulário abaixo
ou contate meu tutor pelo seu telefone ou e-mail.
Tenho algum problema de saúde?
Não.
Nome
Sobrenome


https://contatoregpet.wixsite.com/regpet/account/my-account
giustixavier
0 Followers
0 Following
Geolocalização
POR FAVOR, ME AJUDE A ENCONTRAR MEU TUTOR!
Tutor: Rita Xavier
E-mail de contato: giustixavier@outlook.com
Telefone de contato: (19) xxxx-xxxx
(19) xxxx-xxxx
Endereço: Me achou? Preencha o formulário abaixo
ou contate meu tutor pelo seu telefone ou e-mail.
Tenho algum problema de saúde?
Não.
Nome
Sobrenome
Email de contato
Telefone
Ex. (21) 2452-7230
Este é o e-mail que o tutor usará para entrar em contato com você.
Este é o telefone que o tutor usará para entrar em contato com você.
Enviar
RegPet © 2018 | Fofamente criado com Wix.com
(19) xxxxx-xxxx | (19) xxxxx-xxxx
contato.regpet@gmail.com
Centro • Americana/São Paulo

APÊNDICE D – PRINTS DO APLICATIVO REGPET


RegPet
Registro e Identificação Pet
Área do Tutor
giustixavier
Minha Conta
Visualize e edite suas informações pessoais abaixo.
Email de login
giustixavier@outlook.com
URL da sua página da comunidade
https://contato.reggetwaste.com/reggetprofile/giustixavier
giustixavier
Nome
Sobrenome
Rita
Xavier
Email de contato
Telefone
giustixavier@outlook.com


RegPet
Registro e Identificação Pet
NINO XAVIER
DASCHUND, 8 ANOS, PRETO E CARAMELO
giustixavier
0 Followers
0 Following
Geolocalização
POR FAVOR, ME AJUDE A ENCONTRAR MEU TUTOR!
Tutor: Rita Xavier
E-mail de contato: giustixavier@outlook.com
Telefone de contato: (11) xxxx-xxxx
(11) xxxx-xxxx
Endereço: Me acheu? Preencha o formulário abaixo ou contate meu tutor pelo seu telefone ou e-mail.
Tenho algum problema de saúde?
Não.
Nome
Sobrenome
Email de contato
Telefone
Enviar


RegPet
Registro e Identificação Pet
ATENÇÃO!
Sou um cão idoso e com necessidades especiais.
Tenho displasia e diabetes.
Talvez eu esteja sem minha medicação e com dor.
Por favor, contate meu tutor com urgência!
NANA XAVIER
PASTOR ALEMÃO, 12 ANOS, CAPA PRETA
giustixavier
0 Followers
0 Following
Geolocalização
POR FAVOR, ME AJUDE A ENCONTRAR MEU TUTOR!
Tutor: Rita Xavier
E-mail de contato: giustixavier@outlook.com
Telefone de contato: (11) xxxx-xxxx
(11) xxxx-xxxx
Endereço: Me acheu? Preencha o formulário abaixo ou contate meu tutor pelo seu telefone ou e-mail.
Tenho algum problema de saúde?
Sim
Nome
Sobrenome
Email de contato
Telefone
Enviar