FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Thiago Augusto de Asevedo de Sousa

Estudo de caso: Análise de Certificado SSL de sites e-commerce utilizando Qualys SSLLABS

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Thiago Augusto de Asevedo de Sousa

Estudo de caso: Análise de Certificado SSL de sites e-commerce utilizando Qualys SSLLABS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof.(a) Esp. Rodrigo Nogueira Tofani

Área de concentração: Segurança da Informação

Americana, SP.

2017

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

S698e SOUSA, Thiago Augusto de Asevedo de

Estudo de caso: análise de certificado SSL de sites e-commerce utilizando Qualys SSL-LABS. / Thiago Augusto de Asevedo de Sousa. – Americana: 2017.

39f.

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

Orientador: Prof. Esp.Rodrigo Nogueira Tofani

1. Comércio eletrônico I. TOFANI, Rodrigo Nogueira II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 658.845

Thiago Augusto de Asevedo de Sousa

Estudo de caso: Análise de Certificado SSL de sites e-commerce utilizando Qualys SSLLABS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 28 de Junho de 2017.

Banca Examinadora:

Rodrigo Nogueira Tofani (Presidente)
MBA – Master Business Administrator
FATEC Americana

Edson Roberto Gaseta
MBA em Gestão Empresarial.
FATEC Americana

Henri Alves de Godoy
Mestre em Redes de Computadores
FATEC Americana

AGRADECIMENTOS

Em primeiro lugar agradeço a minha família, sendo minha base em todos os momentos de minha vida, também pela oportunidade em estudar em uma instituição pública na qual possui uma estrutura de curricular essencial para minha formação. Agradeço ao meu orientador pelo suporte na criação desse documento. Acredito que sem ajuda de todas as pessoas envolvidas não seria possível realizar esse estudo de caso.

DEDICATÓRIA

Dedico esse trabalho a todos os estudantes de TI, e interessados em obter conhecimento sobre o assunto, que o mesmo contribua para o desenvolvimento de todos.

RESUMO

Com a expansão da tecnologia em todos os setores da indústria e a possibilidade de efetuar compras pela internet, a necessidade de se obter um meio seguro de trafegar dados e informações sigilosas se tornou ainda mais crucial para a existência de qualquer empresa. O protocolo SSL dentre vários protocolos é o que mais se destaca em atender esse requisito, pois o mesmo tem como principal função estabelecer um meio de comunicação segura entre o cliente e o servidor. Utilizado em grande escala pelo comercio de vendas pela internet, o mesmo possui características únicas, garantindo a integridade e irrefutabilidade dos usuários desse protocolo de modo a ser considerado uma Assinatura Digital. Esse trabalho tem por objetivo, por meio de estudo de caso, analisar se a utilização e configuração desse protocolo nos sites e-commerce que tiveram as maiores receitas em 2016 são considerados seguros. Nesse estudo será gerada uma tabela de checagem dos itens de Segurança da Informação nos relatórios utilizados, seguindo as melhores práticas estabelecidas pelas Autoridades Certificadoras, onde cada item validado será exemplificado e justificado. Para que seja possível realizar essa análise será utilizada uma ferramenta gratuita SSLLABS para gerar os relatórios das configurações do Certificado de cada empresa e-commerce, com esse relatório é possível avaliar e classificar cada empresa de acordo com a sua aderência as melhores práticas validadas, onde assim será possível identificar se as empresas estão se preocupando com a Segurança da Informação em seus sites de venda. Sendo possível afirmar com os dados obtidos, que todos os sites possuem parte dos requisitos avaliados, sendo que 40% das empresas possuem todos os requisitos avaliados em seus Certificados, e somente uma não obteve 50% de aderência aos itens validados, evidenciando a preocupação das empresas em utilizar um relatório seguro.

Palavras Chave: e-commerce; Protocolo SSL; Segurança da Informação.

ABSTRACT

With the expansion of technology in all sectors of the industry and the possibility of buying online, the need to obtain a secure means of the transferring sensitive information and inteligence has become even more crucial for the existence of any company. The SSL protocol, among several others, in the protocol that most fails to meet this requirement, because it's man funcion is to establish a secure communication between the cliente and the server. It is used on a large scale by internet sales, and its has unique characterisctics, guaranteeing the integrity and irrefutability of the users of this protocol so that it is considered a digital signature. This paper presentes a case study that validates if the use and configuration od this protocol in the e-commerce sites that had the hightest revenues in 2016 are considered safe. In this study, a check table of information security items will be generated in the reports used, following the best practices established by the Certification Authorities, where each validated item will be exemplified and ajustified. In order other the perform this analysis, a free SSLLABS tool will be generate the reports of the configurations of the Certificate of each e-commerce company. With this report, it is possible to avaluate and classify each company according to the adherence to the best validated practices, whereby it will be possible to identify if companies are worrying about Information Security on their sles sites. It is possible to see in the obtained data that all the sites have some of the requirements, 40% of the companies have all the requirements of their certificates, and only one has not obtained 50% adherence to the validated items, showing a concern of the companies presented By the secure system.

Keywords: *e-commerce; SSL protocol; Information Security.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Desde quando a Internet deu seus primeiros passos para a área de vendas, a importância da Segurança da Informação com o mesmo vem se desenvolvendo a fim de proteger o máximo os dados dos seus clientes.

Porém com estatísticas realizadas por vários meios de análise, ainda consta que o maior receio do consumidor em efetuar compras pela Internet ocorre por eles não se sentirem seguros na compra.

Esse trabalho tem como objetivo geral analisar se os *sites* com maior venda em *e-commerce* nacional atendem às melhores práticas de utilização do Certificado digital SSL criado pelas Autoridades Certificadoras. Como objetivo específico será analisado quais as melhores práticas de mercado, elencando os itens mais importantes, a fim de analisar quantitativamente se os sites seguem essas práticas, criando uma tabela de porcentagem à aderência às essas melhores práticas.

Para melhor entendimento do tema, o trabalho está dividido em **seis** capítulos, sendo a introdução o **primeiro** capítulo, os conceitos gerais como **segundo** capítulo abordando todos os conceitos necessários para entendimento do estudo de caso, esse capitulo possui diversos subcapítulos, partindo de Segurança da Informação, onde trata do entendimento de segurança da informação, introduzindo o tripé de Segurança, a Criptografia de Chaves e os Certificados Digitais. No **terceiro** capítulo foram definidos os princípios de *e-commerce*, e sua estrutura. No **quarto** capítulo são definidos os critérios para execução do estudo de caso, informando as limitações e escopo do projeto, baseando-se nos itens mais representam a Segurança da Informação através das melhores práticas no protocolo, analisando os sites e seus Certificados. No **quinto** capítulo está o resultado da análise e as considerações dos relatórios gerados no estudo de caso. Concluindo o trabalho com as Considerações Finais como **sexto** capitulo, contextualizando todo trabalho e evidenciando qual empresa de venda pela Internet possui o protocolo de SSL mais seguro, segundo requisitos de empresas certificadoras.

2 CONCEITOS GERAIS

2.1 Segurança da Informação

Com a interconexão e a expansão da era digital, a segurança da informação tornou-se essencial para qualquer existência de organizações, pois assim como a expansão tecnologia aumenta a cada dia, os riscos de ameaças e vulnerabilidade também se expandem.

A ISO/IEC 27002:2015 (ABNT, 2015) define segurança da Informação como:

> “Segurança da Informação é a proteção da Informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos para o negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

Para obter a Segurança da Informação dentro de qualquer instituição é necessário implantar um conjunto de controles. Esses controles incluem criação de políticas, processos e procedimentos que necessitam ser estabelecidos, implementados, monitorados e analisados, onde seu principal maior foco é ter a certeza que os objetivos de negócio e de Segurança da instituição sejam atendidos. Todas essas estruturas de Segurança da Informação devem ser feitas em conjunto com os processos de Negócios, a fim de existir um alinhamento único na estratégia organizacional da instituição.

A segurança da informação é necessária por todas as organizações, pois a informação e os processos existentes são ativos importantes para o negócio. A definição, acompanhamento e melhoria de Segurança da Informação são essenciais para ganho de competitividade e lucratividade em seus produtos e serviços além de auxiliar na imagem da organização e atendimento a requisitos legais.

A ISO/IEC 27002:2015 (ABNT, 2015) ainda informa que umas das várias funções de Segurança da Informação é a viabilização de negócios para o comercio eletrônico, evitando ou mitigando os riscos mais relevantes.

Para se estabelecer os requisitos de Segurança da Informação deve se atentar aos três requisitos descritos na ISO, sendo o primeiro requisito a obtenção de informações a partir de análises de risco, levando em conta os objetivos e

estratégia da Instituição. Nesse primeiro requisito, são apontadas as ameaças e as vulnerabilidades, e a partir disso é possível estimar a probabilidade das ameaças e qual o possível impacto na instituição caso a vulnerabilidade for explorada.

O segundo requisito diz respeito à legislação e regulamentação vigentes, em que a legislação governamental nunca deve ser violada em uma política de Segurança da Informação interna, abrangendo os contratos comerciais, contratos de prestadores de serviços e trabalhistas, contratos com parceiros entre outros.

O terceiro requisito informa sobre um conjunto de princípios, objetivos e requisitos de negócio. Esse conjunto visa apoiar o desenvolvimento de suas operações.

Sêmola (2003) complementa a informação dizendo:

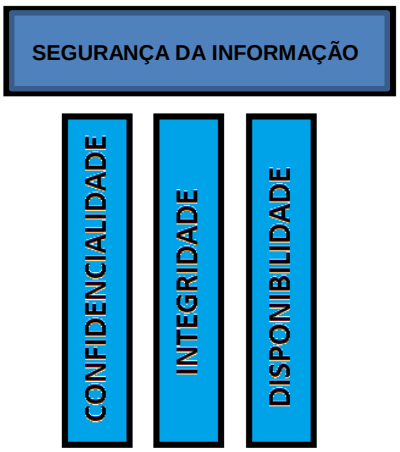
> "Podemos definir segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade."

2.2 Tripé de Segurança da Informação

Merkow e Breithaupt (2014) informa que dentro de Segurança da Informação tem o objetivo garantir ao menos uma das três partes que compõem a base de Segurança da Informação (Confidencialidade, Integridade e Disponibilidade), onde é conhecido como tripé CID, sendo consideradas características básicas para uma Segurança da Informação.

O tripé CID é utilizado amplamente em todas as atividades de segurança da informação, onde se define que uma informação está segura quando o tripé de Segurança está em sua estrutura (Figura 1).

Figura 1: Conceito Tripé de Segurança da Informação



Fonte: Próprio autor

Para deixar mais claro o conceito do CID, será explicada cada base do tripé conforme Prado e Souza (2014) descrevem em seu livro.

Confidencialidade – Parte do processo que protege as informações sensíveis da Organização. Essa ação visa limitar o acesso à informação somente para pessoas autorizadas pelo proprietário da informação.

Integridade – Parte do processo que garante que a informação mantenha todas as características originais feitas proprietário da informação, esse item do tripé ainda visa que as informações trafegadas sejam verdadeiras.

Disponibilidade – Parte do processo que garante que a informação esteja disponível sempre que for necessário esse item ainda deve garantir que os meios para acessar essas informações também estejam disponíveis sempre que for solicitado.

Prado e Souza (2014) também informam que além dos três princípios de Segurança da Informação também a irrefutabilidade e outros que são correlacionados com o tripé CID. Podemos considerar que a esse item é uma composição de autenticidade com a integridade da informação, pois garante a origem da informação e também garante que a informação não foi alterada durante qualquer processo. A irrefutabilidade está diretamente relacionada com a Segurança da Internet, pois o Certificado Digital garante o não repudio do dono do certificado,

sendo assim, se o certificado digital fosse usado somente para esse fim, já seria de grande serventia para a Segurança da Informação.

2.3 Criptografia

Criptografia é uma palavra que surgiu do grego "*kryptós*" = escondido e "*graphé*" = escrita, denominada ciência que usa a matemática para ocultar informações. A criptografia embaralha as informações em códigos que não são possíveis de entender o que está escrito de forma não decifrável. Na qual é necessário efetuar o processo reverso para decifrar e tornar a informação clara novamente.

Monteiro e Mignoni (2007) cita que o nível de Segurança estabelecida pela criptografia depende do tamanho da chave, quanto mais bits a chave possuir, mais difícil será decifrar a mesma. Eles também citam que o uso da criptografia possui recursos para garantir os serviços, conforme Tabela 1.

Tabela 1: Itens de Segurança da Informação

Autenticação	Garante a origem das Informações, garante sua comprovação.
Integridade	Assegura a veracidade e integridade da Informação
Confidencialidade	Garante o acesso às informações somente pessoas autorizadas
Irrefutabilidade	Assegura que o emissor da mensagem não possa negar que foi o autor.

Fonte: Próprio autor

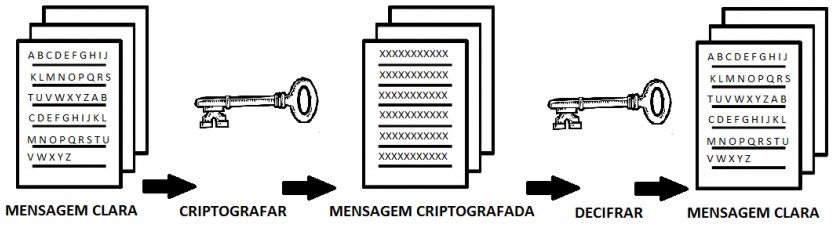
A criptografia é separada em dois tipos: Criptografia Simétrica e Criptografia Assimétrica, onde cada uma possui uma forma de cifrar e decifrar os dados.

2.3.1 Criptografia Simétrica

Primeira forma conhecida para cifrar dados confidenciais. A criptografia simétrica tem como principal característica a utilização de somente uma chave para criptografar e decifrar um arquivo, isso significa que tanto o dono do arquivo quanto o receptor deverão conhecer a chave utilizada. O livro aborda que com a utilização de apenas uma chave, foi necessário criar uma “Política de Segurança para Troca e Guarda de Chaves”, cuja finalidade é evitar que intrusos roubem, usem e distribuam a chave, para outras pessoas.

Para exemplificar o funcionamento de uma criptografia de chave simétrica utilizaremos a Figura 2 como exemplo.

Figura 2: Criptografia de chave Simétrica



Fonte: Próprio autor

Nesse desenho podemos ver que na primeira imagem a mensagem está clara, porém quando é cifrada, sua leitura não é mais compreensível, se tornando clara novamente somente quando a mensagem é decifrada. É possível analisar também que a mesma chave que criptografou a mensagem foi à mesma que decifrou tornado claro o funcionamento da criptografia de modelo simétrico.

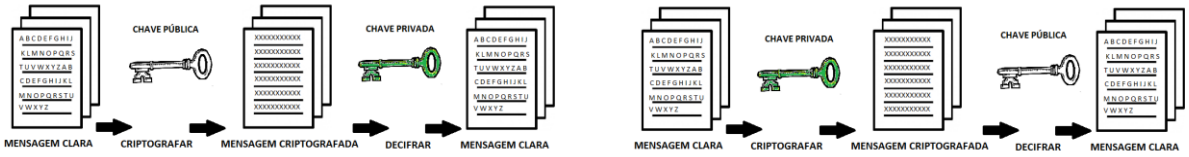
2.3.2 Criptografia Assimétrica

Conhecida como criptografia de chave pública, a Criptografia Assimétrica utiliza um método de par de chaves diferentes, conhecidas como chave privada e chave pública, nas quais cada usuário desse tipo de criptografia possui ambas as chaves.

Uma informação cifrada por uma chave pública só pode ser decifrada pela chave privada, e qualquer informação cifrada por uma chave privada só pode ser decifrada por uma chave pública, ou seja, ambas as chaves podem cifrar ou decifrar uma informação.

Segundo Monteiro e Mignoni (2007), “A chave Privada deve ser mantida no mais absoluto sigilo, entanto a Chave Pública deverá ser tornar pública de alguma forma”. (Figura 3)

Figura 3: Criptografia de chave Assimétrica



Fonte: Próprio autor

A utilização de Criptografia Assimétrica permite utilização do serviço de Certificado Digital, um serviço que utiliza documentos de identificação do emissor além de sua chave pública. Como o serviço faz parte do estudo de caso desse trabalho, haverá uma definição mais aprofundada do serviço, pois a Criptografia assimétrica possui outros serviços.

2.4 Certificado Digital

Com a expansão do comercio eletrônico, houve uma necessidade em ter segurança nas transações bancarias em todo tipo de pagamentos online. A preocupação em ter segurança da informação em transações on-line, e pelo fato das constantes tentativas de ataque que quebraram a segurança que eles possuíam, foi-se necessário desenvolver um novo tipo de tecnologia para que atendessem os requisitos de Segurança da Informação que já não ofereciam tanta segurança. Monteiro e Mignoni (2007) citam que, a criptografia foi à tecnologia com maior êxito para resolver os problemas de Segurança da Informação naquele momento, essa tecnologia que viabilizou a capacidade de assinar digitalmente um documento eletrônico. Porém, para a utilização de uma criptografia de chaves pública existe uma necessidade de possuir mecanismos confiáveis e grandes o suficiente para

publicar e divulgar as chaves, que em 1978 foi divulgada pelo Loren Kohnfelder denominado Identidade Digital ou Certificado Digital, na qual um arquivo que contém informações sobre o usuário é dono da chave, além da própria Chave Pública.

Para que esse Certificado Digital tenha Integridade e Autenticidade em sua existência, o mesmo deve ser assinado por uma entidade confiável chamada Autoridade de Certificação ou AC. Para se tornar uma AC à entidade necessita de softwares para emissão de Certificados Digitais e vários procedimentos administrativos, que no livro são citados como Infraestrutura de Chave Pública ou ICP. A segurança dentro do processo do ICP visa o estabelecimento de regras e procedimentos do seu funcionamento adequado por meio de documentos. Os documentos por si são conhecidos como Política de Certificados e Declaração de Práticas de Certificação. Esses documentos estabelecem todas práticas e procedimentos que serão implementados em todo processo de Certificação.

Monteiro e Mignoni (2007) citam:

> “O processo de Certificação é executado ela AC de acordo com a Política de Certificados (PC) e a Declaração de Práticas de Certificação (DPC). A PC e a DCP são pela AC e Pela ICP”.

Portanto podemos afirmar que a Autoridade de Certificação utiliza a Política de Certificados e a Declaração de Práticas de Certificação para gerarem seus Certificados. E as Políticas de Certificados e a Declaração de Práticas de Certificação são elaboradas pelas Autoridades de Certificação e pelas Infraestruturas de Chave Pública.

Monteiro e Mignoni (2007) ainda citam que o Certificado Digital é um arquivo digital, conhecido pelos tradicionais documentos de identificação onde possui informações do usuário ou entidade além de sua chave pública.

Esses arquivos eletrônicos são rubricados de forma digital pela Autoridade Certificadora interligando esses arquivos ao seu certificado, nesse processo, o Certificado possui o mesmo valor que um documento físico e pode ser utilizado para identificação de usuário ou entidade que foi certificada (servindo de prova de autenticidade) além de servir para distribuir a chave pública.

A Certificação Digital usa como base a criptografia de chaves públicas, onde a chave pública fica alocada no certificado e a chave privada fica armazenada em um lugar sigiloso pelo assinante. Nesse contexto qualquer informação pode ser assinada pela chave privada do assinante, mas essa assinatura só será validada com a chave pública relacionada.

Monteiro e Mignoni (2007) citam que: “A AC, ao emitir um Certificado digital, estará garantindo que o proprietário do certificado é quem realmente diz ser.”, ou seja, quando uma Autoridade Certificadora emite um certificado ela esta garantindo a irrefutabilidade do proprietário do Certificado. Porém para que essa garantia seja formalizada a Autoridade Certificadora assina o certificado com a sua chave privada.

No trabalho, o estudo de caso o trabalho não limitará a nenhuma ICP, pois será analisado o Certificado SSL gerado por qualquer Autoridade Certificadora, acredita-se que existem casos em que sites de vendas online no Brasil sejam assinados por empresas de fora dos pais.

2.5 SSL (Secure Socket Layer)

Segundo dados apresentados por Barros (2015), SSL é um protocolo de comunicação de dados, na qual é implementado um canal de comunicação seguro entre as aplicações de redes. A empresa Netscape Corporation desenvolveu o protocolo em 1994, e, desde então diversas aplicações começaram a se integrar com o protocolo.

O maior impulso no uso do SSL foi à chegada do certificado digital, pois permitiu que em alguns casos substituíssem a autenticação por *login* e senha.

O SSL é responsável por estabelecer um link criptografado entre um navegador e um servidor *web*. Esse *link* garante que tudo dado passado por ele tenha integridade e confidencialidade, sendo dois tripés de Segurança da Informação, sendo o padrão mais utilizado em todo mundo, sendo referência em proteção de transações online.

Para se criar uma conexão SSL é necessário que o servidor web tenha um certificado SSL, em que o servidor preenche várias informações sobre sua identidade, site e empresa. Nessa conexão o servidor cria duas chaves criptografadas, uma chave pública e uma chave privada.

Essas chaves são guardadas por certificados diferentes, em que a chave pública colocada no *Certificate Signing Request* (Solicitação de Assinatura do Certificado ou CSR), um arquivo que contém seus dados detalhados. A chave pública não precisa ser secreta, apenas a chave privada, em que a Autoridade Certificadora validará suas informações que estão alocadas no CSR, e emitirá um Certificado SSL que contem seus dados para que seja possível utilizar o recurso SSL, após isso o servidor irá corresponder com seu Certificado SSL, emitindo a sua chave privada, e assim será possível estabelecer uma conexão criptografada entre o site e o navegador Web de seu cliente.

O procedimento acima mencionado é invisível aos usuários, sendo a única informação sutilmente passada pelo navegador, um cadeado no canto esquerdo, com a cor verde, em que clicando com o botão direto do mouse é possível validar o certificado SSL e seus detalhes.

É importante destacar que o protocolo SSL não é um algoritmo que faz criptografia, ele é responsável por implementar uma via segura na troca de informações, não determinando escolhas de padrão de criptografia ou de certificados, possibilitando a escolha de diversos protocolos para essas funções.

Outro ponto importante é que todos os Certificados SSL válidos na Internet são emitidos por empresas legalmente responsáveis.

Segundo site info.ssl o protocolo SSL é a tecnologia de segurança padrão para estabelecer um *link* criptografado entre um servidor web e um navegador. Este *link* garante que todos os dados transmitidos entre o servidor web e navegadores permaneçam privados e integrais. SSL é um padrão da indústria e é usado por milhões de sites na proteção de suas transações on-line com seus clientes.

2.6 TLS (Transport Layer Security)

O protocolo TLS surgiu em 1999 baseado na versão 3 do SSL. Barros (2015) explica que:

> "[..] Netscape, até então 'dona da Internet' lançou o SSLv2 (Security Socket Layer). O protocolo foi construído para criar um túnel criptográfico entre um navegador e um servidor web, provendo sigilo, autenticação e garantia de integridade da comunicação. No ano seguinte, eles lançam uma nova versão SSL v3 com uma série de melhorias de segurança."

Porém quando o protocolo deixou de ser publicado pela Netscape, o nome foi alterado para TLS (Transport Layer Security), recebendo o número de versão 1.0. Segundo ele mesmo conclui "internamente o protocolo 'responde' como SSL v3.1."

Existem pequenas diferenças entre o SSL e o TLS, sendo a principal diferença a norma que rege. O TLS possui habilidade de trabalhar em diferentes portas e usa algoritmos de criptografias mais fortes enquanto o SSL usa algoritmos mais simples.

Um dado muito interessante dito por Marcel (2015): "O protocolo TLS foi criado para substituir o SSL, um protocolo que já é considerado inseguro". Apesar da sigla "SSL" ser muito utilizada, hoje ela é sinônimo de "TLS".

Ou seja, toda vez que é falado sobre SSL na verdade se fala ao mesmo tempo de SSL e TLS, como sugere Kohl (2016) no seu artigo.

3 E-COMMERCE

Segundo o site significados, e-commerce é a abreviação em inglês de *eletronic commerce*, que significa "Comércio Eletrônico" em português. Refere-se a todo tipo de comercio feito por meio de dispositivos móveis, sejam eles, computadores, celulares e tablets.

Ainda o site gestor de conteúdo afirma que “Comércio electrónico ou *e-commerce* é um conceito aplicável a qualquer tipo de negócio ou transação comercial que implique a transferência de informação através da Internet”. Tendo uma abrangência enorme de comércio, desde produtos, como eletrônicos, brinquedos e presentes, até serviços como, serviços streaming (Spotify, Netflix), aplicativos, ferramentas entre outros.

Nakamura (2011) informa que existem cinco tipos de Comércio eletrônico.

3.1 Business to Business (B2B)

Business to Business ou Negócio para Negócio, mais conhecido como B2B, como o próprio nome diz, são comércios entre empresas. O trabalho cita que:

> “[..]operações de compra e venda de produtos, informações e serviços por meio da web ou utilizando redes privadas partilhadas entre as empresa. Substituindo o tradicional comercio físico nas lojas e estabelecimentos comerciais.”

Ele também reforça que esse tipo de comércio precisa atingir altos níveis de eficiência, processos eficazes que atendam às necessidades do negócio.

Existem três grupos dos principais portais de B2B.

- Intranet: Portal usando para comunicação interna da empresa, sendo de uso exclusivo dos profissionais e colaboradores da empresa.
- Extranet: Acesso utilizado para se relacionar com outras empresas B2B, basicamente uma rede que liga a empresa aos seus parceiros de negócio.
- Portal de terceiros: Negociação de produtos e serviços utilizando a internet como recurso, facilitando a venda de produtos e serviços aos seus clientes.

3.2 Business to Consumer (B2C)

B2C ou Negócio para Consumidor é o comercio realizado por empresas de vários seguimentos com o consumidor através da internet. O maior destaque nesse seguimento é a criação de lojas virtuais, tendo contato direto com consumidores que utilizam a internet como recurso.

Nakamura (2011) cita que existem três tipos de B2C:

- Leilões: Trabalha com licitação eletrônica, existe a possibilidade de acompanhar a apresentação do produto. Sua maior vantagem é a conveniência, a conectividade global, porém é a maior chance de fraude em pagamento acontece nesse tipo de B2C.

- Lojas Online: Sendo o mais conhecido de e-commerce, é o meio mais comum dos B2C, em que várias empresas vendem seus produtos por meio de sites, pela Internet, ganhando muita competitividade, pois propiciam aos seus clientes produtos com preços mais baixos, tendo uma variedade de escolha enorme, contendo todas as informações e descrições dos produtos ofertados.

- Serviços online: Disponibilização de serviços por meio da Internet para seus clientes. O maior objetivo é a praticidade e facilidade em adquirir serviços ou até mesmo mídias (Netflix, Spotify, entre outros).

Nakamura (2011) ainda aborda o fator determinante de sucesso de uma empresa que trabalha em B2C:

> “A grande preocupação do B2C está voltada para o sistema logístico, pois a entrega dos produtos adquiridos via Internet em ótimas condições e no prazo determinado é um dos 18 requisitos fundamentais no comércio eletrônico. Essa estruturação do sistema de logística é um fator determinante para o sucesso do empreendimento.”.

Este trabalho focará no protocolo SSL de sites de comércio eletrônico B2C, onde posteriormente será mais detalhado o motivo da escolha, e limitação da análise.

3.3 Consumer to Consumer (C2C)

Consumidor para Consumidor ou C2C é o comércio realizado somente entre consumidores. Essa venda é apoiada por empresas intermediadoras como Mercado Livre, OLX, porém as mesmas não têm poder sobre o produto. Essas empresas intermediadoras oferecem credibilidade aos vendedores e cobradores, em que os pagamentos só são realizados após o recebimento do produto, dificultando as fraudes.

3.4 Government to Citizen (G2C)

Governo para Consumidor é uma forma de comércio realizado pelo governo ou outro órgão público para com o consumidor via web. São atividades relacionadas a pagamento de taxas de imposto, multas e tarifas suportadas pela Internet. Também classificam G2C sites do governo que oferecem serviços e orientação aos seus clientes sobre educação e empregos, proporcionando ao cidadão conhecimento, informação e os serviços diversos que são disponibilizados pelo governo.

3.5 Government to Business (G2B)

Governo para Negócio são negócios realizados entre governos e empresas em que utilizam a Internet como meio de comunicação. São utilizados para realizar pregões e licitações, compra de fornecedores, entre outras atividades.

4 DEFINIÇÃO E LIMITAÇÃO PARA ESTUDO DE CASO

Para iniciarmos o estudo de caso precisamos montar o escopo do projeto, onde primeiramente identificará quais as melhores práticas na criação e configuração do Certificado, ferramenta para gerar o relatório e sites que serão analisados.

4.1 Definição dos itens e ferramentas que serão utilizados

Para desenvolver a estrutura da pesquisa, de modo que o mesmo se adeque às necessidades de segurança. Utilizaremos o Guia das melhores práticas de SSL da Autoridade Certificadora (AC) SSL, que teve o seu surgimento em 2002, atua em mais de 120 continentes sendo uma das poucas AC com certificado cinco estrelas na instalação e configuração de Certificados Digitais.

Nesse artigo de melhores práticas, as análises foram divididas em quatro partes; sendo elas: Chave Privada e Certificados; Configuração; Desempenho e Segurança em HTTP. Essa estrutura será seguida, juntamente com seus parâmetros.

No item Chave Privada e Certificados será validado em cinco parâmetros definidos, onde o primeiro Item validará se o Certificado utilização pela empresa é aceito e valido pela AC; no segundo parâmetro será validará se a chave utilizada no certificado é a RSA 2048 bits, sendo o mínimo recomendado, pois essas chaves utilizam 112 bits de Segurança. A AC ainda informa que existem outras chaves mais potentes como RSA 3072 bits, que oferecem 128 bits de Segurança, porem são mais lentas. Existem também as chaves ECDSA que podem ser uma alternativa para melhorar o desempenho, pois em 256 bits na chave ECDSA 128 são de Segurança, porem existem alguns sites antigos que não suporta essa chave como primeiro parâmetro.

O terceiro parâmetro a ser avaliado e a renovação de certificados, pois dentro do site ele deixa claro que existe a possibilidade um invasor com experiência em Certificados Digitais consegue as chaves da memória, sendo a melhor pratica renovara chave sempre que receber um novo Certificado. O artigo ainda explica que a troca exige um tempo de configuração, dependendo de quantas bandeiras o a

empresa utiliza seu certificado, nesse contexto avaliaremos se os certificados possuem 30 dias ou mais de validade.

O quarto parâmetro é a abrangência do certificado, para avaliar se existe alguma configuração onde não deixe nenhuma página do site com avisos de certificados inválidos, ou como comunicação não segura, diminuindo a confiança do usuário no site. Esse item ainda sugere avaliar se um site solicita comunicação com e\ou sem prefixo WWW.

O artigo de melhores práticas ainda informa que a Segurança do Certificado depende da força da chave usada para assinar o certificado. E por conta disso precisamos avaliar se o *hash* utilizado por esse certificado é o SHA 256. O antigo *hash* utilizado SHA1 atualmente é considerado inseguro e por isso a utilização dele é considerada um risco para o Certificado digital.

O Segundo item é o de Configuração, onde será avaliado se as credenciais são devidamente apresentadas. Para isso precisamos avaliar três parâmetros básicos de configuração, sendo o primeiro a configuração de cadeias completas de certificados. Segundo o artigo o certificado sozinho em um servidor é insuficiente, sendo necessário dois ou mais certificados para construir uma cadeia completa de confiança. O maior erro que ocorre nesta configuração é justamente a implementação do certificado valido no servidor, porem os certificados intermediários muitas vezes não são totalmente implementados. Esse desvio é facilmente corrigido com a utilização de todos os protocolos concedidos pela AC.

Como segundo parâmetro será analisado qual protocolo está sendo utilizado. Atualmente existem cinco protocolos da família SSL: SSL / TLS: SSL v2, SSL v3, TLS v1.0, TLS v1.1 e TLS v1.2. O artigo evidencia que:

- SSL v2 é inseguro e não deve ser usado;
- SSL v3 é inseguro quando usado com HTTP;
- TLS v1.0 também é um protocolo que não deve ser usado;
- TLS v1.1 e v1.2 são ambos sem problemas de segurança conhecidos, mas apenas v1.2 fornece modernos algoritmos criptográficos.

Nesse parâmetro será validada a configuração e a utilização do TLS 1.2, pois o próprio artigo informa que os outros certificados não são totalmente seguros.

O último parâmetro do item Comparação valida Mitigação de Problemas Conhecidos, na qual validará se os patches de segurança relacionados ao SSL e TSL são aplicados.

O terceiro item que será analisado chama-se Desempenho, pois para uma segurança bem implementada, não devemos ter problemas com o desempenho da aplicação. Selecionamos apenas um parâmetro, sendo ele o parâmetro de avaliação de demasia em Segurança na aplicação. As melhores práticas informam que uma chave muito curta, torna-se o protocolo inseguro, porem se a chave for muito grande, torna-se mais lento a cifra e a decifra das informações, sendo o mínimo ideal uma chave de 2048 bits.

O quarto item avaliará a segurança em HTTP e nas aplicações que utilizam o recurso SSL. O primeiro parâmetro é o envolvimento da criptografia nas aplicações, pois a criptografia ainda é opcional, diminuindo a segurança. A melhor pratica a ser seguida, é criptografia em tudo após a troca de chaves.

O segundo parâmetro validará se existem Cookies Seguros, pois segundo o guia de melhores práticas, informa que uma aplicação com SSL seguro, os cookies devem ser inseridos como Seguro dentro da aplicação quando o mesmo é criado.

Para facilitar a análise foi elaborado a Tabela 2 contendo os itens e parâmetros à serem analisados.

Tabela 2: Itens de Validação dos Certificados

Item	Parâmetro
Chave Privada e Certificados	O emissor do Certificado é reconhecido por alguma Autoridade Certificadora?
	O site utiliza chave RSA 2048 e/ou ECDSA?
	O certificado utilizado tempo de expiração superior há 30 dias?
	Todos os sites possuem sessão com certificado?
	O hash utilizado é no mínimo o SHA 256?
Configuração	Os domínios foram configurados para serem utilizados com o certificado?
	O site utiliza o protocolo TLS 1.2?
	O site possui patches SSL e TLS instalados?
Desempenho	O site possui uma chave igual ou maior que 2048 bits?
Segurança em HTTP	Existe criptografia em todo o site após a troca de chaves?
	Os cookies do site estão configurados como Seguros?

Fonte: Próprio autor

4.1 LIMITAÇÕES DO ESTUDO DE CASO

Para popular as informações na Tabela 2 “Itens de Validação dos Certificados”, o estudo de caso coletou as cinco empresas que tiveram o maior faturamento em 2016 efetuado pelo site e-commerce Brasil. Esse estudo limitará a cinco empresas, pois utilizaremos um software livre, que possui limitações em relatório e as outras empresas que estão nesse ranking possui uma representatividade baixa comparada as TOP 5. A Tabela 3 possui as empresas dessa relação, juntamente a bandeira a ser analisada. Para preservar a identidade da empresa, os nomes e as bandeiras foram alteradas, assim como as URL utilizadas.

Tabela 3: Bandeiras escolhidas para representar as empresas

Empresa	Bandeira Escolhida	URL Utilizada
Empresa 1	bandeira1.com.br	https://www.bandeira1.com.br
Empresa 2	bandeira2.com.br	https://www.bandeira2.com.br
Empresa 3	bandeira3.com.br	https://www.bandeira3.com.br
Empresa 4	bandeira4.com.br	https://www.bandeira4.com.br
Empresa 5	Bandeira5.com.br	https://www.bandeira5.com.br

Fonte: Adaptado de: http://sbvc.com.br/ranking-50-maiores-empresas-do-e-commerce-brasileiro-2016/ (2016)

O site e-commerce Brasil, informou em 02 de Dezembro de 2016, para gerar esse ranking o site utilizou critérios como: - Cotação do dólar, Dados fornecidos pelas empresas, Balanços contábeis, entre outro.

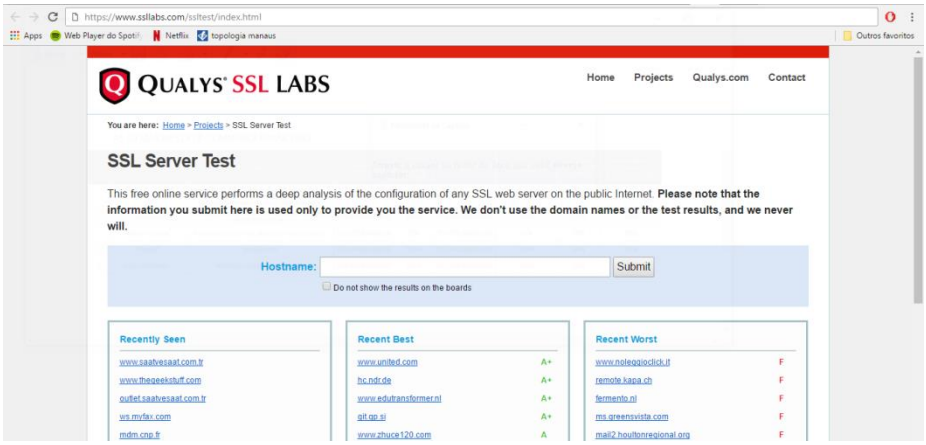
É importante ressaltar que, nesse ranking foi utilizada a empresa que possui o certificado (como mostra o primeiro lugar à empresa que possui o certificado se chama Empresa1, e dentro dessa bandeira possuímos vários sites, porem a configuração e gerado do certificado é a mesma, independente da bandeira que vamos gerar o relatório). Sendo assim, nas empresas que tiverem mais de uma bandeira, será selecionada apenas uma, totalizando cinco bandeiras que terão seus certificados analisados.

Para que seja possível efetuar essa análise, precisamos de uma ferramenta para geração de relatório, onde de acordo com as melhores práticas geram um ranking de aderência. Para geração desse relatório, foi utilizado um laboratório em *Cloud* da Empresa Qualys chamado “SSLLABS”. Para utilizar essa ferramenta é preciso que exista conexão com a internet, pois a ferramenta é WEB, logo na página inicial possui a opção “*test your server*”, que quando clicado já direciona para a página onde se insere a URLS (figura 4) estudada, sem a necessidade de criar um perfil para utilização.

A empresa Qualys é uma empresa que fornece uma plataforma em nuvens integrada para Gerenciamento de Segurança da Informação. A empresa foi fundada em 1999 na Califórnia, foi pioneira oferecer produtos de gestão de vulnerabilidades como aplicações na web utilizando um modelo de software como serviço. A empresa Qualys “[..] tem mais de 7.700 clientes em mais de 100 países, incluindo a maioria dos Forbes Global 100 (Pesquisa efetuada pela Forbes, para validar quais são as 100 maiores empresas do mundo, a pesquisa se baseia em média de receita, lucro, ativos e valor de mercado para eleger as empresas).”. A página do SSLLABS foi desenvolvida para estudos e pesquisa sobre SSL, não possui nenhum vínculo comercial na sua utilização e geração de relatórios.

Para utilizar a mesma, precisamos informar qual URL onde o certificado se encontra, para gerar o mesmo. (Figura 4)

Figura 4: Site SSLLABS



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 12 de Maio de 2017

As empresas solicitam os certificados para utilizar em suas as bandeiras, por isso foi selecionado a primeira bandeira informada, conforme Tabela 3.

O relatório gerado é uma fotografia atual do Certificado, sendo que o mesmo pode ser alterado, renovado e modificado a qualquer momento pelo dono do Certificado e assim alterando resultado caso seja realizado outra análise posterior à mudança. Por conta disso será inserido no Apêndice desse trabalho, seguindo a sequência da Análise.

5 ANÁLISE DOS RELATÓRIOS

Cada empresa teve um relatório gerado pelo site ssllabs, onde o mesmo contém informações do certificado SSL através das URLs inseridas na ferramenta. Esses resultados foram analisados e inseridos na planilha criada contendo os requisitos que serão validados nos Certificados SSL. A planilha foi criada de forma quantitativa, onde as perguntas recebem respostas de “SIM” ou “NÃO” para que somente assim fosse possível avaliar a % de aderência as melhores práticas.

Todos os resultados inseridos na Tabela 4 com resultado “Não” serão justificados, inserindo parte do relatório com a informação coletada na análise de cada empresa.

Tabela 4: Análise dos Certificados SSL de acordo com as melhores práticas

Parâmetro	Empresa1	Empresa2	Empresa3	Empresa4	Empresa5
A chave utilizada é reconhecida por alguma Autoridade Certificadora?	Sim	Não	Sim	Sim	Sim
O site utiliza RSA 2048 e/ou ECDSA?	Sim	Sim	Sim	Sim	Sim
O certificado utilizado tempo de expiração superior há 30 dias ?	Sim	Não	Sim	Sim	Sim
Todos os sites possui sessão com certificado?	Sim	Não	Sim	Sim	Sim
O hash utilizado é no mínimo o SHA 256?	Sim	Sim	Sim	Sim	Sim
Os dominios foram configurados para serem utilizados com o certificado?	Sim	Não	Não	Sim	Sim
O site utiliza o protocolo TLS 1.2?	Sim	Sim	Sim	Sim	Sim
O sites possui patches SSL e TLS instalados?	Sim	Sim	Sim	Sim	Sim
O site possui uma chave igual ou maior que 2048 bits?	Sim	Sim	Sim	Sim	Sim
Existe criptografia em todo o site após a troca de chaves?	Sim	Não	Sim	Sim	Sim
Os cookies do site estão configurados como Seguros?	Sim	Não	Não	Sim	Não

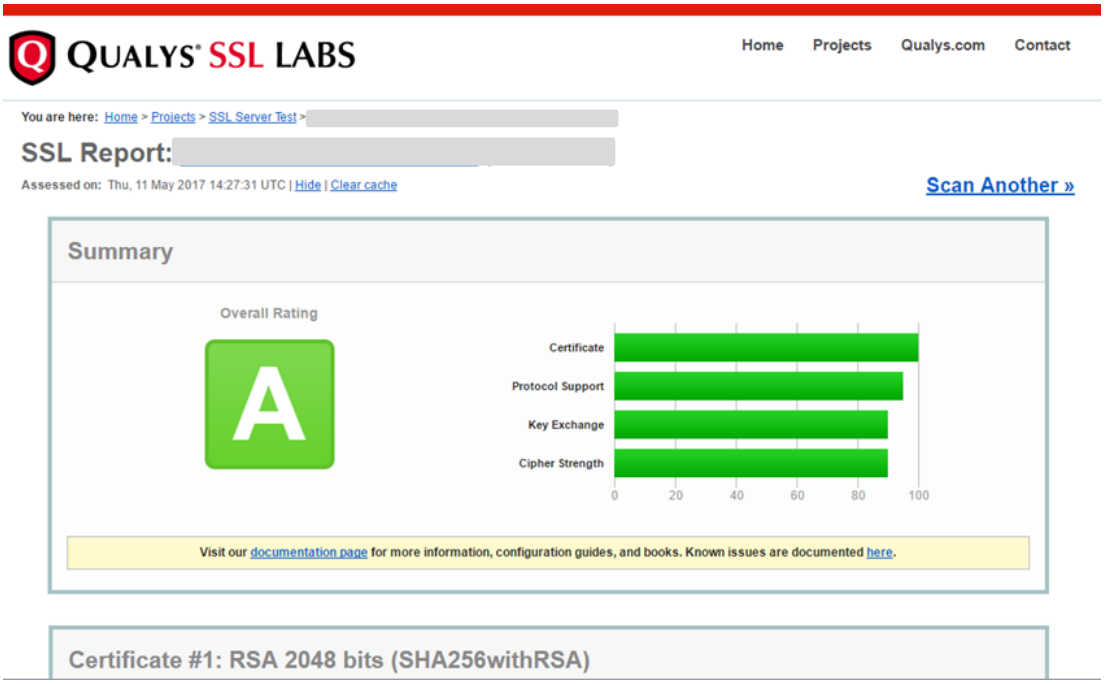
Fonte: Próprio autor

De imediato, podemos validar que existem algumas empresas que não atingem a totalidade os requisitos básicos das melhores práticas recomendado pela AC's, tendo ainda um item que mais de 50% das empresas não atendem, analisaremos com mais detalhe cada empresa. Para tornar mais visível de onde foi extraída a informação para a análise, parte do relatório foi inserido como figura, porem o relatório completo está anexado ao Apêndice desse trabalho.

A Empresa1 que corresponde à Bandeira1, atingiu 100% de aderência aos itens analisados, possuindo um certificado seguindo as melhores práticas.

No relatório podemos identificar de imediato que o relatório possui Classe A emitido pela ferramenta, analisando mais o Certificado é possível notar que a chave de Criptografia RSA 2048, onde o *hash* é o SHA 256. Conforme figura 5.

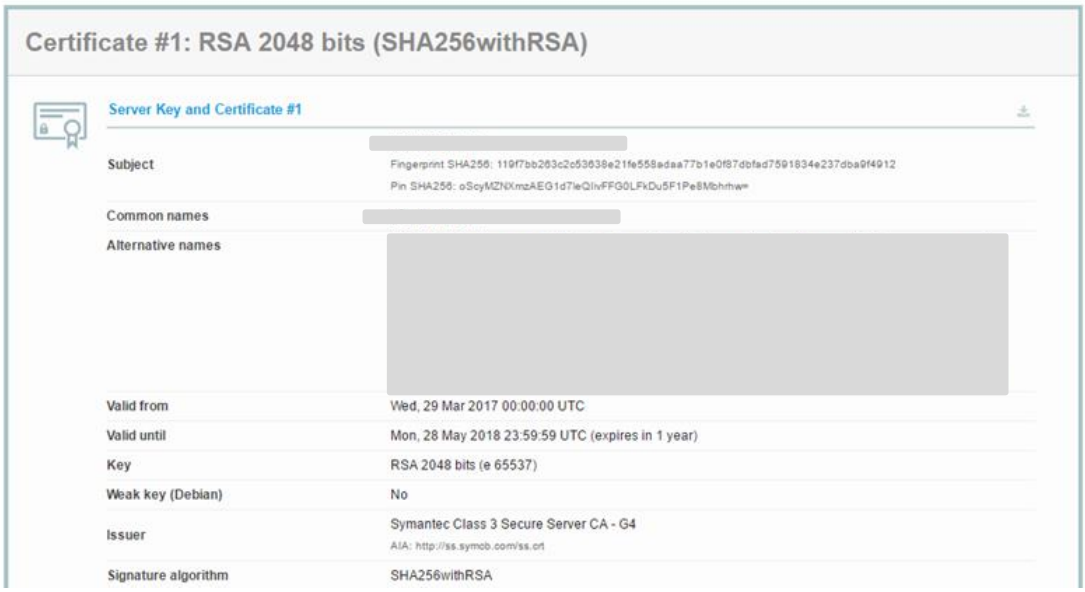
Figura 5: Relatório Empresa 1 – parte 1



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

Identificamos também que a empresa possui suas bandeiras se dentro do certificado, além das bandeiras conhecidas, possuem bandeira de redirecionamento de páginas, bandeiras de testes, bandeira de páginas de informações sensíveis, entre muitas outras. Logo abaixo na mesma página identificamos que a validade do certificado estava com a data 28 de Maio de 2018. Ainda nessa página, está o nome da empresa que gerou esse Certificado (Symantec), conforme Figura 6.

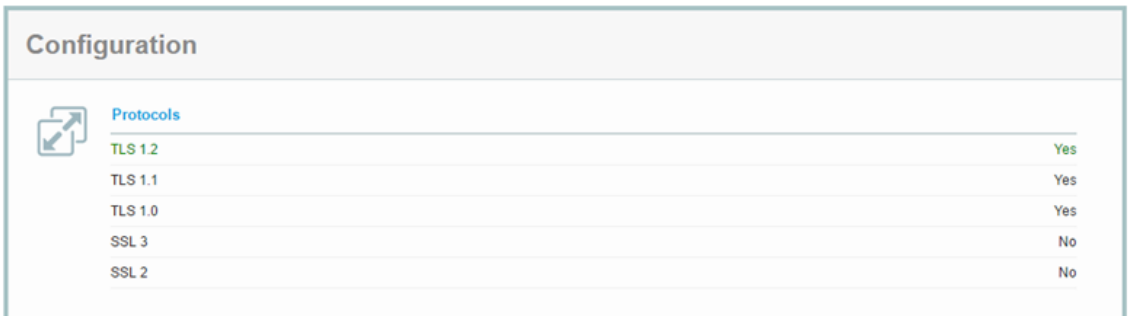
Figura 6: Relatório Empresa 1 – parte 2



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 29 de Maio de 2017

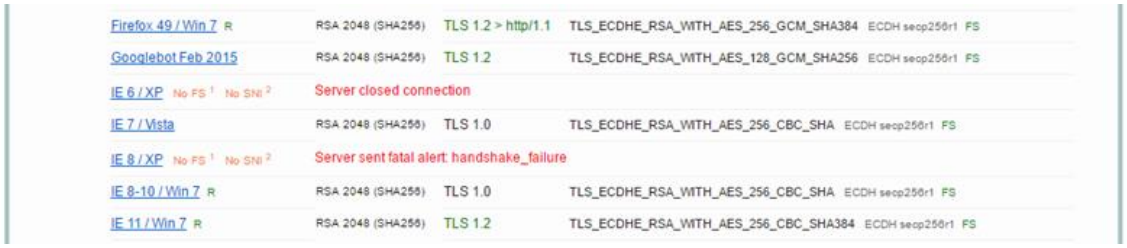
No relatório é possível validar que a Empresa 1, não utiliza mais SSLv2 e SSLv3, considerados inseguros, apenas TLS em todas suas versões, onde cada tipo de comunicação com aplicações Web trabalha com um TLS diferente (Figura 7). Interessante ressaltar que o TLS não faz mais conexão segura com maquinas que utilizam o Windows XP, que foi descontinuado em 8 de Abril de 2014 (figura 8).

Figura 7: Relatório Empresa 1 – parte 3



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 29 de Maio de 2017

Figura 8: Relatório Empresa 1 – parte 4



Firefox 49 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 6 / XP No FS 1 No SNI 2	Server closed connection		
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 8 / XP No FS 1 No SNI 2	Server sent fatal alert: handshake_failure		
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS

Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 29 de Maio de 2017

Nesta análise conseguimos identificar que a ferramenta simulou alguns testes utilizando vulnerabilidades mais conhecidas para validar se os patches de correção foram aplicados, conseguimos identificar, pois os nomes das vulnerabilidades estão inseridos no relatório tendo o resultado *no* (não), (*Beast Attack, Poodle, Heartbleed, CVE*, entre outros). (Figura 9)

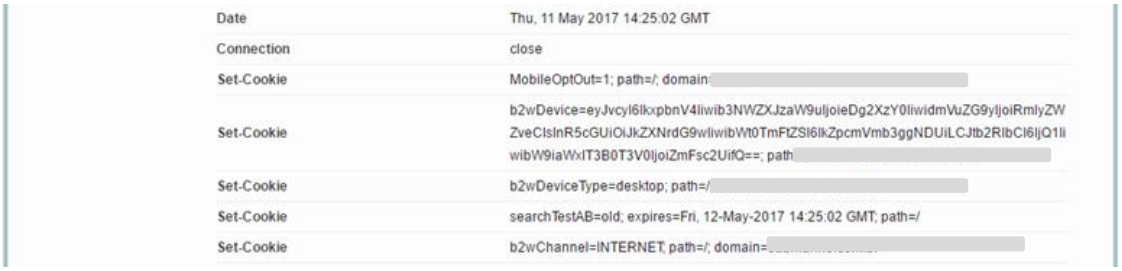
Figura 9: Relatório Empresa 1 – parte 5

BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)

Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 29 de Maio de 2017

E por último, foi validado que toda a conexão do site é fechada indicado na Figura 10, onde também possui a informação dos *Cookies* utilizados nos sites, inclusive os *Cookies* de aplicativos de dispositivos móveis.

Figura 10: Relatório Empresa 1 – parte 6

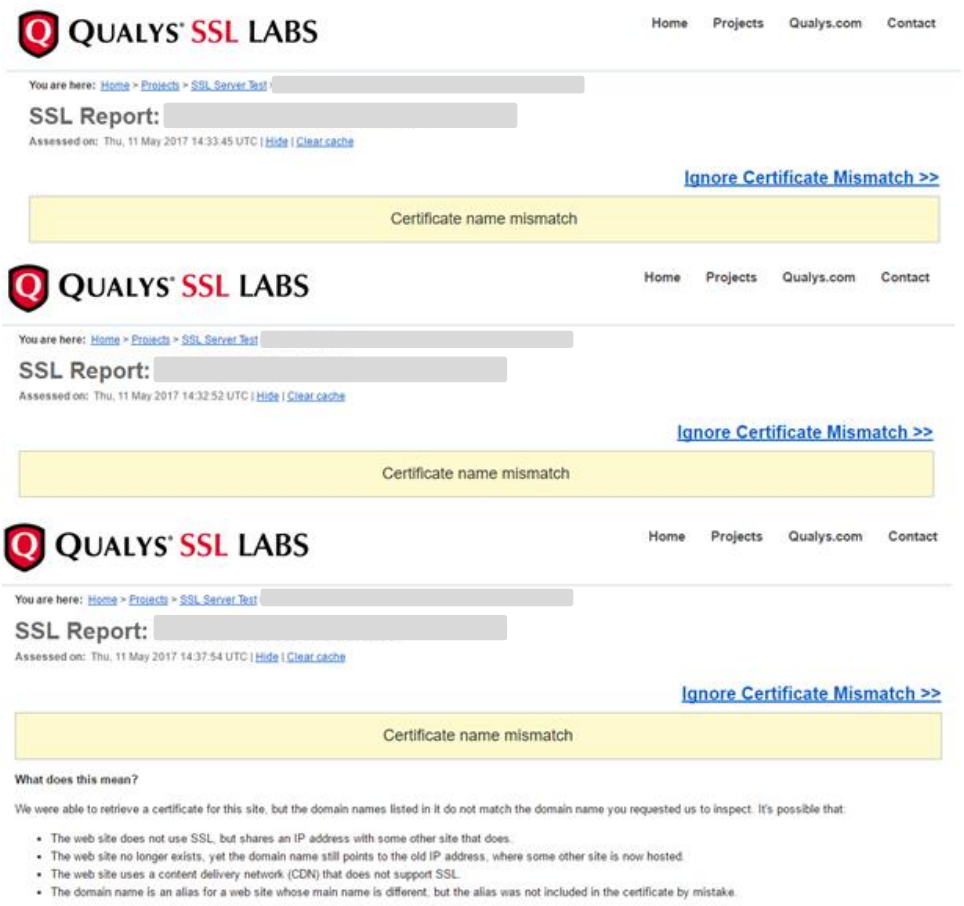


Date	Thu, 11 May 2017 14:25:02 GMT
Connection	close
Set-Cookie	MobileOptOut=1; path=/; domain=
Set-Cookie	b2wDevice=eyJvcyI6IkxpbnV4IiwibSNWZXJzaW9uIjoieDg2XzY0IiwidmVuZG9yIjoiRmlyZWZveCIsInR5cGUiOiJkZXNrdG9wIiwibWt0TmFtZSI6IkZpcmVmb3ggNDUiLCJtb2RlbCI6IjQ1IiwibW9iaWxlT3B0T3V0IjoiZmFsc2UifQ==; path
Set-Cookie	b2wDeviceType=desktop; path=/
Set-Cookie	searchTestAB=old; expires=Fri, 12-May-2017 14:25:02 GMT; path=/
Set-Cookie	b2wChannel=INTERNET; path=/; domain=

Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

A Empresa 2 que corresponde Bandeira 2, teve aderência de apenas 45,45% dos itens aderentes. Logo no processo de geração de relatório, validamos que a empresa na qual foi escolhido para representar a bandeira não possuía um Certificado considerado válido (Figura 11). Dessa forma foram validadas todas as bandeiras da empresa, mas todas possuíam Certificados inválidos. Por esse motivo foi mantido a Bandeira 2.

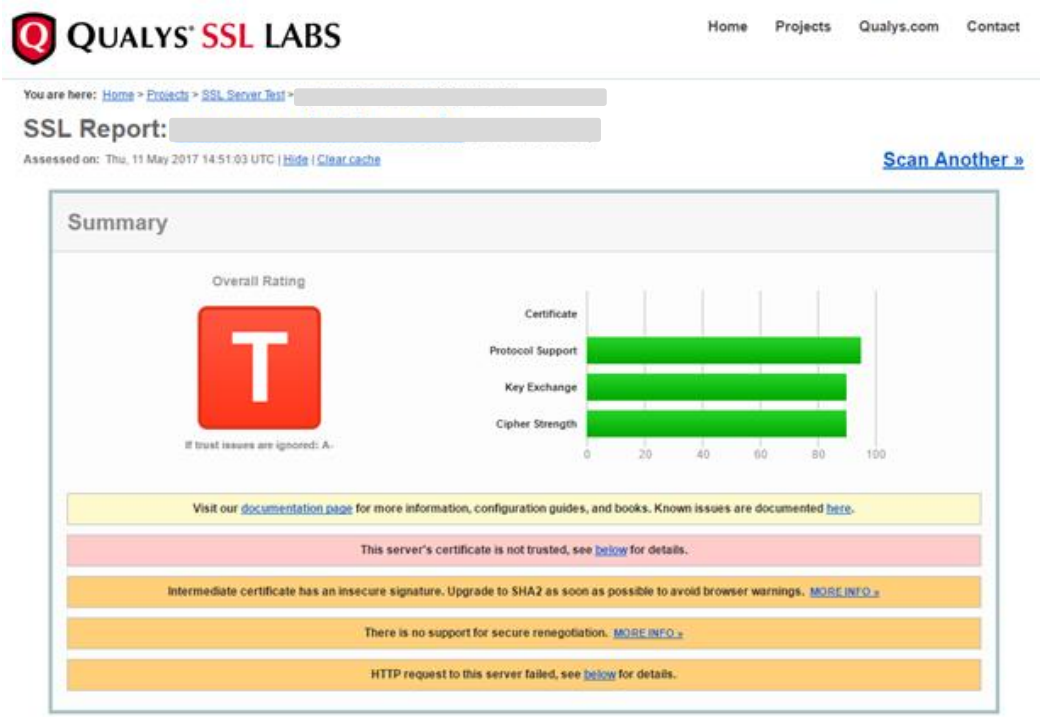
Figura 11: Relatório Empresa 2 – parte 1



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

Diferentemente do primeiro relatório gerado, correspondente a Empresa 1, o relatório gerado gerou um ranking “T” informando que o Certificado não era verdadeiro (assinado pela empresa a248.e.akamai.net), conforme Figura 12.

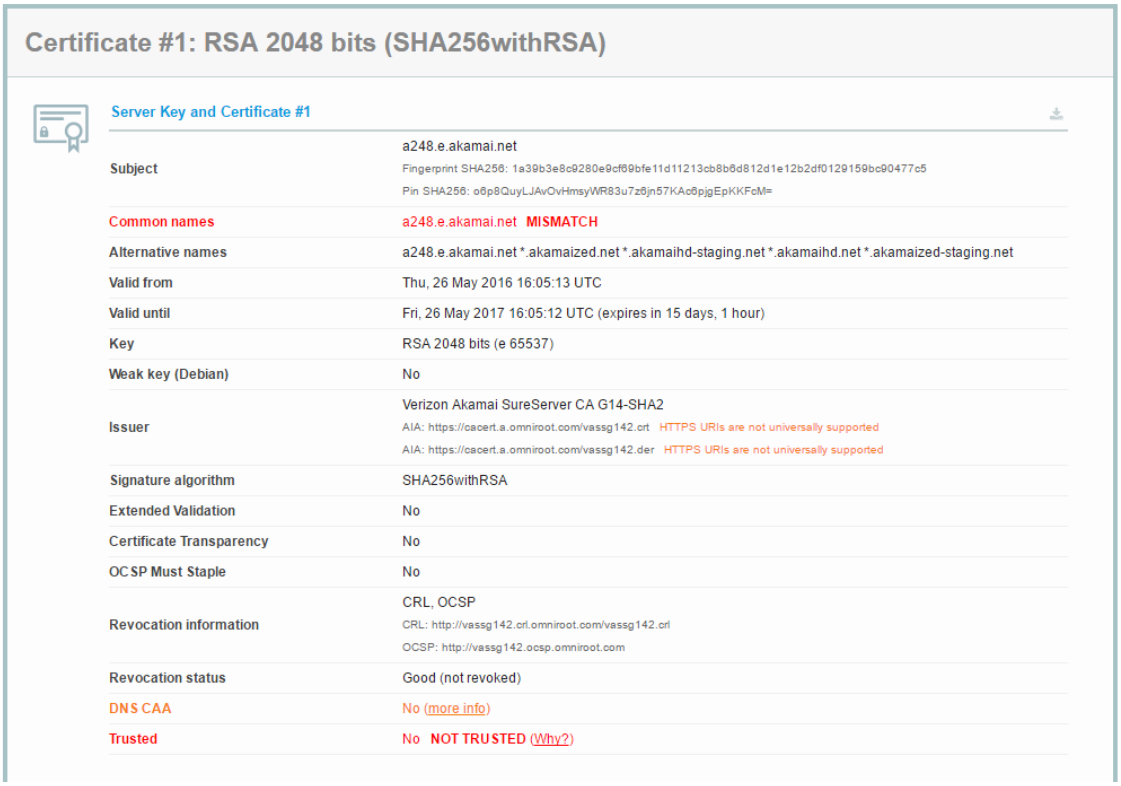
Figura 12: Relatório Empresa 2 – parte 2



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

Nota-se que o Certificado utiliza chave RSA2048 com *hash* SHA256 e também ECDSA utilizando o mesmo *hash* SHA256, configurações citadas no artigo da empresa SSL (2015) como seguras, porem a ferramenta não considera o certificado válido, indicando desconhecimento do emissor do Certificado, nota-se também que o mesmo tinha apenas 15 dias de validade e não encontramos nenhuma empresa do grupo nos "*Alternative Names*", conforme Figura 13.

Figura 13: Relatório Empresa 2 – parte 3



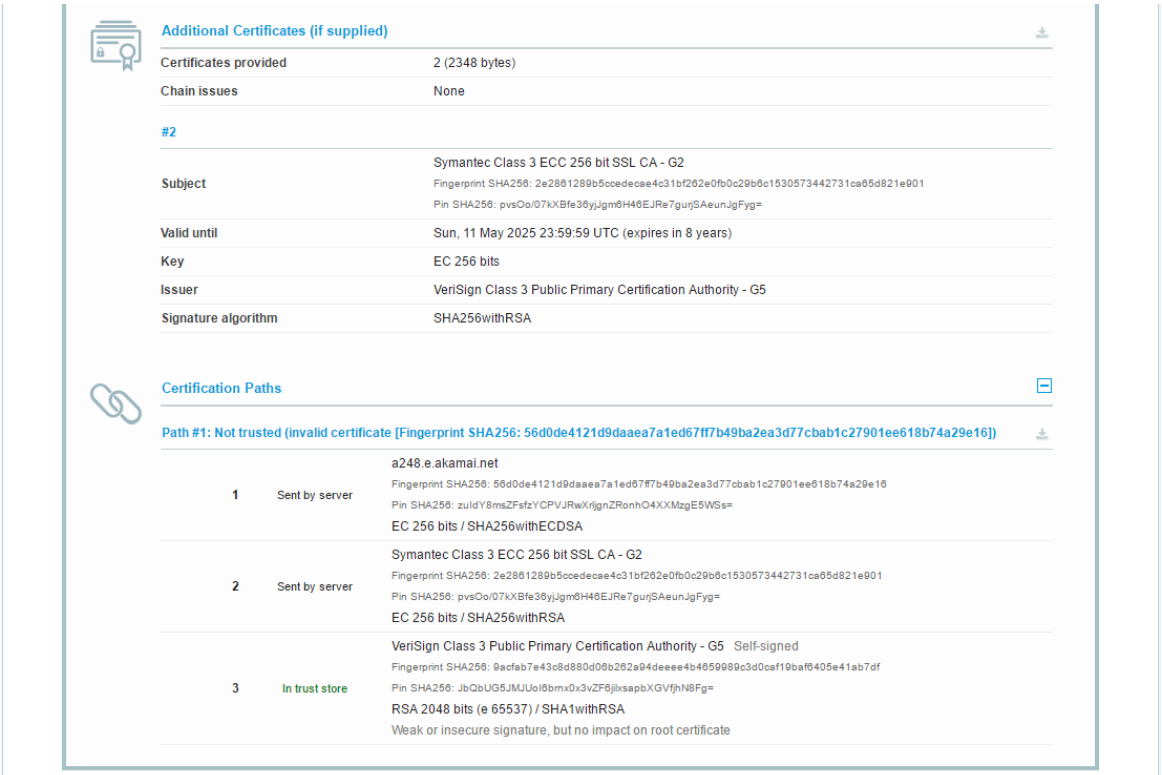
Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 26 de Maio de 2017

A empresa possui um Certificado ECDSA um Certificado adicional com prazo de validade de oito anos, emitido pela mesma empresa Symantec, a mesma que assina o Certificado da Empresa 1, e logo abaixo no "*Certication Paths*" que a empresa que assina o certificado (a248.e.akamai.net), subscreve a assinatura da empresa Symantec (Figura 14).

Na configuração do Certificado, notamos que a Empresa 2 também utiliza os protocolos TLS para fechar a comunicação, possuindo os principais patches para mitigar vulnerabilidades. (Figura 15).

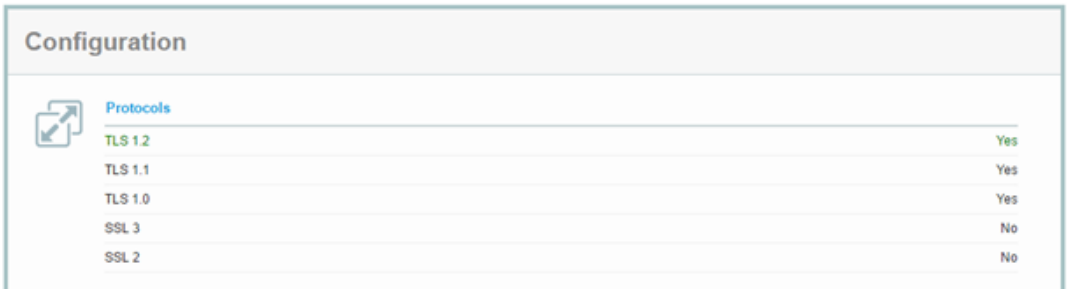
Não foi possível validar nenhum aspecto de segurança em HTTP, pois o relatório teve falha em sua requisição. Esse mesmo erro foi apresentado em todos os relatórios da Empresa 2. (figura 16).

Figura 14: Relatório Empresa 2 – parte 4



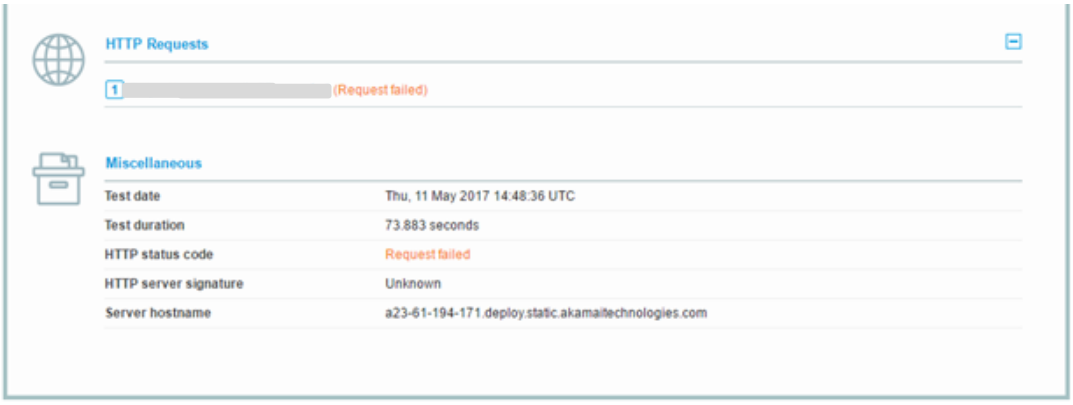
Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

Figura 15: Relatório Empresa 2 – parte 5



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

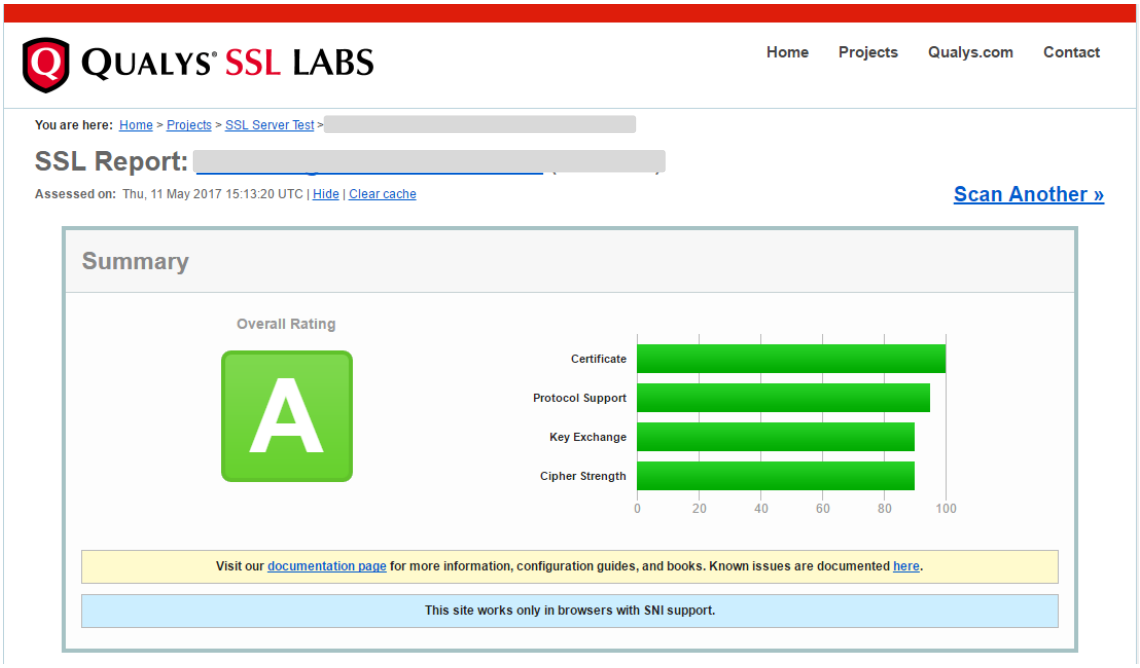
Figura 16: Relatório Empresa 2 – parte 6



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

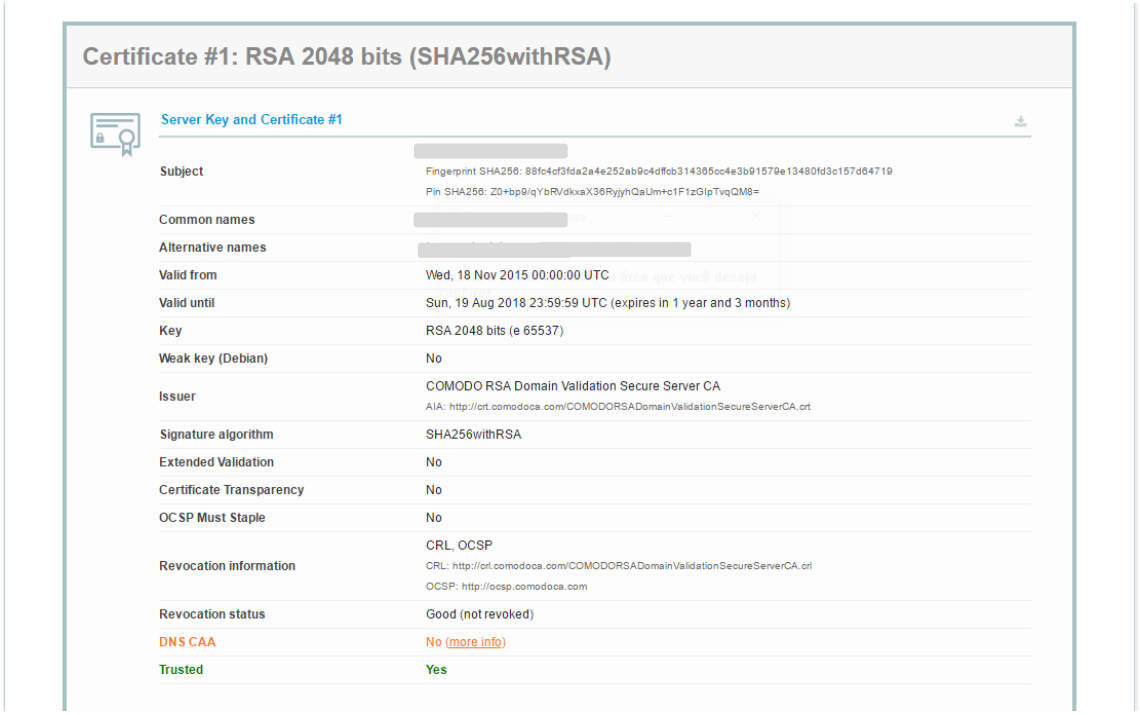
A Empresa 3 que possui a Bandeira 3, atingiram 8 dos 11 itens validados. O Certificado Digital foi classificado como ranking “A” na ferramenta (Figura 17), possui chave RSA de 2048 bits com um *hash* SHA256, similar às demais empresas, nota-se que as bandeiras compostas no Certificado, são apenas duas, sendo a única diferença o ”.” (ponto), no início da URL, isso indica que a empresa pode utilizar indicações dentro das URLs (Ex.: compras.bandeira3.com.br; faturamento.bandeira3.com.br). Esse tipo de utilização, se não for bem configurado, pode se tornar uma ameaça para a empresa, sendo a melhor prática, especificar as bandeiras dentro do Certificado. Identificamos também que o Certificado foi adquirido em 2015 com validade de 3 anos, e também a empresa que assinou esse Certificado (COMODO RSA), e a indicação que o Certificado é indicado como Verdadeiro. O Certificado ainda possui assinaturas de Certificados que responde à mesma bandeira, conforme Figura 18.

Figura 17: Relatório Empresa 3 – parte 1



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

Figura 18: Relatório Empresa 3 – parte 2



Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

Em suas configurações identificamos que a Empresa 3 utiliza somente TLS, tendo a maioria de suas conexões com TLS 1.2, sendo o mais seguro dos TLS.

Ainda nas configurações é possível identificar que existe a existência de patches. Analisando a Segurança do HTTP indica que a conexão é fechada, mas não existe indicação se cookies são armazenados com segurança. Os desvios encontrados por nessa analise pode impactar a segurança do usuário na compra, pois algumas sessões não garantem a integridade e a irrefutabilidade do site. (Figura 19).

Figura 19: Relatório Empresa 3 – parte 3

Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

A Empresa 4, assim como a Empresa 1, teve 100% de aderência aos itens validados, tendo seu certificado uma chave RSA 2048 utilizando um hash RSA de 256, todos seus domínios estão configurados dentro do Certificado. A empresa que assinou o Certificado Digital é reconhecida pela Autoridade Certificadora.

Em suas configurações, o Certificado trabalha apenas com TLS e nos testes efetuado pela ferramenta é possível identificar que o mesmo possui patches instalados. E para finalizar o protocolo HTTP utilizado possui armazenamento seguro de Cookie, e criptografia em toda comunicação após a troca de Certificados. Todas as configurações informadas fazem parte do artigo de melhores práticas para criação de um Certificado SSL.

O Certificado da Empresa 5 atingiu atendeu 10 itens validados, sendo classificado como Certificado ranking “A”, onde o Certificado possui todas as características do Certificado da Empresa 1 e 4, onde a única diferença na configuração do Certificado se dá por conta dos cookies utilizados pelos sites, que não possuem segurança de armazenamento de informações para próximos acessos, podendo ser explorada por algum atacante em busca de informações (Figura 20).

Figura 20: Relatório Empresa 5 – parte 1

Fonte: Extraído de: https://www.ssllabs.com/ssltest/ em 11 de Maio de 2017

6 CONSIDERAÇÕES FINAIS

Nesse trabalho foi possível identificar que a Segurança da Informação está presente nos sites de vendas pela internet, e nas análises do Certificado SSL fica ainda mais claro existe essa atenção. Importante evidenciar que apenas um relatório gerado ficou abaixo de 50% de aderência aos itens validados, sendo que dois dos cinco relatórios analisados tiveram aderência total aos itens.

Um ponto que chamou muita atenção na análise foi o ranking da ferramenta, que 4 dos 5 relatórios possuem ranking “A”, porem conforme foi identificado, nem todos os itens que foram validados estavam em todos os Certificados, tendo relatório nesse ranking com 20% de desvios.

Se tratando de sites *e-commerce*, é indispensável informar que os maiores receios nas compras são sobre a confiança que o site transmite ao usuário, e já se percebe que a empresas estão trabalhando nesse critério, pois dentro do Certificado, onde se nota dentro dos relatórios gerados informam que as empresas aplicam patches para reduzir vulnerabilidades, após a troca de chaves só efetua conexões fechadas, utilizam meios seguros de criptografia.

Também é importante ressaltar que todos os sites possuem um Certificado SSL, e por mais que o relatório da Empresa 2 não é considerado válido pela ferramenta, ainda sim foi possível identificar que o seu Certificado possuí configurações de Segurança, desde a escolha da Criptografia a ser utilizada até as configurações do TLS e seus Patches.

Sendo assim podemos concluir a maior parte das empresas de *e-commerce* estão trabalhando na segurança de seus sites, criando formas de deixar os mesmos mais seguros, com um Certificado bem estruturado e aplicado, que por mais que essas ações que aos olhos dos usuários passam despercebidos são justamente as maiores provas de segurança e confiança que os sites estão preparados para receber suas informações pessoais e bancarias para efetuar as compras.

Como as melhores práticas para utilização de SSL elaborado nesse trabalho pode ser utilizado para qualquer site que faz uso do mesmo, compreende-se que o estudo efetuado pode ser expandido para outras empresas, ou mesmo para outros nichos de mercados, como sites de bancos, sites de redes sociais, sites de e-mail,

não se restringindo apenas em sites de comércio eletrônico, validando de maneira mais abrangente se todas as empresas que faz uso desse Certificado seguem as melhores práticas estabelecidas.

REFERÊNCIAS

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005. 120 p.

ASCENSÃO, CARLOS. **O que é e-Commerce?**. Disponível em: < http://www.gestordeconteudos.com/tabid/3850/>. Acesso em: 08 Maio 2017.

BARROS, M.A. **Uso de SSL em Sites.** 2015. 21 p. Dissertação (Trabalho de Pós Graduação) – Universidade Estadual de Maringá Centro de Tecnologia Departamento de Informática, Maringá, 2005.

CRUZ, A. **Segurança no e-commerce** e os selos de segurança. 2014. Disponível em: < https://www.ecommercebrasil.com.br/artigos/seguranca-e-commerce-e-os-selos-de-seguranca//>. Acesso em: 08 maio 2017.

FELIPINI, A. **Segurança na Internet**. 2015. Disponível em: < https://www.e-commerce.org.br/seguranca-na-internet/>. Acesso em: 08 maio 2017.

MARCEL, L. **TLS vs SSL**: Qual é a diferença?. 2015. Disponível em: <https://lenonmarcel.com.br/2015/04/07/ssl-vs-tls.html>. Acesso em: 10 maio 2017.

KOHL, L. RAMON. **TLS ou SSL**: Qual é a diferença?. 2016. Disponível em: <https://www.ssl.net.br/blog/ssl-ou-tls//>. Acesso em: 10 maio 2017.

MERKOW, M. S.; BREITHAUPT, J. **Information Security**: Principles and Practices. 2. ed. USA: Person, 2014

MONTEIRO, E. MIGNONI, M. **Certificados Digitais**: Conceitos e Práticas. Rio de Janeiro: Brasport, Brasil. 2007. p. 5-33. 2004.

NAKAMURA, A. M**. Comércio Eletrônico**: Riscos nas Compras pela Intenet. 56 p. Dissertação (Monografia) – Faculdade de Tecnologia de São Paulo, São Paulo 2011.

PRADO, E. SOUZA, C. **Fundamentos de Sistemas de Informação**. Rio de Janeiro: Elsevier. Brasil. 2014. p.93-107.

SÊMOLA, M. **Gestão da Segurança da Informação**: uma visão executiva. Rio de Janeiro: Campus. 2003. p. 43-54;

Significados. **Significado de E-commerce**: O que é E-commerce. Disponível em: <https://www.significados.com.br/e-commerce/>. Acesso em: 05 Maio 2017.

SSL Corp. **SSL Best Practices**: a Quick and Dirty Guide. 2015. Disponível em: <https://www.ssl.com/guide/ssl-best-practices-a-quick-and-dirty-guide//>. Acesso em: 09 Maio 2017.