Universidade Europeia

LAUREATE INTERNATIONAL UNIVERSITIES

A Segurança das Comunicações dos Sítios Web Disponibilizados pelo Estado Português

André Nuno Miguel Pereira da Silva

Dissertação para obtenção do grau de
Mestre em Sistemas de Informação para a Gestão

Orientador: Prof. Doutor Manuel Menezes de Sequeira

Lisboa, 28 de agosto de 2015

Agradecimentos

A dissertação que agora se apresenta não poderia ter existido sem o apoio das pessoas que, de uma maneira ou de outra, contribuíram para este estudo. Foram estas pessoas que tornaram este trabalho possível e por esse motivo expresso a todos a minha profunda gratidão.

Ao Prof. Doutor Manuel Menezes de Sequeira por me ter orientado e por, apesar das dificuldades inerentes a esta investigação, sempre me ter ajudado a procurar e a encontrar as melhores soluções. Estou-lhe grato, também, pelos elevados conhecimentos e saber que me transmitiu, pelas suas opiniões e críticas, pela sua disponibilidade, confiança que depositou em mim, pelas várias, pelas revisões que efetuou, pela sua colaboração em todo o projeto e pela exigência que em muito contribuiu para um melhor produto final.

A todos os autores e investigadores que trabalham nas áreas referidas neste estudo. Sem eles, este projeto não teria existido. Em particular, a Ivan Ristić, pelo seu enorme contributo na área, pelas ferramentas que criou, pelos artigos e livros que escreveu. Por, apesar de todos os projetos em que está envolvido, ter utilizado um pouco do seu precioso tempo para responder aos meus contactos e por ter autorizado a utilização da ferramenta usada nesta investigação.

A todas as organizações que responderam aos contactos, em particular à organização que permitiu a realização dos testes e ao seu diretor da área das tecnologias de informação pela autorização.

Ao Dr. Paulo Marinho Pereira, pela revisão efetuada.

Aos meus colegas do mestrado, pela partilha de experiências.

Aos meus colegas do trabalho, pelo interesse e paciência demonstrada.

À minha irmã, pelo seu constante apoio, pelos contactos efetuados e pela revisão.

Aos meus pais, por nunca terem desistido de me convencer a tirar o mestrado e por todo o apoio dado e pela sua compreensão nos momentos mais difíceis.

Por último, um agradecimento especial à minha mulher por (depois de muitos esforços) me ter convencido a inscrever no mestrado. Por toda a paciência que teve ao longo deste último ano. Por, apesar de não ser da área das tecnologias de informação, ter feito um enorme esforço por compreender os conceitos, de alguma complexidade, referidos ao longo do documento. Pelo seu espírito crítico e pelas várias revisões do documento que efetuou ao longo do projeto. Por estar sempre disponível para me apoiar incondicionalmente. A ela dedico este trabalho.

Obrigado a todos!

Índice Geral

Índice dos Quadros

Índice dos Gráficos

Lista de Abreviaturas

Resumo

O Estado português disponibiliza aos cidadãos e às organizações um conjunto vasto de sítios Web que lhes permite consultar informação e realizar serviços à distância. Dada a natureza dos dados transmitidos, muitas vezes de carácter sensível, confidencial ou ambos, é importante que as comunicações efetuadas entre os cidadãos ou organizações e o Estado português sejam realizadas de forma segura.

Este trabalho estuda a segurança das comunicações efetuadas entre os sítios Web disponibilizados pelo Estado português e os cidadãos ou organizações que os utilizam.

Decisores e gestores de projetos na área das tecnologias da informação e comunicação devem ter em consideração a componente da segurança de comunicações na abordagem de projetos de governo eletrónico. Cidadãos e organizações têm também interesse em saber se as suas atividades e os seus dados, que são transmitidos nas interações efetuadas com estes sítios Web, são devidamente protegidos.

Através do uso de uma ferramenta automatizada e da adaptação de um sistema de classificação utilizado a nível global, este estudo verifica o cumprimento das mais recentes recomendações de segurança de comunicações publicadas por organizações nacionais e internacionais. Conclui que apesar de se verificar algum esforço em tornar as comunicações seguras, muito há ainda a fazer para que estas sejam efetuadas de forma efetivamente segura.

Por fim, este estudo efetua recomendações que, a serem seguidas, permitiriam garantir que as comunicações nesses sítios Web do Estado fossem efetuadas de forma segura.

Palavras-chave

Governo eletrónico; Tecnologias da informação e comunicação; Proteção de dados; Internet; Web; Segurança de comunicações.

Abstract

The Portuguese state provides citizens and organizations a wide range of websites that allows them to find information and perform services at distance. Given the nature of the data transmitted, often sensitive, confidential, or both, it's important that communications made between citizens or organizations and the Portuguese state are carried out with security.

This paper studies the security of communications between the websites, made available by the Portuguese State, and citizens or organizations that use them.

Decision makers and project managers in the information and communication technologies field should take into account the security component in electronic government projects. Citizens and organizations are also interested in whether their activities and their data, which are transmitted in the interactions made with these sites, are properly protected.

Through the use of an automated tool and the adaptation of a classification system used globally, this study verifies the compliance with the latest communication security recommendations published by national and international organizations. It arrives to the conclusion that despite the existence of some effort into making the communications work in a secure way, a lot still has to be done for these to be made in a real secure way.

Finally, this study makes recommendations which, if followed, would ensure that communications in public websites were carried out in a secure way.

Keywords

e-Government; Information and communication technologies; Data protection; Internet; Web; Communications security.

I. Introdução

Atualmente, cidadãos e organizações (empresas, organizações não governamentais, associações, entre outras) têm a possibilidade de realizar à distância, por via eletrónica, ações que anteriormente apenas se podiam efetuar presencialmente. A simplificação e a agilidade na relação entre o Estado e os cidadãos e organizações são alguns dos benefícios do governo eletrónico.

Através de plataformas de governo eletrónico o Estado português informa e presta serviços à distância a cidadãos e a organizações. Nesse âmbito, foram criados vários sítios Web que permitem que estes se relacionem com o Estado português através da Internet. Estes sítios, durante a interação, transmitem dados contendo informação sobre a atividade dos cidadãos ou organizações, a qual frequentemente é de carácter sensível, confidencial ou ambos. Disponibilizados na Internet, estes sítios podem ser acedidos pelos seus destinatários em diferentes locais, tais como: em casa, no trabalho, em locais públicos (através de *hot spots*, nomeadamente cafés, restaurantes, hotéis e aeroportos) ou na rua (através de redes móveis). As consultas podem ainda ser realizadas em diferentes dispositivos, designadamente computadores, *tablets* e telefones inteligentes. Considerando a natureza dos dados transmitidos, é importante que as comunicações efetuadas entre os cidadãos ou organizações e o Estado português sejam realizadas de forma segura.

Nos últimos anos foram identificadas diversas vulnerabilidades de segurança, consideradas graves ou muito graves, nos protocolos, nas cifras e nas aplicações que implementam a segurança ao nível das comunicações nos sítios Web. Portanto, os sítios Web que não forem atualizados e devidamente configurados ficam vulneráveis a ataques que se aproveitam dessas falhas. Ao que acresce o facto de o poder computacional todos os anos aumentar, tornando assim menos seguras, ou mesmo inseguras, algumas cifras que antes eram consideradas seguras. Qualquer uma destas situações pode comprometer a segurança dos dados dos cidadãos ou das organizações.

No contexto da privacidade da atividade dos cidadãos na Internet, é também relevante o «caso Snowden» («Edward Snowden», 2015), que levantou questões sobre a vigilância da atividade dos cidadãos na Internet por parte de organizações governamentais estrangeiras.

O presente estudo, tendo em consideração as mais recentes recomendações de segurança de comunicações, verifica se os sítios Web disponibilizados na Internet pelo Estado português estão configurados de forma proteger os dados, quer pessoais, quer da atividade em linha, dos cidadãos e das organizações.

Os resultados deste estudo têm relevância para os cidadãos e organizações, pois a ambos importa saber se o Estado português, no âmbito das comunicações realizadas nos serviços disponibilizados via governo eletrónico (que podem até ser de carácter obrigatório), protege devidamente os seus dados. Sendo a segurança das comunicações um aspeto relevante a considerar no planeamento e implementação de projetos no âmbito do governo eletrónico e na manutenção dos sistemas daí resultantes, os resultados desta investigação são também importantes para os decisores e gestores desses projetos.

O presente documento encontra-se subdividido em seis capítulos, sendo o primeiro, esta introdução. No segundo capítulo é realizada uma investigação sobre os temas em análise e às recomendações de segurança de comunicações das principais organizações nacionais e internacionais. No terceiro capítulo é descrita a metodologia utilizada para avaliar as comunicações seguras dos sítios Web. No quarto capítulo são expostos, de forma sucinta, os resultados dos testes efetuados. O quinto capítulo analisa os resultados e formula recomendações. No sexto e último capítulo são apresentadas as conclusões do estudo, indicadas as limitações do mesmo e identificadas as perspetivas de trabalho futuro a realizar neste domínio.

II. Estado da Arte

1. Governo Eletrónico

1.1. Conceito de governo eletrónico.

O governo eletrónico pode ser definido pela «entrega eletrónica de informação e serviços governamentais, 24 horas por dia, 7 dias por semana» (Holden, Norris, & Fletcher, 2003). Jeong (2007) define o conceito de governo eletrónico como a «utilização de Tecnologias da Informação (TI), Tecnologias da Informação e Comunicação (TIC) e outras tecnologias de telecomunicação baseadas na Web para melhorar e/ou aumentar a eficiência e a eficácia de disponibilização de serviços pelo sector público». Jeong (2007) define ainda que existem vários componentes de governo eletrónico:

- Entre organismos do Estado (G2G, do inglês *Government to Government*).
- Entre o Estado e os cidadãos (G2C, do inglês *Government to Citizens*).
- Entre o Estado e os seus funcionários (G2E, do inglês *Government to Employees*).
- Entre o Estado e as empresas (G2B, do inglês *Government to Business*).

As definições de governo eletrónico, apesar de diferentes entre si, reúnem aspetos comuns: são as TIC que permitem a sua existência e são também estas que incorporam os serviços informativos ou transacionais prestados a cidadãos e organizações.

Na fase inicial do governo eletrónico, vários autores analisaram a evolução da implementação do governo eletrónico numa sociedade. Coursey e Norris (2008) compilaram as análises de diversos autores quanto às etapas dessa evolução numa tabela:

Tabela 1
Etapas de evolução do governo eletrónico.

Autor	Etapa 1	Etapa 2	Etapa 3	Etapa 4	Etapa 5	Etapa 6
Layne e Lee (2001)		Catalogação	Transação	Integração vertical	Integração horizontal	
Baum e Di Maio (2000)		Presença	Interação	Transação	Transformação	
Ronaghan (2001)	Presença emergente	Presença otimizada	Interativo	Governo transacional	Uniforme	
Hiller e Bélanger (2001)		Disseminação de informação	Comunicação nos dois sentidos	Integração	Transação	Participação
Wescott (2001)	E-mail e rede interna	Disponibilização de informação	Comunicação nos dois sentidos	Troca de valor	Democracia digital	Governo conjunto

Fonte. Coursey e Norris (2008, p. 524)

Coursey e Norris (2008, p. 533) são críticos destes modelos, pois consideram que, «embora intelectualmente interessantes, estes modelos são praticamente apenas especulativos» e que «não foram baseados nem em teorias existentes nem em dados empíricos» (Coursey & Norris, 2008, p. 532). Concluem que «após uma presença inicial […] os governos adotam o governo eletrónico devagar e incrementalmente» (Coursey & Norris, 2008, p. 533).

Conforme mostra a Tabela 1, os autores divergem quanto às etapas que ocorrem aquando da implementação do governo eletrónico numa determinada sociedade. Estão, no entanto, de acordo de que existe uma evolução. Atualmente, o governo eletrónico faz parte da vida dos cidadãos e das organizações e, de acordo com a perspetiva evolutiva do governo eletrónico, a sua importância será cada vez maior no futuro.

1.2. O governo eletrónico em Portugal.

O *e-government development index* (EDGI) da Organização das Nações Unidas (ONU) (2015) indica que, numa avaliação de 191 países, Portugal se encontra na 37.ª posição[1]. A evolução de Portugal entre 2004 e 2014 neste índice é refletida na tabela seguinte:

Tabela 2
Evolução da posição de Portugal no EDGI.

Posição	**2004**	**2005**	**2008**	**2010**	**2012**	**2014**
Portugal	31.ª	30.ª	31.ª	39.ª	33.ª	37.ª

Fonte. ONU (2015)

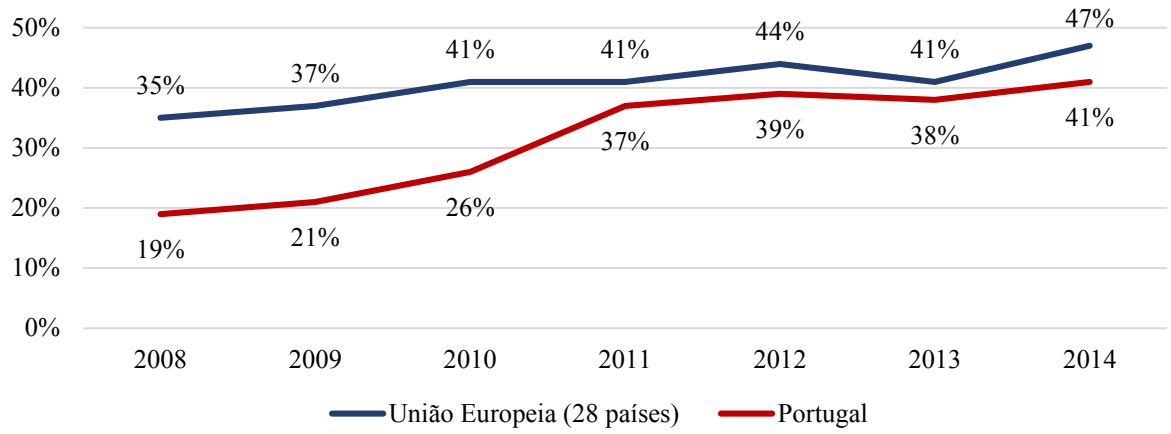
É possível observar que Portugal, de 2002 a 2014, esteve entre a 30.ª e a 39.ª posição. Conclui-se que, após um ímpeto inicial que durou até 2008, em que esteve entre a 30.ª e a 31.ª posição, a posição de Portugal na lista dos países do índice de desenvolvimento do governo eletrónico tem diminuído.

De acordo com o Eurostat (2014b), conforme representado na Figura 1, a percentagem de indivíduos em Portugal que utilizaram a Internet para recorrer a serviços disponibilizados pelo Estado em 2014 foi de 41 %, sendo que a média europeia foi de 47 %. Ainda de acordo com o Eurostat (2014a), conforme representado na Figura 2, a percentagem de empresas em Portugal que utilizaram a Internet para recorrer a serviços disponibilizados pelo Estado em 2013 foi de 92 %, sendo a média europeia de 88 %.

[1] O EDGI contabiliza os países por ordem decrescente, i.e., os melhores estão nas primeiras posições e os piores nas últimas.

Figura 1

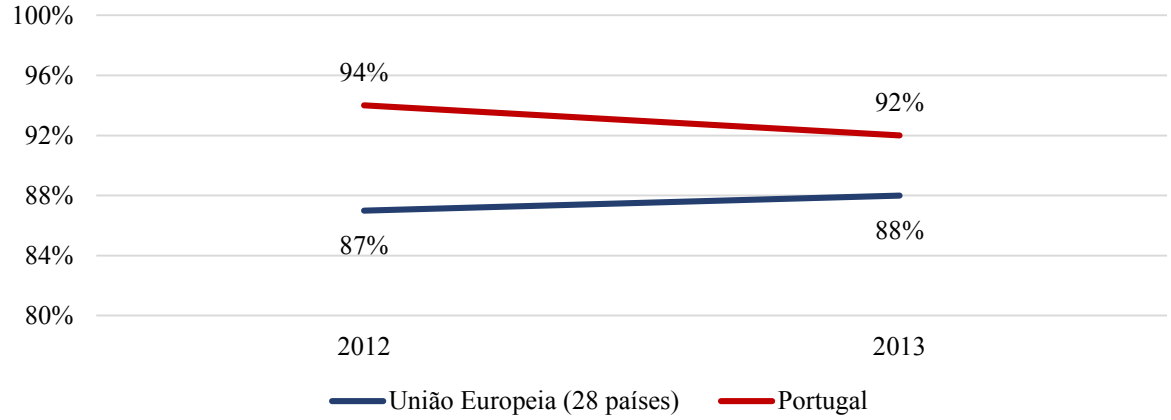
Evolução de utilização por indivíduos de serviços do Estado pela Internet.



Fonte. Eurostat (2014b)

Figura 2

Evolução de utilização por empresas de serviços do Estado pela Internet.



Fonte. Eurostat (2014a)

A nível nacional, existe uma tendência crescente da utilização de serviços públicos na Internet. Em Portugal, serviços como o Portal do Cidadão, Portal da Empresa, Mapa do Cidadão, Portal das Finanças, e-Fatura, entre muitos outros, são utilizados por milhões de cidadãos e organizações.

1.3. A importância de comunicações seguras no governo eletrónico.

Os serviços prestados no contexto do governo eletrónico são na sua maioria prestados através de sítios Web que permitem a interação entre o Estado e cidadãos ou organizações. Estes sítios Web transmitem informação através da Internet, a qual na sua forma física é composta por redes e equipamentos. As informações transmitidas pela Internet podem ser desde dados informativos até dados privados dos cidadãos ou das organizações. Ao utilizarem estes

sítios Web de governo eletrónico, os cidadãos e as organizações confiam que o Estado português protege os dados envolvidos nestas interações.

Quando se observa a evolução do governo eletrónico em Portugal e noutros países verifica-se uma tendência inequívoca para que cada vez mais informação e serviços passem a estar disponíveis na Internet. Também se percebe que é cada vez maior o número de cidadãos e organizações que os utilizam. Todos estes fatores reforçam a necessidade de as comunicações entre Estado e cidadãos e organizações serem efetuadas de forma segura. Se as comunicações não forem seguras, podem ser escutadas ou modificadas por qualquer agente que tenha acesso a um dos equipamentos de rede que compõem a Internet.

2. Comunicações Seguras na Internet

2.1. Comunicações na Internet.

Durante o início da década de 1980 foi criado um modelo de referência em camadas com o objetivo de modelar os protocolos de comunicação entre sistemas (Day & Zimmermann, 1983). Este modelo foi posteriormente formalizado e designado como modelo Open Systems Interconnection (OSI) (ISO/IEC JTC 1, 1994).

Na Internet é utilizado o Transmission Control Protocol/Internet Protocol (TCP/IP) (Braden, 1989a, 1989b), também designado por *Internet protocol suite*, que resultou do projeto Advanced Research Projects Agency Network (ARPANet) do Departamento de Defesa (DoD) dos Estados Unidos da América (EUA). O TCP/IP utiliza um modelo em camadas bastante semelhante ao modelo OSI, embora com algumas diferenças significativas. As diferenças encontram-se principalmente na camada «Aplicação» do modelo TCP/IP, que no modelo OSI se divide em três camadas, e na camada de «Interface com a rede» do modelo TCP/IP, que o modelo OSI divide em duas camadas[2]. A relação entre o modelo OSI e o modelo TCP/IP é demonstrada na Tabela 3.

Tabela 3
Correspondência entre o modelo OSI e o modelo TCP/IP.

Camadas do modelo OSI	Camadas do modelo TCP/IP	Descrição
Aplicação	Aplicação	Interface com o utilizador.
Apresentação		Representação de dados, conversão, compressão, encriptação.
Sessão		Gestão de conexões entre aplicações.

[2] Este último caso é sujeito a diferentes interpretações, sendo que alguns autores, ao manter as duas camadas inferiores do modelo OSI, transformam o modelo TCP/IP num modelo de cinco camadas (Tanenbaum, 2003).

Camadas do modelo OSI	Camadas do modelo TCP/IP	Descrição
Transporte	Transporte	Gestão da transferência eficiente de dados entre dois pontos de uma rede.
Rede	Internet	Controlo da operação da rede.
Ligação de dados	Interface com a rede	Controlo da transmissão e receção de dados entre dois nós conectados pela camada física.
Física		Transmissão física de dados sobre um meio físico.

Usando como referência o modelo OSI, no caso de um acesso a uma página Web[3]:

- utiliza-se o HyperText Transfer Protocol (HTTP) (Fielding et al., 1999) na camada de «Aplicação»,
- que é encapsulado em segmentos através do Transmission Control Protocol (TCP) na camada de «Transporte»,
- segmentos esses que são divididos em pacotes que são endereçados ao nível da rede através do Internet Protocol (IP) na camada de «Rede»,
- pacotes esses que são divididos em tramas pelos dispositivos de rede (placas de rede, placas de rede móvel, placas de rede sem fios, etc.) na camada de «Ligação de dados»,
- tramas essas, constituídas por sequências de *bits*, que são enviados sob a forma de sinais eletromagnéticos através de um determinado meio físico (cabo de cobre, fibra ótica, ondas rádio, etc.) na camada «Física».

A Tabela 4 resume o processo.

Tabela 4

Exemplo de uma conexão HTTP no modelo OSI.

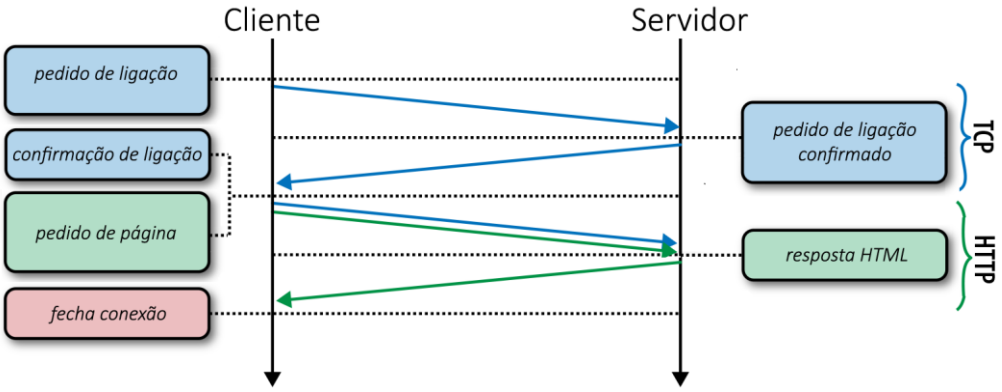
Camada do Modelo OSI	Descrição	Utilização de:
Aplicação	Acesso a página Web.	Protocolo HTTP
Apresentação	Conversão de dados.	Tipo de *MIME* text/html[4]
Sessão	Estabelecimento de ligação.	Porta 80
Transporte	Encapsulamento de segmentos.	Protocolo TCP
Rede	Endereçamento através de pacotes.	Protocolo IP
Ligação de dados	Encapsulamento em tramas.	IEEE 802.3ab[5]
Física	Envio de *bits* sob a forma de sinais eletromagnéticos.	Cabo Cat6e

A Figura 3 representa o funcionamento de um pedido HTTP (sobre o qual este estudo se irá focar) quando um utilizador acede a uma página Web com o seu navegador.

[3] Os acessos a páginas Web são realizados através de uma aplicação designada por navegador Web (*browser*).
[4] O Multi-purpose Internet Mail Extensions (MIME) é o padrão de classificação dos tipos de ficheiro utilizados na Internet.
[5] O 802.3ab é uma norma do Institute of Electrical and Electronics Engineers (IEEE).

Figura 3

Representação de uma comunicação através de HTTP na Internet.



Fonte. Adaptação de imagem obtida de Grigorik (2013, Capítulo 11)

Quando se utiliza o protocolo HTTP simples o envio dos dados é efetuado sem qualquer encriptação, podendo os dados ser intercetados por outros agentes (*hackers*, espiões, etc.) no seu percurso entre o cliente e o servidor.

Importa realçar que a comunicação entre um cliente e um servidor através da Internet não é efetuada utilizando apenas o protocolo HTTP na camada de aplicação[6]. Outro protocolo importante é o Domain Name System (DNS) (Mockapetris, 1987), cujo «principal objetivo é estabelecer um espaço de nomes consistente que irá ser utilizado para referenciar recursos» (Mockapetris, 1987, p. 2)[7]. Existem ainda outros protocolos utilizados ao nível da camada aplicacional do modelo OSI que contribuem para as comunicações na Internet. No anexo A são enumerados alguns desses protocolos.

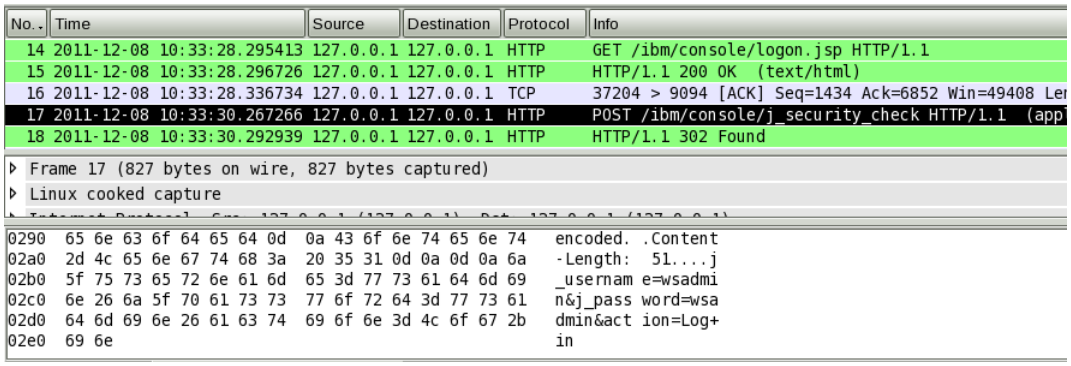
2.2. Comunicações seguras num sítio Web.

Como foi verificado no ponto anterior, as comunicações na Internet através do protocolo HTTP não são encriptadas, isto é, circulam pela rede em texto simples. A Figura 4 exemplifica como um atacante pode, através de uma aplicação de escuta de pacotes, ter acesso aos dados de um utilizador num determinado sítio Web.

[6] Designa-se por cliente o dispositivo que pede os dados e por servidor o dispositivo que fornece os dados.
[7] A resolução de nomes de domínio é o processo de converter, isto é, resolver um nome de domínio no respetivo endereço IP.

Figura 4

Representação de uma captura de pacotes de dados através da rede[8].



Fonte. Adaptação de imagem obtida de Grigorenko (2011)

Neste caso, o utilizador introduziu o nome de utilizador «wsadmin» e a palavra-passe «wsadmin» quando submeteu o formulário de autenticação no endereço «http://127.0.0.1/ibm/console/logon.jsp»[9].

Para resolver este problema foi criado o protocolo Transport Layer Security (TLS) (Dierks & Allen, 1999), que permite encriptar as comunicações através da rede. Este protocolo teve como base o protocolo Secure Sockets Layer (SSL) 3.0, desenvolvido pela Netscape Communications e, por razões históricas (Freier, Karlton, & Kocher, 2011), posteriormente publicado pela Internet Engineering Task Force (IETF)[10].

O principal objetivo do TLS é «providenciar privacidade e integridade dos dados entre duas aplicações em comunicação» (Dierks & Allen, 1999, p. 3). A privacidade da comunicação é obtida através do designado «aperto de mão» do TLS (*TLS handshake*) que «permite ao servidor e ao cliente autenticarem-se entre si e negociarem um algoritmo de encriptação e as chaves criptográficas antes do protocolo aplicacional transmitir ou receber o seu primeiro octeto de dados» (Dierks & Allen, 1999, p. 4). Este protocolo funciona ao nível da camada de apresentação do modelo OSI e, por esse motivo, permite ao cliente e ao servidor estabelecerem, previamente à transmissão dos dados da mensagem, um código seguro de comunicação para encriptar a mensagem que será transmitida através da rede. A Tabela 5 exemplifica o processo.

Tabela 5

Exemplo de uma conexão HTTP segura no modelo OSI.

Camada do Modelo OSI	**Descrição**	**Utilização de:**
Aplicação	Acesso a página Web.	Protocolo HTTP

[8] A captura foi obtida utilizando a aplicação Wireshark.

[9] Neste exemplo é utilizado o endereço de *loopback* do dispositivo, designado por *localhost* ou pelo IP 127.0.0.1, para efeitos de demonstração, i.e., não é um endereço real.

[10] A IETF é uma comunidade internacional de profissionais que define as normas para o funcionamento da Internet.

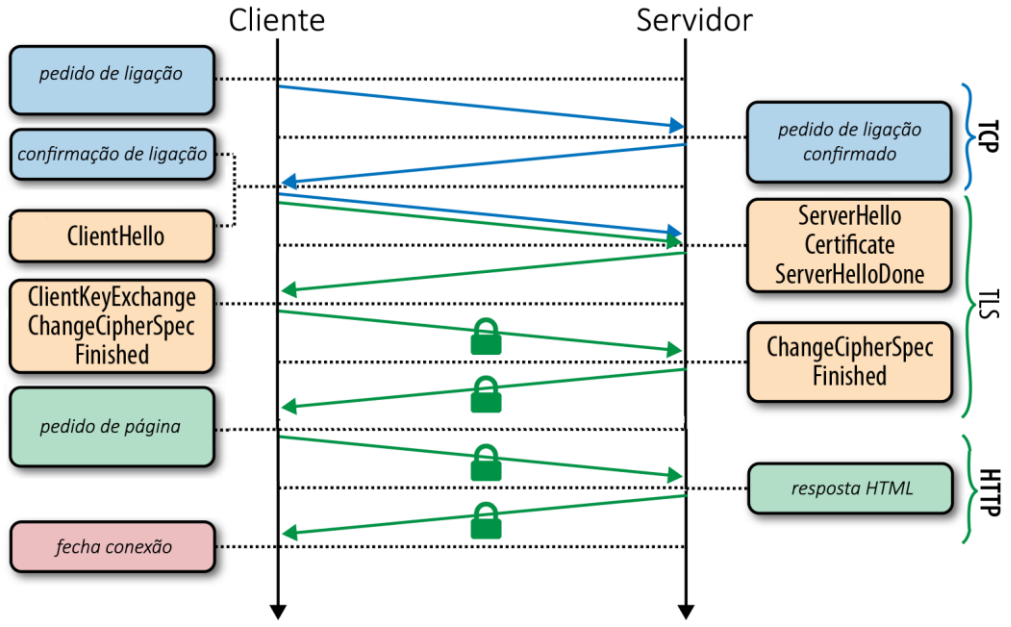
Camada do Modelo OSI	Descrição	Utilização de:
Apresentação	Conversão de dados e encriptação.	Tipo de *MIME* text/html Protocolo TLS
Sessão	Estabelecimento de ligação.	Porta 443
Transporte	Encapsulamento de segmentos.	Protocolo TCP
Rede	Endereçamento através de pacotes.	Protocolo IP
Ligação de dados	Encapsulamento em tramas.	IEEE 802.3ab
Física	Envio em *bits*.	Cabo Cat6e

A utilização de comunicações seguras ao nível das páginas da Web é conseguida através do prefixo «https» no Uniform Resource Identifier (URI) (Berners-Lee, Fielding, & Masinter, 2005), ao invés do prefixo «http», que é usado para comunicações não seguras. O prefixo «https» significa que está em utilização o protocolo HTTP com uma camada de encriptação através de SSL ou TLS, também designado por HyperText Transfer Protocol Secured (HTTPS). Também é utilizada outra porta para o efeito, a 443. As portas, por padrão, são distintas de modo a que seja possível que o mesmo servidor tenha comunicações não encriptadas, através de HTTP na porta 80, em paralelo com comunicações encriptadas, através de HTTP sobre SSL ou TLS na porta 443 (Khare & Lawrence, 2000).

A Figura 5 representa o funcionamento de um pedido HTTPS quando um utilizador acede a uma página Web encriptada com o seu navegador.

Figura 5

Representação de uma comunicação através de HTTPS na Internet[11].



Fonte. Adaptação de imagem obtida de Grigorik (2013, Capítulo 4)

[11] As designações utilizadas pelo TLS serão explicadas nos próximos capítulos.

2.3. Anatomia de uma comunicação segura num sítio Web.

Vários componentes funcionam em conjunto para estabelecer uma sessão de comunicação encriptada com um sítio Web. Todos esses componentes são acordados no «aperto de mão» do TLS. Este «aperto de mão» tem, entre outras, a função de permitir que o cliente e o servidor cheguem aos seguintes acordos: acordo de utilização de protocolo, acordo de troca de chaves e acordo de utilização de especificação de cifra.

2.3.1. Acordo de utilização de protocolo.

O acordo de utilização de protocolo consiste no envio por parte do cliente «da versão do protocolo TLS que […] pretende utilizar durante a sessão» (Dierks & Allen, 1999, p. 35). Esta informação é transmitida na primeira mensagem enviada no aperto de mão do TLS, o olá do cliente (*ClientHello*). Além dos protocolos suportados pelo cliente, é enviada mais informação sobre as suas capacidades (Dierks & Allen, 1999, p. 30). A mensagem de olá do cliente tem sempre como resposta um olá do servidor (*ServerHello*) (Dierks & Allen, 1999, p. 30).

A versão do TLS acordada deve ser «o valor mais alto suportado pelo cliente» (Dierks & Allen, 1999, p. 35), desde que o servidor o suporte. Este ponto é relevante devido ao facto de este protocolo ter tido várias evoluções para reforçar a segurança e adicionar novas funcionalidades, tendo sido já publicadas as suas versões 1.1 (Dierks & Rescorla, 2006) e 1.2 (Dierks & Rescorla, 2008), além de várias outras extensões ao protocolo. A versão 1.3 está em processo de elaboração (Rescorla, 2015a).

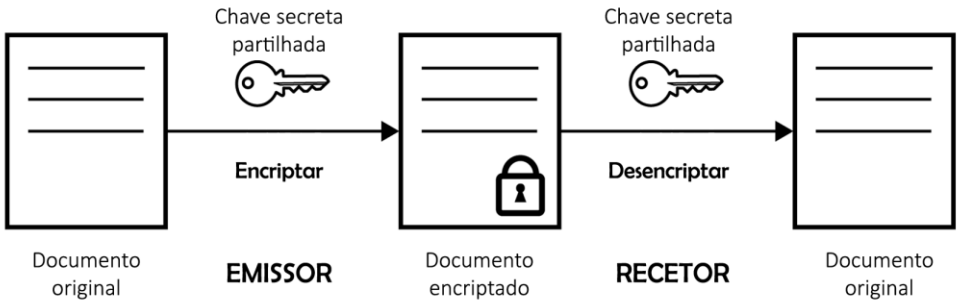
Além do TLS, outro protocolo que pode ser acordado é o SSL (Freier et al., 2011). O SSL é o percussor do TLS e está já obsoleto. A versão 1.0 do SSL nunca foi lançada pela Netscape, a versão 2.0 foi declarada insegura (Turner & Polk, 2011) e, no seguimento de recentes investigações, verificaram-se vulnerabilidades na implementação deste protocolo (Möller, Duong, & Kotowicz, 2014), pelo que a IETF descontinuou também a versão 3.0 (Barnes, Thomson, Pironti, & Langley, 2015).

2.3.2. Acordo de troca de chaves.

De acordo com o famoso criptógrafo, Auguste Kerckhoffs (1883), «um sistema criptográfico deve ser seguro mesmo que o atacante conheça todo o funcionamento do sistema, exceto a chave secreta» (Kerckhoffs, 1883). Este princípio aplica-se a dois conceitos da criptografia designados por encriptação simétrica e encriptação assimétrica.

Figura 6

Representação de uma comunicação utilizando encriptação simétrica.



Fonte. Adaptação de imagem obtida de Ristić (2014, p. 6)

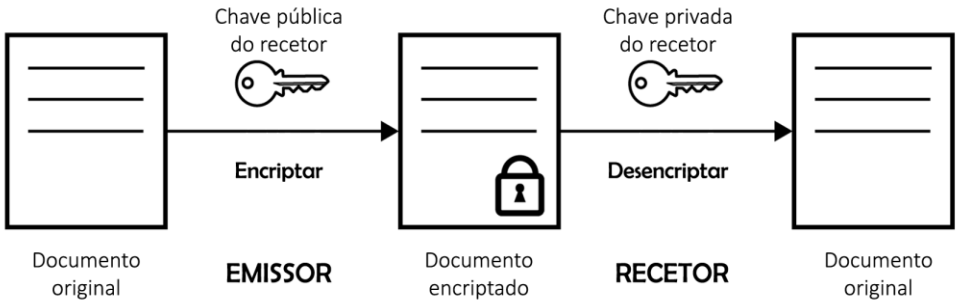
Na encriptação simétrica, representada na Figura 6, é utilizada uma chave secreta, que é acordada previamente entre emissor e recetor. Esta chave é utilizada, por ambas as partes, para encriptar e para desencriptar a mensagem. Através deste mecanismo garante-se a confidencialidade da mensagem, evitando-se que agentes externos a possam ler, pois utiliza-se a chave secreta para encriptar a mensagem e apenas quem tiver chave secreta a poderá decifrar. A chave secreta partilhada entre emissor e recetor é a «chave secreta» que Kerckhoffs refere.

Pode-se ainda utilizar a chave secreta para, através da utilização de uma função de dispersão (*hashing*), assinar a mensagem. Essa assinatura pode ser verificada utilizando a mesma chave secreta e a mesma função de dispersão, e, assim, autenticando a origem da mensagem e verificando, ao mesmo tempo, a integridade da mensagem.

No TLS a encriptação simétrica é utilizada para encriptar os dados da mensagem. No entanto, antes que isso possa acontecer, é necessário que o cliente e o servidor acordem qual a chave secreta que será utilizada. Para esse efeito, a encriptação assimétrica é utilizada.

Figura 7

Representação de uma comunicação utilizando encriptação assimétrica.



Fonte. Adaptação de imagem obtida de Ristić (2014, p. 13)

A encriptação assimétrica, representada na Figura 7, utiliza duas chaves: uma pública e uma privada. Como a própria designação o indica uma das chaves será do conhecimento público

e a outra apenas do conhecimento do detentor da chave. A chave pública do recetor é utilizada pelo emissor para encriptar a mensagem, que só pode ser desencriptada pelo recetor usando a sua chave privada. Através deste mecanismo garante-se a confidencialidade da mensagem, evitando-se que agentes externos a possam ler, pois utiliza-se a chave pública para encriptar a mensagem e apenas quem tiver acesso à chave privada a poderá desencriptar. Na encriptação assimétrica, a chave privada é a «chave secreta» referida por Kerckhoffs.

Para exemplificar uma comunicação utilizando a encriptação assimétrica recorrer-se-á a um casal muito conhecido na criptografia: a Alice e o Bob (Rivest, Shamir, & Adleman, 1978). O Bob (emissor da mensagem) envia uma mensagem encriptada à Alice (recetora da mensagem), i.e., o Bob utiliza a chave pública da Alice para encriptar a mensagem, e a Alice, por sua vez, utiliza a sua chave privada para desencriptar a mensagem do Bob.

Até agora apenas existe comunicação unidirecional, do Bob para a Alice. Para a Alice responder ao Bob de forma encriptada, tem de conhecer a chave pública do Bob. Tendo o Bob acesso à chave pública da Alice e tendo a Alice, por sua vez, acesso à chave pública do Bob, consegue-se confidencialidade nas mensagens trocadas durante uma comunicação bidirecional.

A Alice (emissora, neste último caso) pode ainda utilizar a sua chave privada para, através da utilização de uma função de dispersão (*hashing*), assinar a sua mensagem[12]. Essa assinatura pode posteriormente ser utilizada pelo Bob (recetor) para, utilizando a chave pública da Alice e a mesma função de dispersão, autenticar a Alice como a origem da mensagem e, ao mesmo tempo, verificar a integridade da mensagem.

No TLS, os principais algoritmos utilizados para geração das chaves privadas e públicas são o RSA (cujo nome deriva das iniciais dos apelidos dos seus criadores, Ron Rivest, Adi Shamir e Leonard Adleman), o Digital Signature Algorithm (DSA) e o Elliptic Curve Digital Signature Algorithm (ECDSA)[13].

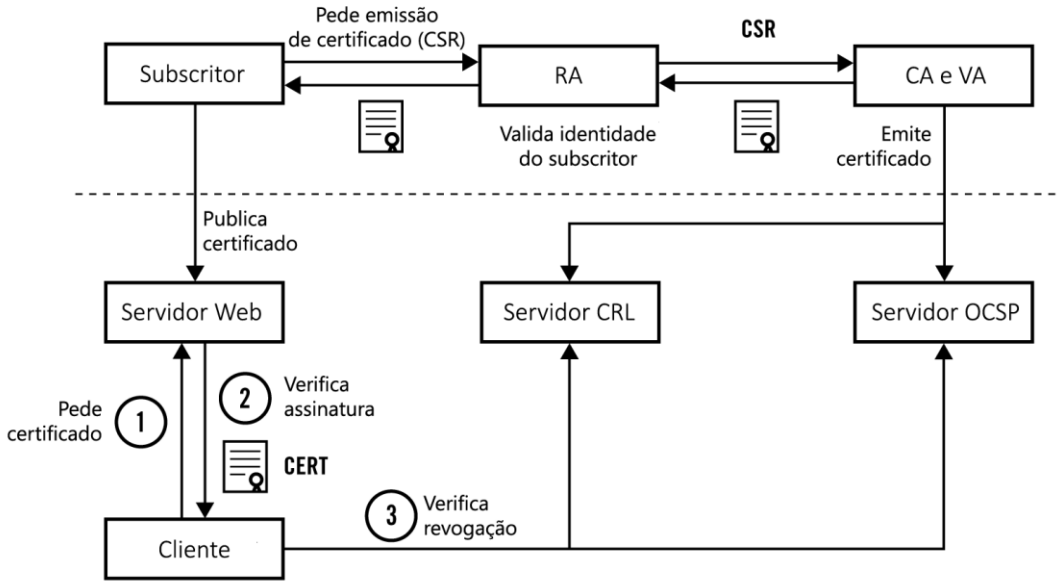
No contexto da Internet, o Bob (detentor do servidor) tem que distribuir a sua chave pública, sem possibilidade de adulteração, a todos os clientes que tentem comunicar consigo. Ao mesmo tempo, a Alice (cliente) tem que confiar que Bob é o legítimo detentor da chave pública do servidor com que está a comunicar. Para certificar que a chave pública pertence realmente a

[12] A sequência das operações pode ser assinar depois encriptar (*sign then encrypt*) que garante que quem assinou a mensagem tinha conhecimento do conteúdo. Outra sequência que é possível utilizar é o encriptar depois assinar (*encrypt then sign*), neste caso o objetivo é mostrar a todos os detentores da chave pública que a mensagem encriptada foi assinada pelo emissor. Dependendo do objetivo qualquer sequência pode ser utilizada. Uma combinações dos dois métodos também é possível.

[13] O DSA é o algoritmo utilizado nos certificados Digital Signature Standard (DSS).
Embora, como será referido nos capítulos seguintes, existem recomendações para a utilização de ECDSA, atualmente o algoritmo mais utilizado é o RSA (Durumeric, Kasten, Bailey, & Halderman, 2013).

Bob é necessário que esta seja validada por alguma entidade externa. Para servir estes propósitos, existe uma arquitetura de segurança designada infraestrutura de chaves públicas (PKI, do inglês *public key instrastructure*) da Internet.

Figura 8
Ciclo de vida dos certificados na PKI da Internet.



Fonte. Adaptação de imagem obtida de Ristić (2014, p. 64)

Utilizando a PKI da Internet (Figura 8), o Bob (subscritor e detentor do servidor) gera e envia para a autoridade de registo (RA, do inglês *registration authority*) um pedido de assinatura de certificado (CSR, do inglês *certificate signing request*) que inclui, além da chave pública, o nome de domínio e a identidade do subscritor. Esta, por sua vez, verifica o CSR, valida a identidade do Bob e, se estiver tudo correto, envia-o para a autoridade de certificação (CA, do inglês *certification authority*), que emite o certificado com uma determinada validade[14]. O certificado emitido é enviado para a RA, que o entrega a Bob. Este certificado (que é assinado digitalmente pela CA) contém a identificação do subscritor e, entre outros elementos, a chave pública do Bob[15]. A assinatura digital efetuada pela CA permite também garantir a integridade do certificado e, consequentemente, da chave pública.

[14] O período de validade que as CA permitem para os certificados varia de CA para CA.
[15] A assinatura do certificado é efetuada através da utilização de uma função de dispersão (*hashing*) para gerar um resumo (*hash*) do certificado que é posteriormente assinado digitalmente com a chave privada da CA.

Tendo em consideração que qualquer um pode criar uma CA e assinar o seu próprio certificado, o facto de o certificado do Bob ser assinado por uma CA não garante que esse certificado seja confiável. Para validar a confiança no certificado existe, na PKI da Internet, um mecanismo que se designa por cadeia de confiança (*chain of trust*) ou cadeia de certificação.

Figura 9
Exemplo da cadeia de confiança de um certificado.

Fonte. Adaptação de imagem obtida de GeoCerts, Inc (s.d.)

A cadeia entre as CA e o certificado de nome de domínio exemplificado na Figura 9 permite garantir que o certificado é confiável. Assim, para o certificado do Bob ser confiável, toda a cadeia de confiança desse certificado tem de ser confiável. Só com a validação desta confiança se garante a autenticidade do certificado de Bob.

Na Figura 9 a CA «Baltimore» auto-assinou o certificado «Baltimore CyberTrust Root» e delegou parte do seu papel à CA ao Sistema de Certificação Electrónica do Estado (SCEE) através do certificado «ECRaizEstado»[16]. O SCEE, por sua vez, delegou a si mesmo parte do seu papel de CA, assinando o certificado «ECCE» (de Entidade Certificadora Comum do Estado). Por fim, o SCEE utilizou o certificado «ECCE» para assinar o certificado «*.portaldasfinancas.gov.pt» da AT (de Autoridade Tributária e Aduaneira)[17]. Neste exemplo, o certificado

[16] A CA de raiz (que auto-assina o seu certificado), mediante o cumprimento de determinados requisitos, pode delegar parte do seu papel de CA a outras entidades, que por sua vez podem delegar parte desse papel a outras entidades.
[17] O certificado «*.portaldasfinancas.gov.pt» certifica todos os subdomínios do nome de domínio portaldasfinancas.gov.pt.

«Baltimore CyberTrust Root» é designado por certificado raiz, os certificados «ECRaizEstado» e «ECCE» são designados por certificados intermédios e o certificado «*.portaldasfinancas.gov.pt» é designado por certificado de nome de domínio. Assim, respetivamente, a CA «Baltimore» é designada CA de raiz (*root* CA) e a CA SCEE designada por CA intermédia.

Uma vez que a cadeia de confiança se baseia na confiança da CA de raiz, para garantir que esta é confiável, os certificados de todas as CA de raiz confiáveis estão incorporados nos sistemas operativos de todos os dispositivos (computadores, telefones inteligentes, etc.)[18].

Na posse de um certificado confiável, o Bob (detentor do servidor) instala o seu certificado e os certificados das CA intermédias no seu servidor Web[19]. Quando a Alice (cliente) acede ao servidor do Bob utilizando HTTPS, pede o certificado do servidor, verifica a integridade do certificado, verifica toda a cadeia de confiança, verifica se a data de validade não foi atingida e, finalmente, se o certificado não foi revogado[20]. Para verificação da revogação do certificado junto da autoridade de validação (VA, do inglês *validation autorithy*) é utilizada a lista de revogação de certificados (CRL, do inglês *certificate revocation list*) (Housley, Ford, Polk, & Solo, 1999) ou o Online Certificate Status Protocol (OCSP) (Myers, Ankney, Malpani, Galperin, & Adams, 1999)[21].

Por fim, a Alice (cliente) possui um certificado que contém a chave pública do servidor do Bob e sabe que a chave é íntegra, válida e autêntica[22].

Em seguida, para efetuar o acordo de troca de chaves, utilizando o algoritmo RSA, a Alice gera um número aleatório, utiliza a chave pública do servidor do Bob para o encriptar, e envia-o para o servidor do Bob[23]. Esse número aleatório consiste no chamado segredo mestre prévio (*premaster secret*) e é utilizado pelo servidor e pelo cliente, conjuntamente com números aleatórios trocados nas mensagens de olá do cliente e de olá do servidor, para calcular o segredo mestre (*master secret*). O segredo mestre contém, entre outros elementos, a chave secreta que será utilizada durante o processo de encriptação da mensagem.

Tendo sido encriptada utilizando a chave pública do servidor, o segredo mestre prévio pode ser decifrado pelo servidor do Bob recorrendo à sua chave privada. Pode verificar-se que

[18] A cadeia de confiança é verificada recorrendo à lista de CA de raiz confiáveis presentes nos sistemas operativos.
[19] Uma vez que os certificados das CA de raiz estão presentes em todos os sistemas operativos, não é necessário instalá-los nos servidores. Pode, no entanto, existir casos que uma CA de raiz é válida para um fabricante de determinado dispositivo, mas não é válida para outro. É importante realçar que nestes casos um certificado pode ser confiável num determinado dispositivo e noutro não. Por esse motivo, é comum as CA de raiz indicarem no seu sítio Web o nível de compatibilidade.
[20] Uma CA pode revogar, i.e., invalidar um certificado se este não cumprir os requisitos definidos pela própria CA.
[21] A VA, a RA e a CA são muitas vezes a mesma entidade.
[22] O TLS também permite o processo reverso, i.e., que o cliente se autentique perante o servidor. Para esse efeito são utilizados os designados certificados de cliente. Um exemplo deste processo é a utilização do Cartão de Cidadão que contêm um certificado para se autenticar, por exemplo, no Portal das Finanças. Embora seja também um aspeto relevante nesta área, por questões de exequibilidade, a autenticação do cliente não está no âmbito deste estudo.
[23] Utilizando o RSA o termo correto é «transporte de chave» e não «troca de chave».

a segurança do acordo de troca de chave depende da chave privada do servidor de Bob. Imagine-se agora que todas as comunicações do servidor são escutadas por um atacante que as armazena durante vários anos e que este, num determinado momento, consegue obter a chave privada do servidor do Bob. Além de todas comunicações futuras estarem comprometidas, todas as comunicações anteriores a essa data ficam também comprometidas, pois a chave privada permite descodificar as comunicações armazenadas pelo atacante. Ou seja, para cada sessão de comunicação, permite descodificar a informação trocada no aperto de mão e, assim, obter o segredo mestre, o que lhe permite descodificar a informação transmitida durante a sessão em qualquer dos sentidos.

Se se garantir que toda a informação encriptada até o momento em que a chave privada foi comprometida continua segura, diz-se que existe sigilo persistente (FS, do inglês *forward secrecy*) (Shannon, 1949). Através de algoritmos matemáticos que utilizam outras chaves para gerar do segredo mestre prévio, o FS garante que o segredo mestre não pode ser descoberto mesmo que a chave privada venha a ser comprometida[24]. No TLS, o FS é conseguido através da utilização do algoritmo Diffie-Hellman (DH) (Diffie & Hellman, 1976) no acordo de troca de chaves[25].

No entanto, se no algoritmo do FS se utilizar sempre a mesma chave na geração do segredo mestre prévio, e se essa chave de geração for comprometida, os segredos mestres de todas as sessões de comunicação poderão ficar comprometidas. Se, por outro lado, se usar sempre chaves diferentes, diz-se que existe sigilo persistente perfeito (PFS, do inglês *perfect forward secrecy*). No TLS, o PFS é conseguido através da utilização do algoritmo de Diffie-Hellman efémero (DHE, do inglês Diffie-Hellman *ephemeral*).

Devido ao peso computacional do algoritmo DH, para uma melhor relação entre custo e benefício no acordo de troca de chaves, foram desenvolvidas versões dos algoritmos DH que recorrem à utilização de curvas elípticas (Blake-Wilson, Bolyard, Gupta, Hawk, & Moeller, 2006): o Diffie-Hellman de curva elíptica (ECDH, do inglês *elliptic curve* Diffie-Hellman) e o Diffie-Hellman efémero de curva elíptica (ECDHE, do inglês *elliptic curve* Diffie-Hellman *ephemeral*).

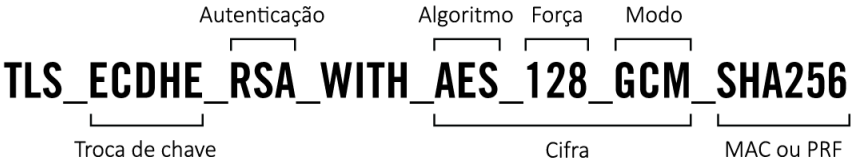
[24] O conceito de FS é explicado num vídeo utilizado pela Khan Academy (Gambling with Secrets, 2012a).
[25] O algoritmo DH é explicado num vídeo utilizado pela Khan Academy (Gambling with Secrets, 2012b).

2.3.3. Acordo de utilização de especificações de cifra.

A lista de especificações de cifra é uma lista «transmitida do cliente para o servidor na mensagem de olá do cliente, contendo as combinações de algoritmos criptográficos suportadas pelo cliente, pela ordem de preferência do cliente (a escolha favorita primeiro)» (Dierks & Allen, 1999, p. 35)[26]. Cada especificação de cifra «define um algoritmo de troca de chaves, um algoritmo de encriptação em massa (incluindo o tamanho da chave secreta) e um algoritmo de código de autenticação de mensagem» (Dierks & Allen, 1999, p. 35)[27]. O servidor recebe a lista de especificações de cifra enviada pelo cliente e «irá selecionar uma das especificações de cifra ou, se não lhe for apresentada uma escolha aceitável, irá devolver um alerta de falha no aperto de mão e terminar a conexão» (Dierks & Allen, 1999, p. 35)[28].

Além do protocolo e do algoritmo de autenticação (definido pelo certificado), na especificação de cifra são também indicados quais serão os algoritmos utilizados nos processos de troca de chaves, encriptação em massa e autenticação de mensagem.

Figura 10
Identificação dos componentes de uma especificação de cifra.



Fonte. Ristić (2014, p. 50)

Como representado na Figura 10, a especificação de cifra inclui também a cifra (algoritmo, força e modo de operação) a utilizar na encriptação em massa e a função de dispersão ou a função pseudoaleatória (PRF, do inglês *pseudo random function*) a utilizar para obter o código de autenticação da mensagem (MAC, do inglês *message autentication code*) para a autenticação e verificação da integridade da mensagem.

Tabela 6
Exemplos de algoritmos de cifra.

Designação	Abreviatura
Advanced Encryption Standard	AES
Data Encryption Standard	DES

[26] O servidor pode definir que deve ser utilizada a sua preferência de especificações de cifra, e não a do cliente. Nesse caso, será escolhida a primeira especificação de cifra da lista do servidor que conste na lista de especificações de cifra do cliente.
[27] O processo de encriptação em massa é o processo de cifragem da mensagem, isto é, da encriptação dos dados.
[28] A título de exemplo, o sítio Web da aplicação OpenSSL, uma das mais utilizadas, contém a lista de especificações de cifra suportadas pela sua biblioteca (OpenSSL Software Foundation, s.d.).

Designação	Abreviatura
Triple Data Encryption Standard	3DES
Ron Rivest 4	RC4
Camellia	-
ChaCha20	-

A «cifra» indica qual o «algoritmo» de cifra a utilizar (Tabela 6), qual a «força», isto é, o tamanho da chave secreta a utilizar nesse algoritmo (e.g., 128 bit, 256 bit) e qual o «modo» de operação a utilizar (Tabela 7) no processo de encriptação em massa dos dados[29].

Tabela 7

Exemplos de modos de operação de cifra.

Designação	Abreviatura
Cipher Block Chaining	CBC
Counter with CBC-MAC	CCM
Galois/Counter Mode	GCM
Stream	-

O MAC é composto por um pequeno resumo (*hash*) obtido utilizando uma função de dispersão ou uma função pseudoaleatória que tem a mensagem e a chave secreta como fontes (*inputs*)[30]. Tem a dupla função de verificar a integridade e autenticar a mensagem enviada.

Tabela 8

Exemplos de funções de dispersão.

Designação	Abreviatura
Message Digest 5	MD5
Secure Hash Algoritm 1	SHA-1
Secure Hash Algoritm 2	SHA-2

Tanto os algoritmos de cifra como as funções de dispersão podem ter maior ou menor força (medida em *bits*) para resistir a ataques[31]. Ao longo deste documento será utilizada a nomenclatura algoritmo/força ou função/força (e.g., AES/128 ou SHA-2/256) para especificar os algoritmos ou funções criptográficas e a respetiva força utilizada. Pode também ser utilizado o sinal «+» para indicar uma força igual ou superior à especificada (e.g., AES/128+). A mesma nomenclatura será utilizada para os algoritmos dos processos de autenticação e de troca de

[29] Os modos de operação dependem do algoritmo de cifra. A título de exemplo, para o AES existem os modos CBC, CCM e GCM, para o RC4 apenas existe o modo *stream*. Os modos de operação também podem estar apenas implementados em certas versões do protocolo. A título de exemplo, para o algoritmo AES, no TLS 1.0 apenas existe o modo CBC, no TLS 1.1 e TLS 1.2 existe também o modo de operação CCM. O modo GCM só pode ser utilizado no TLS 1.2 ou superior.

[30] Na criptografia o MAC é designado por Hash-based Message Authentication Code (HMAC).

[31] É necessário ter em consideração que esta força tem significados distintos em algoritmos de encriptação assimétrica, algoritmos de encriptação simétrica, curvas elípticas ou funções de dispersão. No anexo B é efetuada uma comparação de algumas das forças mais utilizados. Adicionalmente, o sítio Web da BlueKrypt permite comparar as forças dos vários algoritmos. Disponibiliza também recomendações de várias organizações relativas às forças a utilizar (Giry, 2015).

chave (e.g., RSA/2048+). Realça-se que nem todos algoritmos ou funções criptográficas permitem diferentes forças. Nestes casos, não será colocada indicação da força (e.g., SHA-1).

2.4. Vulnerabilidades nas implementações, protocolos e cifras.

A segurança das comunicações na Internet é um processo contínuo. Isto é, exige monitorização e reconfiguração permanentes. Praticamente todos os anos são identificadas e divulgadas novas vulnerabilidades. Estas frequentemente geram pânico na Internet, como foi o caso da vulnerabilidade, designada por Heartbleed, descoberta na implementação do TLS no OpenSSL em 2014.

De realçar que algumas vulnerabilidades são teóricas, isto é, sem demonstração prática. Outras, dado que necessitam de supercomputadores, tipicamente disponíveis apenas para organismos estatais, tais como agências de espionagem, são de muito difícil exploração. Não obstante, algumas vulnerabilidades podem ser exploradas com relativa facilidade por um indivíduo ou organização criminosa com conhecimentos na matéria.

Importa distinguir três tipos de vulnerabilidades:

- vulnerabilidades nas implementações,
- vulnerabilidades nos protocolos e
- vulnerabilidades nos algoritmos de cifra ou nas funções de dispersão.

As vulnerabilidades nas implementações e as vulnerabilidades nos protocolos, quando descobertas, são inseridas na base de dados de Common Vulnerabilities and Exposures (CVE). As CVE são o «padrão para a indústria quanto a designações de vulnerabilidades e exposições» (The MITRE Corporation, 2014b)[32].

As vulnerabilidades na implementação (Tabela 9) ocorrem quando uma determinada aplicação não implementa corretamente a especificação do protocolo ou do algoritmo da cifra. Por norma, estas vulnerabilidades, depois de descobertas, são rapidamente corrigidas pelo produtor, que disponibiliza uma atualização da aplicação que resolve o problema.

Tabela 9

Exemplos de vulnerabilidades detetadas nas implementações.

Vulnerabilidade[33]	**Código CVE**
Heartbleed	CVE-2014-0160
OpenSSL CCS Injection Vulnerability	CVE-2014-0224

[32] Os CVE podem ser consultados em linha (The MITRE Corporation, 2014a).

[33] As designações das vulnerabilidades não são traduzidas por se tratar de designações padrão na indústria, refletidas nas CVE.

As vulnerabilidades nos protocolos (Tabela 10), neste caso nos protocolos SSL ou TLS em conjugação com o HTTP, são vulnerabilidades na especificação dos próprios protocolos. Estas vulnerabilidades atingem os sistemas que os usam e habitualmente conduzem a melhoramentos nos protocolos.

Tabela 10
Exemplos de vulnerabilidades detetadas nos protocolos.

Vulnerabilidade	Código CVE
Insecure Renegotiation (Ray & Dispensa, 2009)	CVE-2009-3555
Browser Exploit Against SSL/TLS Attack (BEAST) (Duong & Rizzo, 2011)	CVE-2011-3389
Compression Ratio Info-leak Made Easy (CRIME) (Duong & Rizzo, 2012)	CVE-2012-4929
Lucky Thirteen (AlFardan & Paterson, 2013)	CVE-2013-0169
Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH) (Gluck, Harris, & Prado, 2013)	CVE-2013-3587
Triple Handshake (Bhargavan, Lavaud, Fournet, Pironti, & Strub, 2014)	CVE-2014-1295
Padding Oracle On Downgraded Legacy Encryption (POODLE) (Möller et al., 2014)	CVE-2014-3566
Padding Oracle On Downgraded Legacy Encryption (POODLE) over TLS (Langley, 2014)	CVE-2014-8730
Factoring Attack on RSA-EXPORT Keys (FREAK) (Bhargavan et al., 2015)	CVE-2015-0204
The Logjam Attack (Adrian et al., 2015)	CVE-2015-4000

As vulnerabilidades nos algoritmos de cifra (Tabela 11) ou nas funções de dispersão (Tabela 12) estão habitualmente relacionadas com o incremento do poder computacional, que faz com que cifras ou funções de dispersão anteriormente consideradas seguras passem a ser consideradas menos seguras, ou até mesmo inseguras, para um determinado tipo de utilização.

Tabela 11
Exemplos de algoritmos de cifra considerados menos seguros ou inseguros.

Algoritmo de cifra
DES (Matsui, 1994)
RC4 (AlFardan, Bernstein, & Paterson, 2013)

Tabela 12
Exemplos de funções de dispersão consideradas menos seguras ou inseguras.

Função de dispersão
MD5 (Wang & Yu, 2005)
SHA-1 (Stevens, 2013)

2.5. Compatibilidade das tecnologias.

Algumas das tecnologias utilizadas pelo TLS foram padronizadas IETF nos últimos anos. Uma das questões que se levanta é a compatibilidade destas tecnologias com os dispositivos clientes mais antigos. Os casos mais problemáticos são as versões 1.1. e 1.2. do protocolo TLS, a utilização de curvas elípticas (e.g., ECDSA e ECDHE), a utilização do modo de operação de cifra GCM (e.g., AES/128 GCM) e a utilização da função de dispersão SHA-2.

Os três sistemas operativos com maior utilização são o Microsoft Windows, o Google Android e o Apple iOS («Usage share of operating systems», 2015)[34]. A Tabela 13 agrega a compatibilidade destes sistemas operativos com as tecnologias referidas («Comparison of TLS implementations», 2015; GlobalSign, 2015a, 2015b; Qualys, Inc, 2015b; Zoller, 2011).

Tabela 13
Compatibilidade entre tecnologias e sistemas operativos.

Sistema operativo e versão	**TLS 1.1 e TLS 1.2**	**Curvas elípticas**	**Modo de operação GCM**	**Função de dispersão SHA-2**
Microsoft Windows				
XP	Não suporta	Não suporta	Não suporta	Não suporta
XP *service pack* 3	Não suporta	Não suporta	Não suporta	Suporta
Vista	Não suporta	Suporta	Não suporta	Suporta
7 (ou superior)	Suporta	Suporta	Suporta	Suporta
Google Android				
2.3	Suporta	Não suporta	Não suporta	Suporta
4.0	Suporta	Suporta	Não suporta	Suporta
4.4 (ou superior)	Suporta	Suporta	Suporta	Suporta
Apple iOS				
5 a 8	Suporta	Suporta	Não suporta	Suporta
9 (ou superior)	Suporta	Suporta	Suporta	Suporta

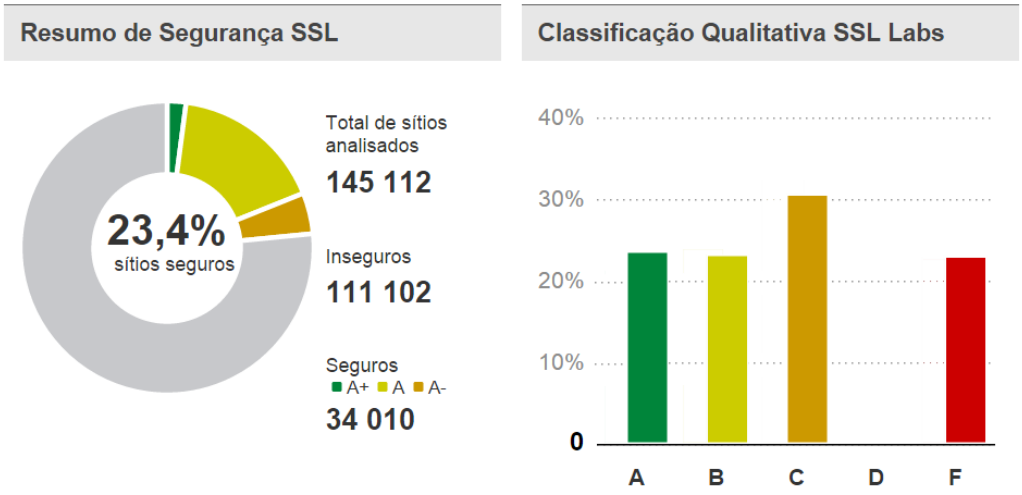
2.6. Estado atual da utilização de comunicações seguras nos sítios Web.

Desde de abril de 2012 que o Trustworthy Internet Movement (TIM), no âmbito do projeto SSL Pulse, analisa mensalmente o estado da utilização de comunicações seguras através de HTTPS nos principais sítios da Internet. A análise realizada pelo SSL Pulse em agosto de 2015 (Figura 11) conclui que, num total de 145 112 sítios Web analisados, apenas 23,40 % (34 010 sítios Web) são considerados seguros (TIM, 2015). Isto significa que 76,60 % dos sítios Web analisados não tem a segurança das comunicações devidamente implementada.

[34] As várias versões destes três sistemas operativos correspondem a cerca de 85 % a 95 % dos dispositivos clientes.

Figura 11

Estado da qualidade das comunicações através de HTTPS em agosto de 2015.



Fonte. Adaptação de gráficos obtidos de TIM (2015)

No panorama nacional existem vários estudos sobre a segurança de sítios e aplicações Web, entre os quais o projeto Nonius, cuja ambição foi «produzir um histórico fidedigno de dados indicadores do nível de segurança da Internet Portuguesa» (Rente, Rela, Trovão, & Alves, 2008), Não foi, no entanto, encontrada nenhuma análise específica à qualidade das comunicações encriptadas dos sítios Web em Portugal.

3. Recomendações de Segurança

3.1. Âmbito da encriptação.

Conforme referido anteriormente, as comunicações na Internet através do protocolo HTTP não são encriptadas. Um atacante com intenções de roubar dados ou simplesmente vigiar a atividade de um cidadão ou organização pode fazê-lo, desde que tenha acesso ou se apodere de um dos equipamentos que integram o canal de comunicação. Como demonstrado recentemente nos documentos disponibilizados pelo antigo consultor da National Security Agency (NSA) dos EUA, Edward Snowden («Edward Snowden», 2015), não são só atacantes que têm acesso a esses equipamentos: agências de espionagem governamentais também o podem ter e, dessa forma, vigiar as atividades dos cidadãos ou das organizações.

As comunicações devidamente encriptadas permitem que os dados que viajam através da rede não possam ser interpretados. Garantem por isso, neste aspeto, a proteção dos dados e a privacidade da atividade. Mas deve-se encriptar todas as comunicações?

Na sequência do caso Snowden, este é um debate que atualmente está a ter lugar entre os principais protagonistas da Internet. De uma forma geral, estes defendem que todo o tráfego deve ser encriptado. A empresa Google lançou um projeto designado HTTPS Everywhere (Grigorik & Far, 2014). Um dos primeiros passos desse projeto foi atribuir maior pontuação no seu algoritmo de pesquisa a sítios que utilizem comunicações encriptadas, i.e., HTTPS (Bahajji & Illyes, 2014). A Eletronic Frontier Foundation (EFF) lançou um projeto designado também HTTPS Everywhere para criar um *plugin* para os navegadores (*browsers*) com o objetivo de facilitar a encriptação das comunicações entre o navegador e os servidores dos sítios Web que se visita (EFF, 2014). A Cisco, a Mozilla, a Akamai, a EFF e a IdenTrust estão a desenhar, no âmbito do projeto Let's Encrypt, um novo protocolo para facilitar todo o processo de obtenção e renovação de certificados (Internet Security Research Group, 2015). Berners-Lee (2014), por muitos considerado o criador da World Wide Web, também concorda com este movimento, referindo que «é uma boa ideia encriptar as coisas em todo o lado». Reconhecendo o valor da privacidade para os seus clientes, muitos dos principais protagonistas da Internet (Facebook, Twitter, Google, Wikipedia, etc.) estão a modificar os seus sítios e aplicações Web para que funcionem exclusivamente sobre HTTPS.

Mas será que toda a informação é suficientemente relevante para ser encriptada? Esta questão não é de resposta simples, pois depende da perspetiva. Se se analisar um sítio Web como um caso isolado, dependerá dos dados que são transmitidos. Se se analisar o sítio em questão como uma fonte de dados que, em conjunto com a atividade de muitos outros sítios Web, permita aplicar algoritmos para analisar comportamentos de um cidadão ou organização, então a perspetiva poderá ser outra. Essa é a razão pela qual estas organizações defendem que todo o tráfego na Internet através do protocolo HTTP deve ser encriptado.

3.2. Recomendações.

3.2.1. Legislação nacional.

Ao nível de legislação nacional existe o Regulamento Nacional de Interoperabilidade Digital (RNID), publicado na Resolução de Conselho de Ministros n.º 91/2012 de 8 de novembro (2012), em cumprimento do artigo n.º 5 da Lei n.º 36/2011 de 21 de julho (2011), que define as especificações técnicas e os formatos digitais a adotar pela administração pública. O RNID indica na Tabela III, relativa às «Tecnologias de interface web, incluindo acessibilidade, ergonomia, compatibilidade e integração de serviços», que o «Protocolo hipertexto seguro para disponibilização de página web» a utilizar de forma «Obrigatória» é o «HTTPS» (2012, p. 6463).

Na Tabela VIII, que representa as «Especificações técnicas de segurança para redes, serviços, aplicações e documentos», especifica que deve ser utilizado de forma «Obrigatória» o «TLS 1.0» (2012, p. 6464). Os números 6 e 7 do RNID referem que «as versões mais recentes das especificações técnicas constantes no presente Regulamento e classificadas como obrigatórias, são suscetíveis de serem adotadas, desde que retrocompatíveis com a versão constante no Regulamento», i.e., obriga a que «sejam disponibilizadas as duas versões, desde que tal seja possível» e acrescenta que «são ainda classificados como "recomendado" versões posteriores das especificações técnicas e formatos digitais definidos nas tabelas I a IX» (2012, pp. 6461–6462).

Conclui-se que, ao nível de legislação nacional, o protocolo a ser utilizado nas comunicações seguras é o TLS (TLS 1.0 obrigatório, versões superiores recomendadas). Não existe indicação sobre os algoritmos, funções e forças a utilizar nas várias etapas deste protocolo.

3.2.2. Recomendações internacionais.

As principais organizações internacionais que emitem recomendações sobre esta temática são o National Institute of Standards and Technology (NIST), a European Union Agency for Network and Information Security (ENISA) e a NSA.

O NIST é responsável pelos Federal Information Processing Standards (FIPS) que, embora tenham sido criados para padronizar assuntos relacionados com a segurança e as comunicações nas instituições não militares do governo dos EUA, são utilizados a nível global. O NIST também é responsável pela publicação das Special Publications (SP), que são guias e recomendações de segurança. Para o TLS em particular foi publicada a SP 800-52 cuja primeira revisão foi efetuada em 2014 (Polk, McKay, & Chokhani, 2014)[35].

A ENISA publica regulamente relatórios e recomendações sobre a utilização de segurança nas comunicações eletrónicas para os Estados-Membros da União Europeia. As publicações mais relevantes para este estudo são o relatório sobre os protocolos criptográficos (Smart, Rijmen, Stam, Warinschi, & Watson, 2014) e o relatório sobre os algoritmos, tamanhos de chave e parâmetros (Smart, Rijmen, Gierlichs, et al., 2014).

A NSA participa na definição de normas e publica recomendações sobre utilização de algoritmos criptográficos. A NSA divide as suas recomendações em duas coleções (*suites)*: a coleção A, que é secreta e por isso não divulgada ao público em geral, e a coleção B, que são as suas recomendações para utilização de encriptação de comunicações pela generalidade do governo dos EUA. Estas recomendações abordam vários protocolos. No caso específico do

[35] No sítio Web do NIST pode ser consultada a lista de publicações de FIPS (NIST, 2014a) e de SP (NIST, 2014b).

TLS, a NSA patrocinou um Request For Comments (RFC) informativo (Salter & Housley, 2012). A coleção B define dois tipos de combinações para cumprimento das suas recomendações: a combinação 1 e a combinação 2 (Salter & Housley, 2012). A principal diferença entre as duas combinações é que a primeira deve ser utilizada em comunicações classificadas como «*secret*» e a segunda deve ser utilizada em comunicações classificadas como «*top secret*». No âmbito deste documento, será utilizada a combinação 1.

a. Protocolo.

O SP 800-52 do NIST recomenda que «servidores que suportem aplicações para cidadãos ou negócios, devem ser configurados para suportar a versão 1.1 e devem ser configurados para suportar a versão 1.2», acrescentando que «estes servidores podem também ser configurados para suportar o TLS versão 1.0», adiantando ao mesmo tempo que «se o TLS 1.0 for suportado, o uso de TLS 1.1 e TLS 1.2 deve ser preferido ao TLS 1.0» (Polk et al., 2014, p. 9).

A ENISA recomenda a utilização do TLS 1.2 e indica que considera «difícil recomendar que o TLS 1.0 e o TLS 1.1 sejam utilizados para qualquer aplicação recente» e que «a migração de aplicações antigas é aconselhada» (Smart, Rijmen, Stam, et al., 2014, p. 10). Conclui-se que a ENISA apenas recomenda a utilização de TLS 1.2. No entanto, por razões de interoperabilidade com sistemas antigos, permite a utilização do TLS 1.1 e do TLS 1.0.

A NSA recomenda a utilização do TLS 1.2 e afirma que, quando «o cliente ou o servidor não suportam o TLS versão 1.2 […], um perfil transitório, que não cumpre a coleção B, pode ser utilizado para garantir interoperabilidade» (Salter & Housley, 2012, pp. 2–3). Adianta ainda que esse perfil transitório permite o TLS 1.0 e o TLS 1.1 (Salter & Housley, 2012, p. 11). Ou seja, a NSA apenas recomenda a utilização de TLS 1.2. No entanto, por razões de interoperabilidade com sistemas antigos, permite a utilização do TLS 1.1 e do TLS 1.0.

b. Autenticação e troca de chaves.

O SP 800-52 do NIST indica que para os certificados «deve» ser utilizado o RSA, «devia» ser utilizado o ECDSA e «pode» ser utilizado o DSA. Adianta que em relação à força da chaves dos algoritmos de autenticação, no caso do RSA e do DSA, deve ser de 2048 bit ou superior, no caso do ECDSA, deve-se utilizar as curvas «P-256 ou P-384», ou seja, 256 bit ou 356 bit (Polk et al., 2014, p. 12). Em relação à troca de chaves, indica que «deve» ser utilizado o RSA, «devia» ser utilizado o ECDHE e «podem» ser utilizados o DH, o DHE e o ECDH (Polk et al.,

2014, pp. 16–18). Relativamente à força da troca de chave, deve ser de 2048 bit ou superior, e, no caso de curvas elípticas de 256 bit ou de 356 bit (Polk et al., 2014, p. 12).

A ENISA é a mais restritiva em relação a este assunto, pois indica que existe «a falta de um algoritmo de assinatura de chave pública com segurança comprovada nas escolhas disponíveis» (Smart, Rijmen, Stam, et al., 2014, p. 8). No entanto, indica que dentro das escolhas disponíveis a sua preferência recai sobre «assinaturas ECDSA que têm maior probabilidade de ser seguras no longo prazo que o método RSA». Dada a «situação atual», permite também a utilização do DSA e do RSA (Smart, Rijmen, Stam, et al., 2014, p. 9). Em relação à troca de chave, a ENISA refere que «o acordo de troca de chave de Diffie-Hellman é considerado muito mais seguro, e oferece o benefício do sigilo persistente perfeito para a chave acordada» e, por esse motivo, recomenda a utilização de DHE ou de ECDHE (Smart, Rijmen, Stam, et al., 2014, pp. 8–9). Em relação à força da autenticação e da troca de chave a ENISA indica que, no caso do RSA, do DSA e do DHE, deve ser utilizada uma força de 3072 bit ou superior e, no caso do ECDSA e o ECDHE, devem ser utilizadas curvas de 256 bit ou superiores, permitindo, no entanto, para efeitos de retrocompatibilidade, a utilização de forças de 1024 bit ou 2048 bit e, no caso de curvas elípticas, de 160 bit (Smart, Rijmen, Gierlichs, et al., 2014, p. 37).

A NSA indica que «tem de ser utlizado ECDSA para as assinaturas eletrónicas; outros métodos de autenticação sem ser o ECDSA-256 e o ECDSA-384 não podem ser utilizados para autenticação no TLS» (Salter & Housley, 2012, p. 5). Em relação à troca de chaves, recomenda a utilização de «ECDH efémero» (Salter & Housley, 2012, p. 8). Estes pontos são válidos também para o perfil transitório. É interessante verificar que, ao recomendar apenas a utilização de ECDSA, exclui o uso de RSA para autenticação. Considerando que nenhuma vulnerabilidade de conhecimento público foi detetada no algoritmo RSA, surgiram rumores que indiciam que a NSA teria forma de o quebrar. Contudo, sendo uma questão que não é do conhecimento público, apenas se pode classificar como rumor.

c. Encriptação em massa e autenticação de mensagem.

O SP 800-52 do NIST recomenda que, para «maximizar a interoperabilidade, as implementações de TLS em servidores devem suportar» as seguintes conjugações de cifras de encriptação em massa e autenticação de mensagem: 3DES em modo CBC com SHA-1 e AES/128 em modo CBC com SHA-1, acrescentando que «deviam suportar» AES/256 em modo CBC com SHA-1. Para os servidores que suportam TLS 1.2, recomenda que também «devem suportar» a combinação AES/128 em modo GCM com SHA-2/256, e que «deviam suportar»

AES/256 em modo GCM com SHA-2/384, AES/128 em modo CBC com SHA-2/256 e AES/256 em modo CBC com SHA-2/384 (Polk et al., 2014, pp. 14–18).

A ENISA indica que «o uso de Camellia e AES, dentro dos modos como GCM ou CCM» são recomendados (Smart, Rijmen, Stam, et al., 2014, p. 9). Para autenticação da mensagem recomenda o SHA-2/256 e o SHA-2/384 (Smart, Rijmen, Stam, et al., 2014, pp. 9–10).

A NSA indica que deve ser utilizado no mínimo o algoritmo de encriptação «AES com chaves de 128 bit em modo GCM», ou seja, AES/128 em modo GCM, e SHA-2/256 para autenticação da mensagem (Salter & Housley, 2012, p. 4). No perfil transitório, permite a utilização de «AES com chaves de 128 bit em modo CBC», ou seja, AES/128 em modo CBC e SHA-1 para autenticação da mensagem (Salter & Housley, 2012, p. 11).

3.2.3. Resumo das recomendações e recomendações do estudo.

A maioria das organizações recomenda a utilização do protocolo TLS 1.2, aceitando o TLS 1.1 e o TLS 1.0 por razões de compatibilidade. Uma exceção é o Estado português que indica que o TLS 1.0 é obrigatório, talvez por o RNID ter sido publicado em 2012, quando ainda se desconheciam algumas falhas entretanto identificadas nos modos de operação dos algoritmos de cifra utilizados nas versões inferiores do TLS.

Relativamente à autenticação e troca de chaves, não existe unanimidade entre as organizações. Para a autenticação o ECDSA/256+ é a melhor escolha para a maioria, mas o DSA/2048+ e o RSA/2048+ também são, por enquanto, recomendados (embora, no caso da ENISA, só para sistemas antigos). Para a troca de chaves, os algoritmos DHE/2048+ e ECDHE/256+, que permitem PFS, são os recomendados, embora o NIST também permita o RSA/2048+, o DH/2048+ e o ECDH/256+. A ENISA, para sistemas antigos, permite forças menores tanto na autenticação como na troca de chaves. No entanto, para sistemas novos recomenda a utilização de forças maiores que o NIST.

Em relação à encriptação dos dados e autenticação da mensagem, o AES/128+ em modo GCM é consensual, o AES/128+ em modo CCM e o Camellia/128+ em modo GCM também são recomendados. O AES/128+ em modo CBC e o 3DES em modo CBC apenas por questões de interoperabilidade com sistemas antigos. Para autenticação da mensagem o SHA-2/256+ é o recomendado. O SHA-1 apenas para interoperabilidade com sistemas antigos.

Na Tabela 14 são resumidas as recomendações das várias organizações.

Tabela 14

Resumo das recomendações de várias organizações.

Entidade	Protocolos	Autentica-ção	Troca de chaves	Cifra	MAC ou PRF
Estado português	TLS 1.0 TLS 1.1 TLS 1.2	n.d.	n.d.	n.d.	n.d.
NIST	TLS 1.0[1] TLS 1.1 TLS 1.2	RSA/2048+ DSA/2048+ ECDSA/256+	RSA/2048+ DH/2048+ DHE/2048+ ECDH/256+ ECDHE/256+	AES/128+ GCM AES/128+ CBC 3DES CBC	SHA-2/256+ SHA-1
ENISA	TLS 1.0[1] TLS 1.1[1] TLS 1.2	RSA/3072+ RSA/1024+[1] DSA/3072+ DSA/1024+[1] ECDSA/256+ ECDSA/160+[1]	DHE/3072+ DHE/1024+[1] ECDHE/256+ ECDHE/160+[1]	AES/128+ GCM AES/128+ CCM Camellia/128+ GCM	SHA-2/256+
NSA	TLS 1.0[1] TLS 1.1[1] TLS 1.2	ECDSA/256+	ECDHE/256+	AES/128+ GCM AES/128+ CBC[1]	SHA-2/256+ SHA-1[1]

[1] Para efeitos de interoperabilidade com sistemas antigos.

Uma nova cifra, a ChaCha (Bernstein, 2008), foi recentemente adaptada para utilização nos protocolos da IETF. O objetivo desta adaptação é existir uma cifra sem vulnerabilidades conhecidas e com desempenho elevado que permita que o algoritmo de cifra AES deixe de ser a «única escolha prática» (Nir & Langley, 2015, p. 3). Por esse motivo, é importante considerar também a cifra ChaCha20 e o seu mecanismo de autenticação da mensagem designado por Poly1305[36].

Por fim, obtém-se a Tabela 15, que será referida ao longo deste documento como «Recomendações do estudo»[37].

Tabela 15

Recomendações do estudo: cruzamento das recomendações das organizações.

Protocolos	Autenticação	Troca de chaves	Cifra	MAC ou PRF
TLS 1.0[1] TLS 1.1 TLS 1.2	RSA/2048+ DSA/2048+ ECDSA/256+	RSA/2048+[1] DH/2048+[1] DHE/2048+ ECDH/256+[1] ECDHE/256+	ChaCha20 AES/128+ GCM AES/128+ CCM[2] AES/128+ CBC[1] Camellia/128+ GCM[2] 3DES CBC[1]	Poly1305 SHA-2/256+ SHA-1[1]

[1] Para efeitos de interoperabilidade com sistemas antigos.

[2] Apenas com DHE ou ECDHE na troca de chaves.

[36] A ChaCha20 é a variante da cifra ChaCha que foi adotada pela IETF.

[37] No anexo C é apresentada a lista de especificações de cifra que cumprem as recomendações do estudo.

III. Metodologia

Com o objetivo de avaliar o grau de cumprimento das recomendações de segurança estabelecidas pelas organizações nacionais e internacionais por parte dos sítios Web disponibilizados pelo Estado português foi efetuada uma análise quantitativa sobre a temática.

1. Sítios Web a Analisar

Considerando que a Agência para a Modernização Administrativa (AMA), nos termos do n.º 4 do artigo 47.º do Decreto-Lei n.º 73/2014, de 13 de maio (2014), deve «desenvolver e atualizar o cadastro dos sítios na Internet do Estado» (2014, p. 2754), foi solicitada a lista de sítios Web do Estado à AMA. Em resposta, a AMA enviou uma lista contendo 396 sítios Web.

Foi também consultado o serviço Web (*web service*) público do Sistema de Informação da Organização do Estado (SIOE), da responsabilidade da Direção-Geral da Administração e do Emprego Público (DGAEP), onde foi possível identificar 4 363 endereços de sítios Web (2 200 sítios Web únicos)[1].

A diferença entre o número de sítios Web devolvidos pelas duas entidades decorre do facto de o cadastro dos sítios Web do Estado da AMA estar ainda no seu primeiro ano. É expectável que, com o tempo, os números se aproximem.

Os testes a realizar nesta investigação podem ser, do ponto de vista legal, considerados uma tentativa de deteção (*scanning*) de vulnerabilidades para recolher informação para futuros ataques. Tendo em vista obter esclarecimentos sobre essa questão e, se necessário, autorização para a realização dos testes a todos os sítios Web do Estado, foi contactada a AMA, o Centro Nacional de Cibersegurança (CNCS) e a Autoridade Nacional de Comunicações (Anacom). Porém, estes esforços revelaram-se infrutíferos. Os pedidos de apoio jurídico efetuados junto da Associação Portuguesa para a Defesa do Consumidor (Deco) e da Universidade Europeia também não obtiveram êxito.

Dadas estas dificuldades, a alternativa encontrada foi solicitar autorização individualmente a várias entidades para a realização de testes aos seus sítios Web. Destas, apenas uma autorizou os testes em tempo útil. A entidade autorizou os testes, desde que não fosse identificada. Essa entidade disponibiliza 89 sítios Web, o que representa 4,05 % do total de sítios Web retornados pelo serviço Web do SIOE.

[1] A discrepância entre o número de sítios Web e o número de sítios Web únicos deve-se ao facto de o SIOE contabilizar como contactos as páginas Web de entidades nos sítios Web dos Ministérios ou Direções-Gerais.
O SIOE e o serviço Web estão disponíveis na Internet (DGAEP, s.d.a, DGAEP, s.d.b).

Dado que a política para as TIC (coordenada pela AMA) é comum a toda a Administração Pública e que a entidade que autorizou os testes, além de disponibilizar sítios Web informativos, presta também serviços em linha, considera-se que esta amostra de sítios Web, não sendo o inicialmente planeado e dadas as restrições já referidas, permite representar, dentro do possível, os sítios Web do Estado.

2. Instrumentos de Recolha de Dados

Tendo em conta o número de sítios Web a testar e a necessidade de posterior processamento dos dados, optou-se por utilizar métodos automáticos para recolher os dados. Investigou-se qual seria ferramenta mais adequada para realizar essa tarefa e considerou-se que a ferramenta SSL Server Scan (Qualys, Inc, 2015a) é a indicada pelas seguintes razões:

- Tem um método de avaliação da utilização de comunicações encriptadas disponibilizado gratuitamente na Internet.
- Possui documentação sobre os critérios utilizados na avaliação (Qualys, Inc, 2015c).
- Disponibiliza publicamente uma *application programming interface* (API) (Qualys, Inc, 2015e)[2], a qual permite recolher de forma sequencial dados sobre a utilização de HTTPS em sítios Web[3].
- O seu desenvolvimento é liderado por Ivan Ristić, autor reputado de várias ferramentas e livros sobre a utilização de comunicações seguras na Internet.

3. Recolha de Dados

A recolha de dados teve início a 3 de agosto de 2015 utilizando a API referida no ponto anterior[4]. Para se poder compreender a evolução da implementação de comunicações encriptadas os testes são efetuados, de forma automática, uma vez a cada mês. Os dados recolhidos são guardados em base de dados, sendo que, por omissão, apenas o mais recente é contabilizado.

Na recolha de agosto, que é a utilizada neste estudo, foram efetuados testes ao fornecimento de comunicações encriptadas a 89 sítios Web, sendo que 5 não foram completados com sucesso por não ter sido possível o contacto com o servidor. Assim, para efeitos deste estudo, esses 5 foram ignorados, tendo sido considerados os restantes 84 sítios Web.

[2] Esta API foi alvo de contributos do autor desta dissertação, que identificou problemas e fez sugestões de melhorias que podem ser consultados em https://goo.gl/T1151E.
[3] A ferramenta utiliza um *script* na linguagem de programação Go (Google, Inc, s.d.). Um *script* é um conjunto de instruções que permitem automatizar uma sequência de tarefas a serem executadas numa linguagem de programação de *scripting*.
[4] A utilização da API para este estudo foi autorizada por Ivan Ristić.

4. Análise e Classificação

Os dados recolhidos são posteriormente agregados utilizando um *script* desenvolvido para o efeito. Este *script* utiliza como base a metodologia de classificação pela ferramenta SSL Server Scan (Qualys, Inc, 2015c) com algumas adaptações. Para cada servidor de publicação do sítio Web, os métodos de análise e classificação são descritos nas próximas secções[5].

4.1. Inspeção de comunicações.

Neste passo, que é uma adaptação à metodologia da Qualys, é efetuada uma análise das comunicações do servidor. Verifica-se se existe possibilidade de realizar o teste. Quando não é possível, é atribuída a classificação «X». Quando é possível e se verifica que o servidor não disponibiliza comunicações encriptadas, é atribuída a classificação «N» (de *not encrypted*)[6].

4.2. Inspeção de certificados.

Neste passo é efetuada uma análise aos certificados enviados pelo servidor. Verifica-se «se o certificado é válido e se é confiável» (Qualys, Inc, 2015c, p. 2). Se o certificado não corresponde ao nome de domínio do sítio Web, é atribuída a classificação «M» (de *mismatch*). Se existem problemas de confiança no certificado ou na cadeia de confiança, i.e., se faltam certificados intermédios, se a CA não é confiável, se o certificado é auto-assinado, foi revogado ou expirou, ou se não é assinado por uma CA, é atribuída a classificação «T» (de *trust issues*).

4.3. Obtenção de classificação numérica.

Para obtenção da classificação numérica efetua-se a análise dos protocolos, da troca de chaves e das cifras, i.e., inspeciona-se a «configuração do servidor em três categorias: suporte de protocolos; suporte de troca de chaves; suporte de cifras» (Qualys, Inc, 2015c, p. 2).

Para obter a classificação da categoria «suporte de protocolos» verifica-se os protocolos suportados pelo servidor. Depois, utilizando a Tabela 16, obtém-se a classificação da categoria através da média aritmética de soma do valor do melhor e do pior protocolo suportado.

[5] Um sítio Web pode ser publicado por vários servidores Web, quer para balanceamento de tráfego, quer para distribuição geográfica do tráfego ou distribuição por protocolos IP (IPv4 e IPv6). No caso de sítios Web que são disponibilizados por mais do que um servidor de publicação Web, a classificação mais baixa dos servidores em questão será a considerada.

[6] É importante ressalvar que mesmo que um sítio Web permita comunicações encriptadas não significa que se apliquem a todos os pedidos efetuados ao sítio Web (e.g., páginas HTML, ficheiros estáticos, redireccionamentos, páginas de erro, etc.). Não sendo possível, por questões de exequibilidade, determinar com exatidão quais os sítios Web que permitem comunicações encriptadas de forma exclusiva essa questão não é verificada neste estudo.

Tabela 16

Valores de referência da categoria suporte de protocolos.

Protocolo	Valor (em percentagem)
SSL 2.0	0 %
SSL 3.0	80 %
TLS 1.0	90 %
TLS 1.1	95 %
TLS 1.2	100 %

Fonte. Qualys, Inc (2015c, p. 5)

Para se obter a classificação da categoria «suporte de troca de chaves» verifica-se a força do processo de troca de chaves suportada pelo servidor, identificada por *KS* (de *key strength*), e obtém-se a classificação através da correspondência definida pela Tabela 17.

Tabela 17

Valores de referência da categoria suporte de troca de chaves.

Força da troca de chave (*KS*)	Valor (em percentagem)
$KS = 0$ (sem autenticação)	0 %
$0 < KS < 512$ bit	20 %
512 bit $\leq KS <$ 1024 bit	40 %
1024 bit $\leq KS <$ 2048 bit	80 %
2048 bit $\leq KS <$ 4096 bit	90 %
$KS \geq$ 4096 bit	100 %

Fonte. Qualys, Inc (2015c, p. 6)

Para se obter a classificação da categoria «suporte de cifras» verifica-se a força das cifras suportadas pelo servidor. Em seguida, através da média aritmética de soma dos valores da cifra com a maior e menor força suportada, é calculada a força da cifra, identificada por *CS* (de *cipher strength*), e obtém-se a classificação através da correspondência definida pela Tabela 18.

Tabela 18

Valores de referência da categoria suporte de cifras.

Força da cifra (CS)	Valor (em percentagem)
$CS = 0$ (sem encriptação)	0 %
$0 < CS <$ 128 bit	20 %
128 bit $\leq CS <$ 256 bit	80 %
$CS \geq$ 256 bit	100 %

Fonte. Qualys, Inc (2015c, p. 7)

Por fim, combina-se «os resultados de cada categoria num resultado global», identificado por *N*, «expresso de forma numérica (0 a 100)» (Qualys, Inc, 2015c, p. 2), de acordo com o peso definido pela Tabela 19.

Tabela 19

Pesos relativos por categoria para obtenção de classificação numérica.

Categoria	Peso (em percentagem)
Suporte de protocolos	30 %
Suporte de troca de chaves	30 %
Suporte de cifras	40 %

Fonte. Qualys, Inc (2015c, p. 2)

4.4. Obtenção de classificação qualitativa.

A classificação numérica permite, através da correspondência definida pela Tabela 20, calcular a classificação qualitativa «numa escala de A a F» (Qualys, Inc, 2015c, p. 2).

Tabela 20

Conversão de classificação numérica para classificação qualitativa.

Classificação numérica (*N*)	Classificação qualitativa
$N \geq 80$	A
$65 \leq N < 80$	B
$50 \leq N < 65$	C
$35 \leq N < 50$	D
$20 \leq N < 35$	E
$N < 20$	F

Fonte. Qualys, Inc (2015c, p. 2)

Para obter a classificação qualitativa final, aplica-se ainda uma «série de regras […] para lidar com alguns aspetos da configuração do servidor que não podem ser expressos de forma numérica. A maior parte das regras reduzem a classificação» qualitativa «para A-, B, C, D, E, ou F se encontrarem uma funcionalidade que não deve ser utilizada. Algumas regras, de forma a recompensar configurações excecionais, aumentam a classificação para A+» (Qualys, Inc, 2015c, p. 2). Quando a classificação qualitativa é A+, A ou A- e no caso de incumprimento das recomendações do estudo (Tabela 15), é introduzida outra adaptação à metodologia da Qualys ao se reduzir a classificação qualitativa para B.

4.5. Obtenção do nível de segurança de comunicações.

Por último, este estudo introduz o conceito de nível de segurança de comunicações do sítio Web. Conforme demonstra a Tabela 21, este nível é obtido através do agrupamento das classificações qualitativas em nível de segurança de comunicações.

Tabela 21

Conversão de classificação qualitativa em nível de segurança de comunicações.

Nível de segurança de comunicações do sítio Web	Classificações qualitativas
Seguro	A+, A e A-
Razoavelmente seguro	B e C
Pouco seguro	D e E
Inseguro	F, T, M e N
Teste falhou	X

5. Disponibilização de Resultados

Além da disponibilização dos resultados neste estudo, tendo em vista tornar mesmos facilmente acessíveis ao público em geral, foi desenvolvido um sítio Web designado por «Web Pública» (https://webpublica.pt/)[7]. Com o intuito de demonstrar que, utilizando *software* de código aberto e gratuito, é possível implementar comunicações seguras num sítio Web, o referido sítio Web segue as recomendações deste estudo.

No sítio, os resultados são apresentados sob a forma de gráficos. Foi também desenvolvido um mecanismo que permite filtrar os resultados de diversas maneiras (e.g., visualizar apenas os resultados de uma determinada classificação qualitativa, visualizar apenas os resultados num determinado período, visualizar os resultados ignorando a classificação qualitativa «M», etc.). Adicionalmente, o sítio disponibiliza ligações para manuais e guias de configuração e outras ligações de referência, bem como hiperligações para todas as ferramentas utilizadas na sua construção. Uma vez que os dados individuais de cada sítio Web só podem ser divulgados para motivos de investigação (Qualys, Inc, 2015d, Capítulo Terms and Conditions), o sítio «Web Pública» disponibiliza também um formulário que permite a investigadores obter (mediante pedido) os dados recolhidos e os *scripts* criados para processar e agregar os dados dos testes efetuados.

Após o término deste estudo, este sítio Web continuará disponível e servirá para se efetuar análises regulares da segurança das comunicações dos sítios Web registados na sua base de dados. Estas análises regulares irão permitir obter uma perspetiva evolutiva da encriptação de comunicações nesses sítios Web. Esta plataforma poderá, caso surja interesse, estender-se a outros objetos de análise, tais como a segurança do DNS, a acessibilidade, entre outros.

[7] Para a construção deste sítio Web foi utilizada a ferramenta em código aberto Joomla (Open Source Matters, Inc, s.d.).

IV. Resultados

1. Nível de Segurança de Comunicações

De forma a obter os resultados do nível de segurança de comunicações dos 84 sítios Web analisados, é necessário identificar quais os sítios Web que disponibilizam encriptação através de HTTPS. No entanto, disponibilizar encriptação não significa que esta seja disponibilizada de forma adequada. Nesse sentido, é importante verificar a correspondência do certificado com o nome de domínio do sítio Web e a qualidade da encriptação fornecida, utilizando, para esse efeito, os resultados da classificação qualitativa (Tabela 20).

Tabela 22
Sítios Web por classificação qualitativa.

Designação	Classificação qualitativa	Quantidade	Percentagem
Disponibiliza encriptação	A+ a F, T e M	67	79,76 %
Certificado corresponde	A+ a F e T	33	39,28 %
Classificação qualitativa A+	A+	0	0,00 %
Classificação qualitativa A	A	3	3,57 %
Classificação qualitativa A-	A-	0	0,00 %
Classificação qualitativa B	B	5	5,95 %
Classificação qualitativa C	C	23	27,38 %
Classificação qualitativa D	D	0	0,00 %
Classificação qualitativa E	E	0	0,00 %
Classificação qualitativa F	F	0	0,00 %
Classificação qualitativa T	T	2	2,38 %
Certificado não corresponde	M	34	40,48 %
Não disponibiliza encriptação	N	17	20,24 %
Total	-	84	100,00 %

Conforme demonstra a Tabela 22, 79,76 % dos sítios Web permitem estabelecer comunicações encriptadas e 20,24 % não o permitem. No entanto, verifica-se que, em 40,48 % dos sítios, o certificado não corresponde ao nome de domínio do sítio Web. Observa-se então que, do total de 84 sítios Web, apenas 33 sítios Web (39,28 %) disponibilizam comunicações encriptadas com certificado correspondente com o nome de domínio do sítio Web. As classificações qualitativas desses 33 sítios Web são distribuídas da seguinte forma: 3,57% tiveram classificação A, 5,95 % tiveram classificação B, 27,38 % tiveram classificação C e 2,38 % tiveram classificação T.

Se, de acordo com o definido na Tabela 21, se agrupar os sítios Web pelas suas classificações qualitativas obtém-se os resultados do nível de segurança de comunicações.

Tabela 23

Sítios Web por nível de segurança de comunicações.

Nível de segurança de comunicações	Quantidade	Percentagem
Seguro	3	3,57 %
Razoavelmente seguro	28	33,33 %
Pouco seguro	0	0,00 %
Inseguro	53	63,10 %
Total	84	100,00 %

Relativamente ao nível de segurança de comunicações (Tabela 23), conclui-se que, do total dos 84 sítios Web analisados, apenas 3,57 % são considerados seguros, 33,33 % razoavelmente seguros e os restantes 63,10 % inseguros.

2. Cumprimento de Recomendações

Tendo em vista não desvirtuar os resultados do cumprimento das recomendações, não são considerados os sítios Web com certificado que não corresponde ao nome de domínio do sítio Web. Essa opção é tomada dado este ser um problema recorrente na instalação de servidores, pelo facto de os administradores de sistemas deixarem os servidores configurados por omissão com o HTTPS ativo, mas sem que este seja utilizado ou sem que seja comunicado ao público o endereço HTTPS do sítio Web[1]. Dado que os navegadores alertam com um aviso bastante claro, não é aceitável que uma organização de cariz público apresente este aviso aos cidadãos ou organizações no seu sítio Web. Também não são considerados os servidores dos sítios Web que não fornecem encriptação.

Assim, para efeitos de resultados do cumprimento das recomendações, é considerado como universo estatístico o conjunto dos 33 sítios Web (39,28 % do total) que permitem encriptação e cujo certificado corresponde ao nome de domínio do sítio.

Tabela 24

Sítios Web que cumprem as recomendações.

Recomendação	Quantidade	Percentagem
Estado português	29	87,88 %
NIST	3	9,09 %
ENISA	0	0,00 %
NSA	0	0,00 %
Do estudo	3	9,09 %

[1] Por vezes, ao ser replicado um determinado servidor de publicação Web, o certificado do antigo nome de domínio e a correspondente chave privada é deixada no servidor. Além de constituir uma grave falha de segurança para os donos dos servidores replicados, esse certificado não corresponde ao nome de domínio do atual sítio Web. Outro caso possível é, na utilização de múltiplos sítios Web com nomes de domínio diferentes no mesmo servidor Web, técnica designada por hospedagem virtual (*virtual hosting*), se utilizar um certificado que, embora válido, não corresponde ao nome de domínio do sítio Web.

Por organização, verifica-se que as recomendações do Estado português são cumpridas por 87,88 % dos sítios Web, as recomendações do NIST são cumpridas por apenas 9,09 % e nenhum cumpre as recomendações da ENISA ou da NSA. Relativamente às recomendações do estudo (Tabela 15), verifica-se que apenas 9,09 % dos sítios Web estão em conformidade com as mesmas.

3. Qualidade da Encriptação

Tal como para os resultados do cumprimento das recomendações, para os resultados da qualidade da encriptação é considerado como universo estatístico o conjunto dos 33 sítios Web (39,28 % do total) que permitem encriptação e o certificado corresponde ao nome de domínio do sítio Web.

3.1. Certificado e cadeia de confiança.

Foram obtidos resultados relativos ao algoritmo e à força da chave do certificado, à função de dispersão utilizada na assinatura do certificado, aos mecanismos de verificação da revogação disponibilizados pelo certificado, à validade da cadeia de confiança e identificação da CA emissora do certificado.

Tabela 25
Sítios Web por algoritmo utilizado e força da chave do certificado.

Algoritmo utilizado e força da chave	Quantidade	Percentagem
RSA/2048	32	96,97 %
ECDSA/256	1	3,03 %
Total	33	100,00 %

Relativamente ao algoritmo e força da chave do certificado (Tabela 25), observa-se que 96,97 % dos sítios Web utilizam certificados RSA com força de 2048 bit e 3,03 % certificados ECDSA com curvas elípticas de 256 bit. Nenhum utiliza certificados DSS[2].

Tabela 26
Sítios Web por função de dispersão e força da assinatura do certificado.

Função de dispersão e força da assinatura	Quantidade	Percentagem
SHA-2/384	0	0,00 %
SHA-2/256	32	96,97 %
SHA-1	1	3,03 %
MD5	0	0,00 %

[2] Os certificados DSS utilizam o algoritmo DSA.

Função de dispersão e força da assinatura	Quantidade	Percentagem
Total	33	100,00 %

Ao nível da função de dispersão utilizada na assinatura do certificado (Tabela 26), verifica-se que 96,97 % utilizam o SHA-2/256 e apenas 3,03 % utilizam o SHA-1. O SHA-2/384 e o MD5 não são utilizados.

Tabela 27

Sítios Web por mecanismo de verificação de revogação de certificado.

Mecanismo de verificação de revogação	Quantidade	Percentagem
OCSP e CRL	33	100,00 %
Apenas OCSP	0	0,00 %
Apenas CRL	0	0,00 %
Total	33	100,00 %

Relativamente aos mecanismos de verificação da revogação do certificado utilizados (Tabela 27), todos os sítios Web analisados permitem utilizar tanto o OCSP como o CRL.

Tabela 28

Sítios Web por validade da cadeia de confiança do certificado.

Validade da cadeia de confiança	Quantidade	Percentagem
Cadeia de confiança válida	31	93,90 %
Cadeia de confiança inválida	2	6,10 %
Total	33	100,00 %

Relativamente à cadeia de confiança dos certificados (Tabela 28), observa-se que 93,90 % dos sítios Web disponibilizam a cadeia de confiança válida e que, por conseguinte, 6,10 % não disponibilizam a cadeia de confiança válida.

Tabela 29

Sítios Web por CA emissora do certificado.

CA emissora	Quantidade	Percentagem
ECCE	26	78,79 %
Google Internet Authority G2	3	9,09 %
Go Daddy Secure Certificate Authority - G2	1	3,03 %
GlobalSign Organization Validation CA - G2	1	3,03 %
COMODO RSA Domain Validation Secure Server CA	1	3,03 %
COMODO ECC Domain Validation Secure Server CA	1	3,03 %
Total	33	100,00 %

Ao nível da CA emissora (Tabela 29), verifica-se que em 78,79 % dos sítios Web é a «ECCE». Outras cinco são utilizadas: a «Google Internet Authority G2» em 9,09 % dos sítios e, as restantes, cada uma delas em 3,03 % dos sítios.

3.2. Utilização de protocolos.

Foram obtidos resultados relativos aos protocolos de encriptação que os sítios Web disponibilizam. De realçar que, de modo a suportar vários clientes, os sítios podem disponibilizar vários protocolos, pelo que os resultados são apresentados de forma individual e agrupada.

Tabela 30
Sítios Web por protocolo disponibilizado.

Protocolo/Versão	Quantidade	Percentagem
TLS 1.2	8	24,24 %
TLS 1.1	8	24,24 %
TLS 1.0	33	100,00 %
SSL 3.0	4	12,12 %
SSL 2.0	1	3,03 %

Individualmente (Tabela 30), verifica-se que 24,24 % dos sítios Web disponibilizam TLS 1.2, 24,24 % disponibilizam TLS 1.1, todos disponibilizam TLS 1.0, 12,12 % disponibilizam SSL 3.0 e 3,03 % disponibilizam SSL 2.0.

Tabela 31
Sítios Web por grupo de protocolos disponibilizados.

Grupo de protocolo/Versões	Quantidade	Percentagem
TLS 1.1 ou superior	0	0,00 %
TLS 1.0 ou superior	5	15,15 %
Exclusivamente TLS 1.0	24	72,73 %
TLS 1.0 ou superior e SSL 2.0 ou superior	4	12,12 %
SSL 2.0 ou superior	0	0,00 %
Total	33	100,00 %

De forma agrupada (Tabela 31), observa-se que 15,15 % disponibilizam TLS 1.0 ou superior, 72,73 % disponibilizam exclusivamente TLS 1.0 e 12,12 % disponibilizam TLS 1.0 ou superior e SSL 2.0 ou superior. Nenhum disponibiliza apenas TLS 1.1 ou superior assim como nenhum disponibiliza apenas SSL 2.0 ou superior.

3.3. Suporte de sigilo persistente.

Tanto o FS como o PFS dependem de o servidor disponibilizar especificações de cifra que utilizem algoritmos DH (DH, DHE, ECDH ou ECDHE) na troca de chaves. Assim, como é importante realçar que, devido a questões de compatibilidade, um servidor suportar o FS ou

o PFS não significa que o suporte com todos os clientes, i.e., com todos os navegadores utilizados para aceder ao sítio Web. Nesse sentido, é necessário dividir o suporte ao FS ou ao PFS por níveis de suporte.

Tabela 32
Sítios Web por nível de suporte a sigilo persistente[3].

Nível de suporte	Quantidade	Percentagem
Robusto (suporta com todos os navegadores)	2	6,06 %
Moderno (suporta com todos os navegadores recentes)	6	18,18 %
Básico (suporta com pelo menos um navegador)	1	3,03 %
Não suporta	24	72,73 %
Total	33	100,00 %

Pela Tabela 32 verifica-se que 6,06 % dos sítios Web suportam o FS ou o PFS com todos os navegadores, 18,18 % suportam nas versões mais recentes dos navegadores, 3,03 % suportam em pelo menos um navegador e 72,73 % não suportam em nenhum navegador.

3.4. Proteção contra vulnerabilidades conhecidas.

A Tabela 33 apresenta os resultados da capacidade dos sítios Web de fornecerem proteção contra vulnerabilidades conhecidas ao nível de encriptação de comunicações.

Tabela 33
Sítios Web protegidos contra vulnerabilidades conhecidas.

Vulnerabilidade	Quantidade	Percentagem
De implementação		
Heartbleed	33	100,00 %
OpenSSL CCS Injection	32	96,97 %
Nos protocolos		
Insecure Renegotiation	33	100,00 %
BEAST	3	9,09 %
CRIME	33	100,00 %
Lucky Thirteen	3	9,09 %
BREACH	33	100,00 %
Triple Handshake	32	96,97 %
POODLE	33	100,00 %
POODLE TLS	33	100,00 %
FREAK	31	93,94 %
Logjam	32	96,97 %
Nos algoritmos de cifra e funções de dispersão		
Utilização de DES	31	93,94 %
Utilização de MD5	27	81,82 %
Utilização de RC4	28	84,85 %
Utilização de SHA-1	2	6,06 %

[3] Os dados obtidos não fazem distinção entre FS e PFS.

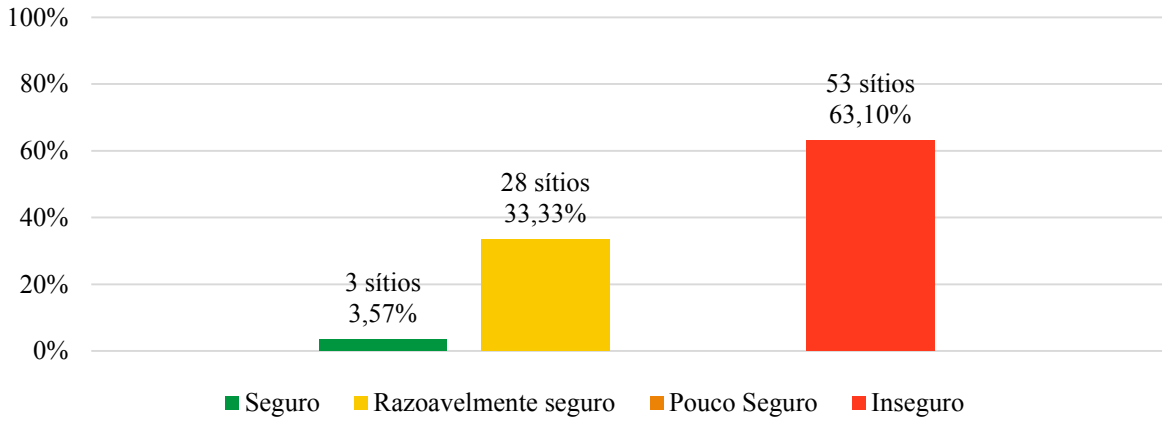
V. Discussão

1. Análise dos Resultados

1.1. Nível de segurança de comunicações.

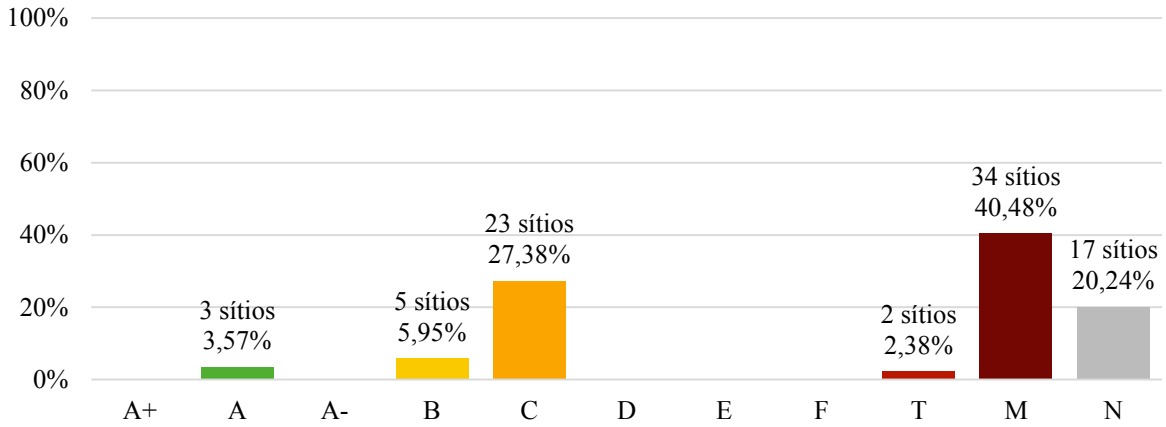
Da análise dos resultados sobressai que, dos 84 sítios web analisados, perto de dois terços (63,10 %, 53 sítios Web) disponibiliza comunicações de forma insegura e apenas uma pequena parte (3,57 %, 3 sítios Web) disponibiliza comunicações de forma considerada segura. Exatamente um terço (33,33 %, 28 sítios Web) disponibiliza comunicações de forma considerada razoavelmente segura.

Figura 12
Sítios Web por nível de segurança de comunicações.



Para identificar as causas destes resultados, serão necessários os resultados da avaliação qualitativa apresentados na Figura 13.

Figura 13
Sítios Web por classificação qualitativa.



1.1.1. Comunicações seguras.

As classificações mais elevadas foram obtidas por sítios Web que têm as comunicações encriptadas corretamente configuradas (classificações A+, A e A-, 3,57 %, 3 sítios Web) e correspondem aos sítios Web considerados seguros a este nível[1]. A configuração destes sítios Web foi bem realizada e demonstra um elevado conhecimento na matéria por parte de quem a efetuou. Conclui-se que as comunicações através de HTTPS destes sítios Web são consideradas seguras, pois estão protegidas contra a grande maioria das vulnerabilidades e encontram-se em conformidade com as recomendações do estudo.

1.1.2. Comunicações razoavelmente seguras.

As configurações dos sítios Web com comunicações razoavelmente seguras (classificações B e C, 33,33 %, 28 sítios Web), revelam que existiu a preocupação de colocar os sítios Web a comunicar de forma segura. Se houve essa preocupação, porque não estão estes sítios Web configurados de forma a serem totalmente seguros?

Pelo que se observa, dos sítios Web que obtiveram classificação B (5,95 %, 5 sítios Web), três deles suportam o protocolo SSL 3.0 e os outros dois suportam a utilização de especificação de cifras não recomendadas[2]. Estes sítios Web, mediante ligeiras correções na configuração dos servidores de publicação Web, poderiam apresentar um nível de segurança de comunicações considerado seguro.

Caso diferente é o dos sítios que obtiveram classificação C (27,38 %, 23 sítios Web), que não permitem a utilização do protocolo TLS 1.2, nem disponibilizam especificações de cifra que permitem o FS ou o PFS[3]. Isto indicia que estes sítios Web utilizam sistemas de publicação Web obsoletos. Este é um problema frequentemente observado na configuração de comunicações encriptadas e que se deve ao facto de sistemas de publicação Web antigos poderem não suportar protocolos ou especificações de cifra mais recentes[4]. Muitas vezes a única operação viável é, dentro do possível, corrigir as vulnerabilidades e desativar protocolos e especificações de cifra vulneráveis até que o equipamento seja substituído por outro mais atual. Esta questão é pertinente, pois demonstra que a disponibilidade de recursos financeiros para investimento e

[1] Os resultados individuais para uma classificação qualitativa podem ser obtidos através dos filtros disponibilizados no sítio Web «Web Pública». Para a classificação qualitativa A estão acessíveis em https://webpublica.pt/res/2015/08/nto=A/.
[2] Os resultados individuais para a classificação qualitativa B estão acessíveis em https://webpublica.pt/res/2015/08/nto=B/.
[3] Os resultados individuais para a classificação qualitativa C estão acessíveis em https://webpublica.pt/res/2015/08/nto=C/.
[4] Alguns exemplos de sistemas de publicação Web que não suportam o TLS 1.2, o FS e o PFS são o Microsoft Internet Security and Acceleration Server 2006 e Microsoft Internet Information Services 6 (Zoller, 2011).

a duração dos procedimentos de aquisição de sistemas informáticos na administração pública pode ter impacto na segurança de comunicações dos sítios Web.

1.1.3. Comunicações pouco seguras.

Nenhum sítio Web obteve classificações D ou E.

1.1.4. Comunicações inseguras.

Nenhum sítio obteve classificação F. Contudo, uma pequena percentagem dos sítios Web, apesar de ter certificados corretos, apresenta problemas de confiança no certificado ou na cadeia de confiança (classificação T, 2,38 %, 2 sítios Web). Normalmente esta situação deve-se à utilização de cadeias de certificação incorretas ou à utilização de um certificado de uma CA de raiz que está em processo de descontinuação[5]. Se não fosse a falta de confiança, seria atribuída aos dois sítios a classificação F, i.e., continuariam a ser considerados inseguros[6]. Assim, podemos concluir que esta classificação revela que a configuração de comunicações encriptadas destes sítios Web foi realizada com muito pouco conhecimento sobre o funcionamento da cadeia de confiança, protocolos, cifras e vulnerabilidades, e sem terem sido efetuados os testes adequados.

Bastante elevada é a percentagem de sítios Web que, embora permitam comunicações encriptadas, não têm sequer correspondência entre o certificado e o nome de domínio do sítio Web (classificação M, 40,48 %, 34 sítios Web). Seria de esperar que a restante configuração destes servidores fosse insegura, mas na realidade, não é o que acontece. Se se ignorar os problemas com o certificado, três destes sítios Web seriam seguros (classificação A), 19 seriam razoavelmente seguros (13 sítios Web com classificação B e 6 com classificação C) e apenas 12 seriam inseguros (classificação F)[7]. Estes resultados parecem indicar que a maioria dos sítios Web em causa utiliza servidores de publicação Web recentes e relativamente atualizados que, por isso, têm configurações por omissão razoavelmente seguras.

---

[5] Apesar das cadeias poderem estar incorretas pode não aparecer o aviso nos navegadores pelo facto de os certificados da cadeia estarem instalados no dispositivo cliente. A título de exemplo, um dado sítio Web tem a cadeia de confiança «Baltimore CyberTrust Root» → «ECRaizEstado» → «ECCE» → «dominio.tld» e não envia o certificado «ECRaizEstado». Se o certificado «ECRaizEstado» estiver instalado no dispositivo do cliente (e.g., por ter a aplicação do Cartão de Cidadão instalada), então, uma vez que o cliente consegue reconstruir a cadeia de confiança, a cadeia de confiança será considerada como válida.
Os certificados de raiz de 1024 bit estão em processo de descontinuação (e.g., o «GTE CyberTrust Global Root»). Os sistemas operativos e navegadores ainda podem permitir a sua utilização por algum tempo e por isso não aparece a mensagem de aviso.

[6] A classificação qualitativa T pode não ser atribuída, i.e., ignorada através da utilização dos filtros. Os resultados com a classificação T ignorada podem ser obtidos em https://webpublica.pt/res/2015/08/ign=1/.

[7] A classificação qualitativa M pode não ser atribuída, i.e., ignorada através da utilização dos filtros. Os resultados com a classificação M ignorada podem ser obtidos em https://webpublica.pt/res/2015/08/ign=2/.

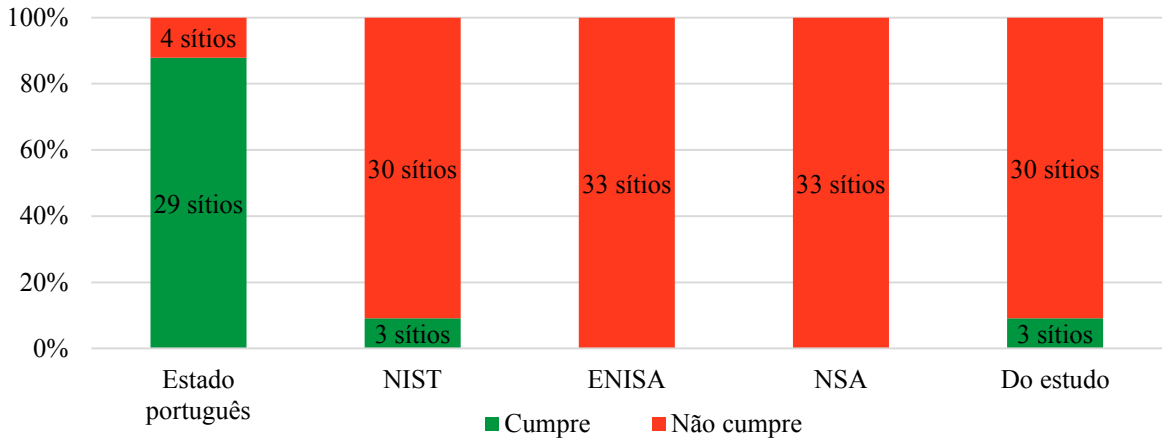
Por fim, temos os sítios Web que não permitem estabelecer comunicações encriptadas (classificação N, 20,24 %, 17 sítios Web), i.e., o HTTPS não está ativo e, por isso, apenas disponibilizam o sítio Web através de HTTP. Esta situação pode-se dever a dois motivos: haver claramente uma opção de não permitir a utilização de HTTPS ou os equipamentos de rede do sítio Web não permitirem a comunicação através da porta 443, utilizada pelo HTTPS. Dada a natureza dos sítios Web, que normalmente têm perfis de edição e de administração do sítio (disponíveis através de autenticação), deveria existir sempre, no mínimo, comunicações encriptadas durante e após a autenticação.

1.2. Recomendações de segurança.

Como referido no Capítulo IV «Resultados», ao nível do cumprimento de recomendações de segurança de comunicações, apenas se considera como universo estatístico os sítios Web que fornecem comunicações encriptadas com certificado corresponde ao nome de domínio do sítio Web (classificações A+ a F e T, 33 sítios Web). Os restantes sítios Web (classificações M e N, 51 sítios Web) claramente não as cumprem, pelos motivos já descritos anteriormente.

Figura 14

Sítios Web com certificado correto por cumprimento de recomendações.



Observa-se que apenas uma pequena percentagem (9,09 %, 3 sítios Web) cumpre as recomendações do estudo (Tabela 15). Estes sítios Web correspondem aos sítios Web que tiveram classificação A e que foram considerados com o nível de segurança seguro.

Para melhor perceber o motivo, é relevante analisar se estes sítios Web cumprem, ao nível de algoritmos de autenticação, troca de chaves, protocolos e especificações de cifra, as recomendações, de forma individual, de cada organização.

1.2.1. Estado português.

Conforme referido anteriormente, o RNID preconiza a utilização do protocolo TLS 1.0 como obrigatória. Dos resultados pode inferir-se que a maioria (87,88 %, 29 sítios Web) cumpre o RNID. Apenas quatro sítios Web não cumprem a legislação em vigor, por permitirem a utilização do protocolo SSL 3.0 ou inferior.

É importante ressalvar que o RNID, nesta matéria, revela-se muito pouco exigente e se encontra desatualizado. Seria importante haver maior detalhe e atualização de forma a estar em sincronia com as recomendações internacionais.

1.2.2. NIST.

O NIST é mais exigente nas suas recomendações. Além dos protocolos a utilizar, recomenda também os algoritmos a ser utilizados para a autenticação, troca de chaves, cifra e as funções de dispersão a utilizar para obter o MAC. Devido ao aumento do nível de exigência, apenas um pequena percentagem (9,09 %, 3 sítios Web) cumpre as suas recomendações. Como seria de esperar, estes são os mesmos sítios Web que têm classificação A, que atingem o nível seguro e que cumprem as recomendações do estudo (Tabela 15).

Verifica-se que o facto de alguns sítios Web não disponibilizarem protocolos mais recentes (TLS 1.2 e TLS 1.1), continuarem a disponibilizar protocolos antigos e inseguros (SSL 3.0 ou SSL 2.0) e permitirem a utilização de determinadas cifras, algumas das quais com vulnerabilidades conhecidas (e.g., RC4), é um enorme entrave ao cumprimento das recomendações e à encriptação de comunicações de forma efetivamente segura.

1.2.3. ENISA.

A ENISA aumenta ainda mais o nível de exigência, uma vez que não permite a utilização de cifras em modo CBC, não permite a utilização o SHA-1 como função de dispersão utilizada para obter o MAC e apenas permite troca de chaves com PFS (através do DHE ou ECDHE). Por essa razão, nenhum dos sítios Web em análise cumpre as suas recomendações.

O que justifica que os três sítios Web considerados seguros não cumpram as recomendações da ENISA? A resposta é relativamente simples: retrocompatibilidade. Estes sítios Web disponibilizam cifras em modo CBC e utilizam o SHA-1 como função de dispersão utilizada para obter o MAC. Fazem-no de forma a garantir que os sítios Web funcionam em dispositivos mais antigos que não suportam os novos modos de operação CCM e GCM e a função de dispersão SHA-2. Uma vez que nem todos os dispositivos mais antigos aceitam a utilização do

algoritmo DHE (ou ECDHE) na troca de chaves, a mesma questão se aplica em relação à troca de chaves com PFS.

Conclui-se que as recomendações da ENISA são aplicáveis em sistemas internos ou em ambiente controlado. Se os sítios Web implementassem todas as recomendações da ENISA, todos os dispositivos com Windows Vista, Android 4.3 e iOS 8 ou versões inferiores destes sistemas operativos (cf. Tabela 13) ficariam sem acesso, i.e., uma parte muito significativa dos utilizadores não poderia aceder aos sítios Web[8].

Porque motivo da ENISA, ao contrário do NIST, não recomenda a utilização do modo CBC, nem a utilização da função de dispersão SHA-1 e recomenda a utilização do PFS? A resposta está nas vulnerabilidades detetadas no modo CBC (vulnerabilidades BEAST e Lucky Thirteen), na vulnerabilidade teórica do SHA-1 e no próprio conceito do PFS, cuja não existência é, em si mesma, uma vulnerabilidade.

1.2.4. NSA.

As recomendações da NSA são as mais rigorosas de todas as organizações, muito embora, ao contrário da ENISA, e no seu perfil transitório de compatibilidade, permita a utilização do modo CBC e do SHA-1. Tal como a ENISA, a NSA obriga à troca de chaves com PFS mas apenas recorrendo a curvas elípticas (através do ECDHE). Ainda mais exigente, tendo em consideração que nem todas as CA emitem certificados ECDSA, é não permitir a utilização de certificados RSA, permitindo apenas e exclusivamente a utilização de ECDSA. Por estes motivos, nenhum dos sítios Web estudados cumpre estas recomendações.

Assim, tal como no caso da ENISA, conclui-se que as recomendações da NSA são extremamente exigentes em termos de segurança e aplicáveis em sistemas internos ou em ambiente controlado. Se os sítios Web implementassem todas as recomendações da NSA, todos os dispositivos com Windows XP e Android 2.3 ou versões inferiores destes sistemas operativos (cf. Tabela 13) ficariam sem acesso, i.e., uma parte significativa dos utilizadores não podiam aceder aos sítios Web[9].

[8] Em junho de 2015 entre 3,88 % e 16,32 % dos dispositivos utilizados no acesso à Internet utilizaram o Windows XP, entre 1,14 % e 2,04 % utilizaram o Windows Vista, entre 12,62 % e 25,63 % utilizaram as várias versões do Android e entre 11,37 % e 30,50 % utilizaram as várias versões do iOS («Usage share of operating systems», 2015).
[9] Em junho de 2015 entre 3,88 % e 16,32 % dos dispositivos utilizados no acesso à Internet utilizaram o Windows XP e entre 12,62 % e 25,63 % utilizaram as várias versões do Android («Usage share of operating systems», 2015).

1.3. Utilização de certificados.

Uma vez que a ECCE emite certificados gratuitos para organismos do Estado, é particularmente relevante analisar que sítios Web utilizam certificados emitidos pela ECCE. Neste aspeto, os resultados são particularmente interessantes. Verifica-se que, dos 33 sítios Web que fornecem comunicações encriptadas com certificado correto (classificações A+ a F e T), a maioria (78,79 %, 26 sítios Web) utiliza certificados emitidos pela ECCE.

As CA emissoras dos certificados dos 7 sítios Web que não utilizam a ECCE como CA emissora são variadas, mas nenhuma delas é, para este efeito, de cariz gratuito[10]. Verifica-se que, no caso de 4 destes 7 sítios Web, o nome de domínio é, na realidade, um subdomínio dos serviços Wordpress ou Blogger, pelo que utilizam os certificados globais da Wordpress e da Google, os certificados multidomínio «*.wordpress.com» e «*.googleusercontent.com» respetivamente, não tendo por isso custos associados[11].

Embora os resultados sejam animadores, coloca-se a questão de saber porque é que os restantes três sítios Web não utilizam certificados emitidos pela ECCE e, dessa forma, estão a incorrer em custos desnecessários para o erário público. Embora existam alguns aspetos relativamente aos certificados emitidos pela ECCE que poderiam ser melhorados no futuro (nomeadamente emitir certificados por mais de um ano, disponibilizar uma ferramenta Web para facilitar o processo de geração de certificados, ter a cadeia de confiança completa em SHA-2 e emitir certificados ECDSA), é possível ter um sítio Web seguro utilizando os certificados emitidos pela ECCE[12]. Depreende-se que o único motivo plausível será o desconhecimento de que a ECCE emite estes certificados gratuitamente.

Outra questão relevante é se os certificados emitidos pela ECCE são realmente confiáveis ao nível de soberania nacional. Ao contrário do que acontece noutros países (e.g., Países Baixos, Japão, Turquia, França) ou até regiões (e.g., Catalunha, Valência) (Mozilla Foundation, 2015a), a ECCE não é uma CA de raiz, i.e., depende de uma CA de raiz localizada noutro país para ter o seu certificado principal assinado, neste caso, a Baltimore[13]. Deste modo, qualquer problema que ocorra na CA de raiz, que está fora do controlo do Estado português, propagar-se-á a todos os sítios Web do Estado português que utilizam a ECCE como CA emissora. Embora pouco

[10] Como a Terena para o caso das universidades.
[11] O Wordpress e o Blogger são serviços gratuitos para publicação de blogues na Web.
Nos certificados multidomínio, o «*.» significa que todos os subdomínios do nome de domínio estão no âmbito do certificado.
[12] É internacionalmente recomendado que todos os certificados sejam assinados, no mínimo, com SHA-2/256. Além das questões de segurança associadas, este problema faz com que nos navegadores mais atuais o símbolo do HTTPS na barra de endereços apareça com um aviso amarelo ou vermelho.
[13] A ECCE é responsável, no âmbito do SCEE, pelos certificados intermédios «ECRaizEstado» e «ECCE». A Baltimore é responsável pelo certificado «Baltimore CyberTrust Root».

provável, a acontecer tal situação, as consequências seriam desastrosas. Adicionalmente, tendo a cadeia de confiança o seu início numa entidade de outro país, levanta questões ao nível de soberania nacional e sobre a proteção dos dados dos cidadãos e organizações pelo Estado português.

1.4. Vulnerabilidades.

Observa-se que a maioria dos sítios Web em análise neste estudo encontra-se protegida da maioria das vulnerabilidades. No entanto, praticamente todos os sítios Web estão vulneráveis aos ataques BEAST e ao Lucky Thirteen, pois permitem, por questões de retrocompatibilidade, a utilização do modo CBC no processo de encriptação em massa. Mais preocupante é os resultados demonstrarem que alguns sítios Web ainda permitem a utilização do algoritmo de encriptação em massa DES, ou permitem a utilização da função de dispersão MD5 como mecanismo de autenticação. Esta situação denota fraco conhecimento na configuração das comunicações encriptadas destes sítios Web. Uma vez que os sistemas mais atualizados removeram a utilização desses algoritmos nas suas definições por omissão, revela também que existem sistemas muito desatualizados.

2. Recomendações

Dado o espaço de tempo necessário para implementar alterações em sistemas com elevada complexidade e de grande dimensão como são os do Estado português, as recomendações deste estudo são divididas em três fases: curto, médio e longo prazo.

No curto prazo é recomendável que os sistemas de publicação Web sejam atualizados e que seja efetuada uma revisão das suas configurações. A publicação de um sítio Web com manuais, guias e boas práticas do conhecimento de todos os organismos do Estado é também uma medida recomendada. Aumentar o período de validade dos certificados da ECCE para um máximo de 3 a 5 anos, ter a cadeia de confiança assinada com SHA-2/256, iniciar o processo de assinatura de certificados ECDSA/256 e disponibilizar um formulário em linha para agilizar o processo de criação de certificados, como, de resto, muitas CA emissoras atualmente o fazem, permitiria agilizar todo o processo de emissão de certificados. Para reduzir custos ao erário público, a utilização de certificados emitidos pela ECCE para sítios Web do Estado português deveria ser obrigatória por lei.

A médio prazo é recomendável que sejam efetuadas ações de informação dos gestores TIC do Estado de forma a sensibilizá-los para o tema das comunicações seguras nos sítios Web.

No mesmo sentido, recomenda-se ações de formação aos administradores de sistemas de forma a treiná-los para a utilização das comunicações seguras nos sítios Web. Ao nível de legislação nacional é recomendável que seja publicada uma nova versão do RNID para o tornar mais adaptado às circunstâncias atuais. Ao nível de comunicações seguras nos sítios Web, a nova versão deverá contemplar os algoritmos, forças e as especificações de cifras que podem ser utilizadas. Em alternativa, de forma a facilitar o processo legislativo, deve remeter para as recomendações internacionais ou para uma organização do Estado (e.g., CNCS) que seja responsável pela atualização dessas recomendações. A introdução da obrigatoriedade ou recomendação de encriptação por tipologia de sítio Web também é importante. Sendo a segurança um processo contínuo, a implementação de um sistema que identifique todos os sítios Web do Estado português, os monitorize com periodicidade mensal e avise os responsáveis de problemas que, eventualmente, sejam detetados é também recomendada[14]. Uma maior utilização de sistemas em código aberto e gratuito, evitando processos de aquisição morosos que necessitam de disponibilidade financeira, facilitaria processos de atualização ou substituição de sistemas com falhas, permitindo uma melhoria contínua do nível segurança de comunicações.

Por fim, a longo prazo, recomenda-se a independência ao nível de CA de raiz, isto é, passar a ser do Estado português a CA de raiz que certifica todos os organismos do Estado. É no entanto, necessário ressalvar que este é um processo moroso e complexo que implica a negociação com fabricantes de forma a incluir a CA de raiz em sistemas operativos e aplicativos[15].

Dada a dimensão do Estado português, a implementação destas recomendações poderá, à primeira vista, parecer difícil. Contudo, é importante realçar que, a nível organizacional, o Estado português possui já entidades relevantes nesta matéria que poderiam levar a cabo este desafio com poucas alterações legislativas: a ECCE, o CNCS e a AMA.

[14] O autor disponibiliza-se a fornecer o sítio Web criado no âmbito deste estudo como protótipo.
[15] A título de exemplo, a Mozilla explica o processo para ser uma CA confiável pela Mozilla (Mozilla Foundation, 2015b).

VI. Conclusões

1. Conclusão

Perante a evolução da utilização da Internet e o crescente uso de plataformas de governo eletrónico é expectável que, com o passar do tempo, cada vez mais serviços passem a estar disponíveis em linha. Situação que conduzirá a que cada vez mais informação de cidadãos e de organizações circule pela Internet. Este estudo conclui que, apesar de ser clara a existência de algum esforço para tornar as comunicações seguras, muito ainda tem que ser feito para que a proteção dos dados e informações dos cidadãos e das organizações se generalize nas plataformas de governo eletrónico do Estado português.

No âmbito desta investigação delinearam-se planos de curto, médio e longo prazo que, a serem realizados, permitiriam a obtenção de um nível superior de maturidade de implementação de comunicações seguras. Através de ações de informação, de ações de formação, da implementação de sistemas em código aberto, de algumas alterações legislativas e da implementação de sistemas de monitorização e alerta de forma a permitir a verificação e melhoria contínua das comunicações encriptadas, seria possível garantir que os dados dos cidadãos e organizações fossem transmitidos de forma efetivamente segura através da Internet.

No entender do autor, este estudo e outros estudos de tema semelhante são da maior importância para contribuir para proteger os dados de cidadãos e organizações e para melhorar os serviços prestados através das plataformas de governo eletrónico. Se, no passado, era necessário entrar fisicamente nas instalações para aceder a esses dados, atualmente o cenário é diferente e a um atacante em qualquer parte do mundo basta, em muitos casos, um computador, ligação à Internet e algumas aplicações para aceder a esta informação. Assim, o Estado português tem de ter em consideração estas ameaças e proteger devidamente os seus sistemas a vários níveis, entre os quais disponibilizando comunicações, não só encriptadas, mas efetivamente seguras.

2. Limitações do Estudo e Trabalho Futuro

Embora todo o sistema de avaliação estivesse preparado para o efeito, apesar de inúmeros contactos com várias entidades públicas, não foi possível obter a autorização para a realização dos testes a todos os sítios Web do Estado, pelo que os testes tiveram de incidir sobre um número limitado de sítios Web. Seria importante o Estado português definir uma organização que fosse legalmente responsável por autorizar estudos deste género. Embora sejam questões de alguma sensibilidade que importa salvaguardar, estudos nesta matéria, além de permitirem ter

um panorama global dos sítios Web do Estado português, ainda contribuiriam para a melhoria da segurança das comunicações do Estado português e, com isso, para a proteção dos dados de todos os cidadãos e organizações que utilizam as plataformas de governo eletrónico do Estado português.

Não foi objetivo desta investigação determinar que sítios Web necessitam de autenticação do lado do cliente. No entanto, dada a crescente utilização do Cartão de Cidadão para autenticação Web, seria pertinente saber se essas comunicações estão a ser efetuadas de forma segura. Também relevante seria saber se a estratégia seguida pelo Estado português, no que diz respeito à utilização de autenticação eletrónica com o Cartão de Cidadão, é a mais adequada.

Nos anos 90, um sítio Web utilizava habitualmente um nome de domínio. Devido à crescente complexidade dos sítios Web, atualmente um sítio Web além de utilizar um nome de domínio (e.g., portaldasfinancas.pt) pode, para fornecer outro tipo de dados (e.g., ficheiros estáticos) ou segmentar a informação, utilizar múltiplos subdomínios do nome de domínio principal (e.g., static.portaldasfinancas.pt, info.portaldasfinancas.pt). Adicionalmente, alguns subdomínios podem corresponder a aplicações privadas de acesso e utilização restrita da organização (e.g., intranet.portaldasfinancas.pt, webmail.portaldasfinancas.pt). O protocolo DNS permite, através da obtenção do ficheiro de zona do DNS (DNS *zone file*), obter todos os subdomínios para um determinado nome de domínio. No entanto, o mesmo protocolo permite também restringir a obtenção desse ficheiro apenas a acessos autorizados (Mockapetris, 1987). Devido a esta limitação, apenas foram avaliados os sítios Web que utilizam o nome de domínio principal ou, em alternativa, que utilizam o subdomínio principal pelo qual se identificam (e.g., www.portaldasfinancas.pt).

Este estudo focou-se nas comunicações dos sítios Web disponibilizados pelo Estado na Internet. Outra investigação relevante seria a análise das comunicações encriptadas no sector privado, nomeadamente, na área financeira e na área da saúde. Conhecer se os dados dos cidadãos e organizações estão a ser devidamente protegidos nas comunicações com as plataformas disponibilizadas pelos bancos e pelos serviços de saúde na Internet seria importante.

Como referido, existem vários protocolos na Internet que são utilizados em diversos tipos de comunicação e que servem diferentes propósitos. Apesar de muitos sítios Web enviarem mensagens de correio eletrónico, a consulta de informação, a submissão e a visualização de dados, que são transmitidos através do protocolo HTTP, são, normalmente, o objetivo principal do sítio Web. Por questões de exequibilidade deste estudo, unicamente foram avaliadas as comunicações sobre o protocolo HTTP. Verificar se o envio de correio eletrónico, através do protocolo Simple Mail Transfer Protocol (SMTP) (Postel, 1982), entre o Estado português e as

organizações e cidadãos é efetuado de forma segura seria um estudo pertinente que complementaria os resultados deste estudo.

A resolução de um determinado nome de domínio no seu IP é uma componente importante da comunicação na Internet. Esta resolução usualmente precede a comunicação que ocorre usando os protocolos referidos neste estudo, tanto nas suas versões encriptadas, como nas não encriptadas. A resolução de nomes é efetuada através do protocolo DNS. Essa resolução coloca também questões de segurança que devem ser consideradas. Por esse motivo, a IETF desenhou extensões de segurança ao protocolo DNS designadas Domain Name System Security Extensions (DNSSEC) (Arends, Austein, Larson, Massey, & Rose, 2005). Conhecer o grau de implementação do DNSSEC nos sítios Web do Estado português seria um estudo interessante.

Num futuro próximo, seria pertinente verificar a utilização das normas que foram recentemente ou estão atualmente a ser desenvolvidas pelo TLS Working Group do IETF, em particular o HTTP Strict Transport Security (HSTS) (Hodges, Jackson, & Barth, 2012), o HTTP Public Key Pinning (HPKP) (Evans, Palmer, & Sleevi, 2015) e o TLS 1.3 (Rescorla, 2015a).

Por último, o sítio Web desenvolvido no âmbito deste estudo permite que, mediante autorização do autor, qualquer sítio Web possa ser introduzido e, assim, avaliado de forma periódica. Apesar do foco deste estudo ter sido os sítios Web do Estado, a forma como o sítio Web está construído permite a sua adaptação investigações análogas, pelo que, caso exista interesse, o autor se disponibiliza a anuir na utilização do sítio Web para o efeito, bem como em colaborar em futuras investigações.

Bibliografia

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., … Zimmermann, P. (2015, Maio). Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. Disponível em: https://goo.gl/q1fpxO

AlFardan, N. J., Bernstein, D. J., & Paterson, K. G. (2013). On the Security of RC4 in TLS and WPA. Apresentado na USENIX Security 2013. Disponível em: http://goo.gl/o0Npfs

AlFardan, N. J., & Paterson, K. G. (2013). Lucky Thirteen: Breaking the TLS and DTLS Record Protocols (pp. 526–540). Apresentado na Security and Privacy (SP), 2013 IEEE Symposium on, Berkeley, CA: IEEE. doi: 10.1109/SP.2013.42

Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). DNS Security Introduction and Requirements. RFC 4033. doi: 10.17487/RFC4033

Bahajji, Z. A., & Illyes, G. (2014, Agosto 6). HTTPS as a ranking signal. Disponível em: http://goo.gl/GGnrwJ

Barnes, R., Thomson, M., Pironti, A., & Langley, A. (2015). Deprecating Secure Sockets Layer Version 3.0. RFC 7568. doi: 10.17487/RFC7598

Baum, C., & Di Maio, A. (2000, Novembro 21). Gartner's Four Phases of E-Government Model. Gartner, Inc. Disponível em: https://goo.gl/r2jyL6

Berners-Lee, T. (2014, Março 11). Tim Berners-Lee: 25 years on, the Web still needs work (Q&A). Disponível em: http://goo.gl/P3R0Tg

Berners-Lee, T., Fielding, R. T., & Masinter, L. (2005). Uniform Resource Identifier (URI): Generic Syntax. RFC 3986. doi: 10.17487/RFC3986

Bernstein, D. J. (2008). ChaCha, a variant of Salsa20. Apresentado na SASC 2008: The State of the Art of Stream Ciphers, Workshop Record. Disponível em: http://goo.gl/nWtr1C

Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., Pironti, A., Strub, P.-Y., … Beurdouche, B. (2015, Março 3). State Machine AttACKs against TLS (SMACK TLS). Disponível em: https://goo.gl/8WK00i

Bhargavan, K., Lavaud, A. D., Fournet, C., Pironti, A., & Strub, P. Y. (2014). Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS. Em *2014 IEEE Symposium on Security and Privacy (SP)* (pp. 98–113). doi: 10.1109/SP.2014.14

Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., & Moeller, B. (2006). Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). RFC 4492. doi: 10.17487/RFC4492

Braden, R. (1989a). Requirements for Internet Hosts - Application and Support. RFC 1123. doi: 10.17487/RFC1123

Braden, R. (1989b). Requirements for Internet Hosts - Communication Layers. RFC 1122. doi: 10.17487/RFC1122

Comparison of TLS implementations. (2015, Agosto 24). Em *Wikipédia: a enciclopédia livre*. Disponível em: https://goo.gl/aQNuK8

Coursey, D., & Norris, D. F. (2008). Models of E-Government: Are They Correct? An Empirical Assessment. *Public Administration Review*, *68*(3), 523–536. doi: 10.1111/j.1540-6210.2008.00888.x

Crispin, M. (1994). Internet Message Access Protocol - Version 4. RFC 1730. doi: 10.17487/RFC1730

Day, J. D., & Zimmermann, H. (1983). The OSI reference model. *Proceedings of the IEEE*, *71*(12), 1334–1340. doi: 10.1109/PROC.1983.12775

Decreto-Lei n.º 73/2014 de 13 de maio. (2014). *Diário da República 1.ª Série, n.º 91/2014*. XIX Governo Constitucional. Lisboa.

Dierks, T., & Allen, C. (1999). The TLS Protocol Version 1.0. RFC 2246. doi: 10.17487/RFC2246

Dierks, T., & Rescorla, E. (2006). The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346. doi: 10.17487/RFC4346

Dierks, T., & Rescorla, E. (2008). The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246. doi: 10.17487/RFC5246

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. doi: 10.1109/TIT.1976.1055638

Direção-Geral da Administração e do Emprego Público. (s.d.a). SIOE Public Web Service. Acedido em: 25 de Agosto de 2015, em: http://goo.gl/7ZKdEs

Direção-Geral da Administração e do Emprego Público. (s.d.b). SIOE - Sistema de Informação da Organização do Estado. Acedido em: 25 de Agosto de 2015, em: http://goo.gl/5AjcFw

Duong, T., & Rizzo, J. (2011, Maio). *Here Come The ⊕ Ninjas*. Disponível em: http://goo.gl/Vsnp2e

Duong, T., & Rizzo, J. (2012, Setembro). *The CRIME Attack*. EKOparty Security Conference. Disponível em: http://goo.gl/AqApdv

Durumeric, Z., Kasten, J., Bailey, M., & Halderman, J. A. (2013). Analysis of the HTTPS Certificate Ecosystem. Em *Proceedings of the 2013 conference on Internet Measurement Conference* (p. 14). Barcelona, Espanha: ACM. doi: 10.1145/2504730.2504755

Edward Snowden. (2015, Agosto 24). Em *Wikipédia: a enciclopédia livre*. Disponível em: https://goo.gl/1XEJLf

Electronic Frontier Foundation. (2014). HTTPS Everywhere. Acedido em: 11 de Janeiro de 2015, em: https://www.eff.org/https-everywhere

Eurostat. (2014a, Dezembro 9). Enterprises using the internet for interacting with public authorities. Acedido em: 13 de Janeiro de 2015, em: http://goo.gl/QfHk3J

Eurostat. (2014b, Dezembro 16). Individuals using the internet for interacting with public authorities. Acedido em: 13 de Janeiro de 2015, em http://goo.gl/XL1tsn

Evans, C., Palmer, C., & Sleevi, R. (2015). Public Key Pinning Extension for HTTP. RFC 7469. doi: 10.17487/RFC7469

Fielding, R. T., Gettys, J., Mogul, J. C., Nielsen, H. F., Masinter, L., Leach, P. J., & Berners-Lee, T. (1999). Hypertext Transfer Protocol -- HTTP/1.1. RFC 2616. doi: 10.17487/RFC2616

Ford-Hutchinson, P. (2005). Securing FTP with TLS. RFC 4217. doi: 10.17487/RFC4217

Freier, A., Karlton, P., & Kocher, P. (2011). The Secure Sockets Layer (SSL) Protocol Version 3.0. RFC 6101. doi: 10.17487/RFC6101

Gambling with Secrets: Part 6/8 (Perfect Secrecy & Pseudorandomness). (2012a). Disponível em: https://youtu.be/FfZurPKYM2w

Gambling with Secrets: Part 7/8 (Diffie-Hellman Key Exchange). (2012b). Disponível em: https://youtu.be/6NcDVERzMGw

GeoCerts, Inc. (s.d.). GeoCerts SSL Checker. Acedido em: 25 de Agosto de 2015, em: https://goo.gl/AGQrrA

Giry, D. (2015, Fevereiro 26). Keylength - Compare all Methods. Acedido em: 25 de Agosto de 2015, em: http://goo.gl/gHlcNl

GlobalSign. (2015a, Julho 9). ECC Compatibility. Acedido em: 24 de Agosto de 2015, em: https://goo.gl/2XMT13

GlobalSign. (2015b, Julho 24). SHA-256 Compatibility. Acedido em: 24 de Agosto de 2015, em: https://goo.gl/2vHHEz

Gluck, Y., Harris, N., & Prado, A. (2013, Julho). *BREACH: Reviving the CRIME Attack*. Disponível em: http://goo.gl/7iHzXm

Google, Inc. (s.d.). The Go Project. Acedido em: 4 de Janeiro de 2015, em: https://goo.gl/ZK4w8S

Grigorenko, K. (2011, Dezembro 8). Using Wireshark to Decrypt WebSphere HTTPS/SSL/TLS Traffic [CT915]. Disponível em: https://goo.gl/XmkMdr

Grigorik, I. (2013). *High Performance Browser Networking: What Every Web Developer Should Know about Networking and Web Performance*. O'Reilly Media. Disponível em: http://goo.gl/8BJPgr

Grigorik, I., & Far, P. (2014, Junho). *HTTPS Everywhere*. Apresentado na Google I/O 2014, São Francisco, Estados Unidos da América. Disponível em: https://youtu.be/cBhZ6S0PFCY

Hiller, J. S., & Bélanger, F. (2001). Privacy Strategies for Electronic Government. *Washington DC: IBM Center for the Business of Government*, 35.

Hodges, J., Jackson, C., & Barth, A. (2012). HTTP Strict Transport Security (HSTS). RFC 6797. doi: 10.17487/RFC6797

Hoffman, P. (1999). SMTP Service Extension for Secure SMTP over TLS. RFC 2487. doi: 10.17487/RFC2487

Holden, S. H., Norris, D. F., & Fletcher, P. D. (2003). Electronic Government at the Local Level: Progress to Date and Future Issues. *Public Performance & Management Review*, *26*(4), 325–344.

Housley, R., Ford, W., Polk, W. T., & Solo, D. (1999). Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459. doi: 10.17487/RFC2459

Internet Engineering Task Force. (2015a, Janeiro 2). RFC Index. Acedido em: 3 de Janeiro de 2015, em: http://www.rfc-editor.org/rfc-index.html

Internet Engineering Task Force. (2015b, Agosto 24). Transport Layer Security (tls) - Documents. Acedido em: 24 de Agosto de 2015, em: https://goo.gl/hMCNeY

Internet Security Research Group. (2015). Let's Encrypt. Acedido em: 11 de Janeiro de 2015, em: https://letsencrypt.org/

ISO/IEC JTC 1. (1994). *ISO/IEC 7498-1:1994, Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model* (2nd Ed.). Genebra, Suiça. Disponível em: http://goo.gl/OmgAFn

Jeong, C. H. (2007). *Fundamental of Development Admistration*. Scholar Press.

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des sciences militaires*, *IX*, 5–83.

Khare, R., & Lawrence, S. (2000). Upgrading to TLS Within HTTP/1.1. RFC 2817. doi: 10.17487/RFC2817

Langley, A. (2014, Dezembro 8). The POODLE bites again. Disponível em: https://goo.gl/Irg7cs

Langley, A., Chang, W.-T., Mavrogiannopoulos, N., Strombergson, J., & Josefsson, S. (2015, Junho). The ChaCha20-Poly1305 AEAD Cipher for Transport Layer Security. Disponível em: https://tools.ietf.org/html/draft-ietf-tls-chacha20-poly1305-00

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly*, *18*(2), 122–136. doi: 10.1016/S0740-624X(01)00066-1

Lei n.º 36/2011 de 21 de junho. (2011). *Diário da República 1.ª Série, n.º 118/2012*. Assembleia da República. Lisboa.

Matsui, M. (1994). Linear Cryptanalysis Method for DES Cipher. Em T. Helleseth (Ed.), *Advances in Cryptology — EUROCRYPT '93* (pp. 386–397). Springer Berlin Heidelberg. Disponível em: http://link.springer.com/chapter/10.1007/3-540-48285-7_33

Mockapetris, P. (1987). Domain names - concepts and facilities. RFC 1034. doi: 10.17487/RFC1034

Möller, B., Duong, T., & Kotowicz, K. (2014, Setembro). This POODLE Bites: Exploiting The SSL 3.0 Fallback. Disponível em: https://goo.gl/3281dQ

Mozilla Foundation. (2015a, Agosto 6). Mozilla Included CA Certificate List. Acedido em: 25 de Agosto de 2015, em: https://goo.gl/eQWt5d

Mozilla Foundation. (2015b, Agosto 24). Mozilla CA Certificate Policy. Acedido em: 24 de Agosto de 2015, em: https://goo.gl/ubJ7C4

Myers, M., Ankney, R., Malpani, A., Galperin, S., & Adams, C. (1999). X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560. doi: 10.17487/RFC2560

National Institute of Standards and Technology. (2014a, Outubro 9). NIST Computer Security Publications - FIPS (Federal Infromation Processing Standards). Acedido em: 22 de Outubro de 2014, em: http://csrc.nist.gov/publications/PubsFIPS.html

National Institute of Standards and Technology. (2014b, Outubro 9). NIST Computer Security Publications - NIST Special Publications (SPs). Acedido em: 5 de Janeiro de 2015, em: http://csrc.nist.gov/publications/PubsSPs.html

Newman, C. (1999). Using TLS with IMAP, POP3 and ACAP. RFC 2595. doi: 10.17487/RFC2595

Nir, Y., & Langley, A. (2015). ChaCha20 and Poly1305 for IETF Protocols. RFC 7539. doi: 10.17487/RFC7539

Open Source Matters, Inc. (s.d.). What is Joomla? Acedido em: 4 de Janeiro de 2015, em: http://goo.gl/mZY8AU

OpenSSL Software Foundation. (s.d.). OpenSSL Ciphers. Acedido em: 25 de Agosto de 2015, em: https://goo.gl/g8utR6

Organização das Nações Unidas. (2015). EGOVKB | United Nations > Data > Country Information. Acedido em: 12 de Janeiro de 2015, em: http://goo.gl/XDkoUF

Polk, T., McKay, K., & Chokhani, S. (2014). *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (Special Publication No. 800-52r1). Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-52r1

Postel, J. B. (1982). Simple Mail Transfer Protocol. RFC 821. doi: 10.17487/RFC821

Postel, J. B., & Reynolds, J. (1985). File Transfer Protocol. RFC 959. doi: 10.17487/RFC959

Qualys, Inc. (2015a). SSL Server Test. Acedido em: 16 de Janeiro de 2015, em: https://goo.gl/E5ahP3

Qualys, Inc. (2015b). User Agent Capabilities. Acedido em: 24 de Agosto de 2015, em: https://goo.gl/O3yL1E

Qualys, Inc. (2015c, Maio 20). SSL Server Rating Guide - version 2009j. Disponível em: https://goo.gl/e4Y8oA

Qualys, Inc. (2015d, Julho 10). SSL Labs API Documentation: v1.19.27. Acedido em: 25 de Julho de 2015, em: https://goo.gl/zykjYL

Qualys, Inc. (2015e, Agosto 25). Repositório ssllabs-scan no GitHub. Acedido em: 25 de Agosto de 2015, em: https://goo.gl/bJGTIM

Ray, M., & Dispensa, S. (2009, Novembro). *Renegotiating TLS*. Disponível em: http://goo.gl/rmkG7Y

Rente, F., Rela, M., Trovão, H., & Alves, S. (2008). Nonius, o nível de Segurança da Internet Portuguesa. Apresentado na 4ª edição da Conferência Nacional sobre Segurança Informática nas Organizações (SINO 2008), Coimbra. Disponível em: http://goo.gl/H8VqsL

Rescorla, E. (2015a, Julho 8). The Transport Layer Security (TLS) Protocol Version 1.3. Disponível em: https://tools.ietf.org/html/draft-ietf-tls-tls13-07

Rescorla, E. (2015b, Julho 10). Transport Layer Security (TLS) Parameters. Acedido em: 10 de Agosto de 2015, em: https://goo.gl/8OToaN

Resolução do Conselho de Ministros n.º 91/2012 de 8 de novembro. (2012). *Diário da República 1.ª Série, n.º 216/2012*. Presidência do Conselho de Ministros. Lisboa.

Ristić, I. (2014). *Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications*. Londres, Inglaterra: Feisty Duck.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Commun. ACM*, *21*(2), 120–126. doi: 10.1145/359340.359342

Ronaghan, S. A. (2001). *Benchmarking E-Government: A Global Perspective*. Nova Iorque, NY: United Nations Division for Public Economics and Public Administration and American Society for Public Administration. Disponível em: http://goo.gl/13zC1m

Rose, M. (1988). Post Office Protocol: Version 3. RFC 1081. doi: 10.17487/RFC1081

Salter, M., & Housley, R. (2012). Suite B Profile for Transport Layer Security (TLS). RFC 6460. doi: 10.17487/RFC6460

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*(4), 656–715. doi: 10.1002/j.1538-7305.1949.tb00928.x

Smart, N. P., Rijmen, V., Gierlichs, B., Paterson, K. G., Stam, M., Warinschi, B., & Watson, G. (2014). *Algorithms, key size and parameters report - 2014* (Relatório). Heraclião, Grécia: European Union Agency for Network and Information Security. Disponível em: https://goo.gl/QoyAJ5

Smart, N. P., Rijmen, V., Stam, M., Warinschi, B., & Watson, G. (2014). *Study on cryptographic protocols* (Relatório). Heraclião, Grécia: European Union Agency for Network and Information Security. Disponível em: https://goo.gl/T7eJgn

Stevens, M. (2013). New Collision Attacks on SHA-1 Based on Optimal Joint Local-Collision Analysis. Em T. Johansson & P. Q. Nguyen (Eds.), *Advances in Cryptology – EUROCRYPT 2013* (pp. 245–261). Springer Berlin Heidelberg. Disponível em: https://goo.gl/EyUp6P

Tanenbaum, A. S. (2003). *Computer Networks*. Prentice Hall PTR.

The MITRE Corporation. (2014a, Janeiro 22). CVE List Master Copy. Acedido em: 4 de Janeiro de 2015, em: https://cve.mitre.org/cve/cve.html

The MITRE Corporation. (2014b, Novembro 6). About CVE. Acedido em: 30 de Dezembro de 2014, em: https://cve.mitre.org/about/index.html

Trustworthy Internet Movement. (2015). SSL Pulse: Survey of the SSL Implementation of the Most Popular Web Sites. Acedido em: 25 de Julho de 2015, em: https://goo.gl/1GrkZU

Turner, S., & Polk, T. (2011). Prohibiting Secure Sockets Layer (SSL) Version 2.0. RFC 6176. doi: 10.17487/RFC6176

Usage share of operating systems. (2015, Agosto 23). Em *Wikipédia: a enciclopédia livre*. Disponível em: https://goo.gl/9d93YX

Wang, X., & Yu, H. (2005). How to Break MD5 and Other Hash Functions. Em R. Cramer (Ed.), *Advances in Cryptology – EUROCRYPT 2005* (pp. 19–35). Springer Berlin Heidelberg. Disponível em: http://link.springer.com/chapter/10.1007/11426639_2

Wescott, C. G. (2001). *E-Government in the Asia-Pacific Region* (pp. 1–24). Asian Development Bank. Disponível em: http://goo.gl/yh6E9n

Zoller, T. (2011). *TLS/SSL hardening and compatibility Report 2011*. Luxemburgo, Luxemburgo: G-SEC. Disponível em: http://goo.gl/WHV45n

Anexos

A. Outros Protocolos Utilizados na Internet

Além do HTTP, outros protocolos, utilizados ao nível da camada aplicacional do modelo OSI, contribuem para as comunicações na Internet. Na Tabela 34 estão enumerados alguns desses protocolos e na Tabela 35 as suas versões seguras.

Tabela 34
Outros protocolos utilizados na Internet.

Protocolo	Utilização	Norma[1]
Domain Name System (DNS)	Resolução de nomes de domínios	RFC 1034 (Mockapetris, 1987)
File Transfer Protocol (FTP)	Troca de ficheiros	RFC 959 (Postel & Reynolds, 1985)
Simple Mail Transfer Protocol (SMTP)	Envio de mensagens de correio eletrónico	RFC 821 (Postel, 1982)
Post Office Protocol Version 3 (POP3)	Receção e gestão de mensagens de correio eletrónico	RFC 1081 (Rose, 1988)
Internet Message Access Protocol (IMAP)		RFC 1730 (Crispin, 1994)

Tabela 35
Outros protocolos utilizados na Internet (versão segura).

Protocolo	Utilização	Norma
Domain Name System Security Extensions (DNSSEC)	Resolução de nomes de domínios de forma segura	RFC 4033 (Arends et al., 2005)
File Transfer Protocol Secured (FTPS)	Troca de ficheiros de forma segura	RFC 4217 (Ford-Hutchinson, 2005)
Simple Mail Transfer Protocol Secured (SMTPS)	Envio de mensagens de correio eletrónico de forma segura	RFC 2487 (Hoffman, 1999)
Post Office Protocol Version 3 Secured (POP3S)	Receção e gestão de mensagens de correio eletrónico de forma segura	RFC 2595 (Newman, 1999)
Internet Message Access Protocol Secured (IMAPS)		RFC 2595 (Newman, 1999)

[1] As normas podem ser consultadas no índice dos Request For Comments (RFC) (IETF, 2015a).

B. Comparação Entre as Forças de Encriptação Mais Utilizadas

A Tabela 36 demonstra a equivalência entre as forças de encriptação mais utilizadas e o tipo de algoritmo ou função criptográfica utilizada.

Tabela 36

Comparação entre as forças de encriptação mais utilizadas.

Simétrico (e.g., AES)	**Assimétrico e DH (e.g., RSA)**	**Curvas elípticas (e.g., ECDHE)**	**Funções de dispersão ou pseudoaleatórias (e.g., SHA-2)**
80 bit	1 024 bit	160 bit	160 bit
112 bit	2 048 bit	224 bit	224 bit
128 bit	3 072 bit	256 bit	256 bit
256 bit	15 360 bit	512 bit	512 bit

Fonte. Adaptação de tabela obtida de Ristić (2014, p. 18)

C. Especificações de Cifra das Recomendações do Estudo

A Tabela 37 enumera as especificações de cifra, divididas por tipo de certificado, permitidas pelas recomendações do estudo. Adicionalmente, indica a norma em que a respetiva especificação de cifra foi padronizada. A lista foi obtida tendo em consideração as especificações de cifra permitidas pelo TLS (Rescorla, 2015b) e as especificações de cifra temporárias do algoritmo de cifra ChaCha20[2].

Tabela 37

Lista de especificações de cifra das recomendações do estudo.

Especificação de cifra	Norma[3]
Para utilização com certificados RSA	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	RFC 5289
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	RFC 5289
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	RFC 5289
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	RFC 5288
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	RFC 5288
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	RFC 5288
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	RFC 5288
TLS_RSA_WITH_AES_256_GCM_SHA384	RFC 5288
TLS_RSA_WITH_AES_128_GCM_SHA256	RFC 5288
TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	RFC 6367
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	RFC 6367
TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	RFC 6367
TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	RFC 6367
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305	ID draft-ietf-tls-chacha20-poly1305
TLS_DHE_RSA_WITH_CHACHA20_POLY1305	ID draft-ietf-tls-chacha20-poly1305
TLS_DHE_RSA_WITH_AES_256_CCM	RFC 6655
TLS_DHE_RSA_WITH_AES_256_CCM_8	RFC 6655
TLS_DHE_RSA_WITH_AES_128_CCM	RFC 6655
TLS_DHE_RSA_WITH_AES_128_CCM_8	RFC 6655
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	RFC 4492
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	RFC 4492
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	RFC 5289
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	RFC 4492
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	RFC 5289

[2] No caso do Chacha20, uma vez que ainda esta em processo de padronização, é designado por Internet Draft (ID). Até padronização para uso no TLS pela IETF é necessário utilizar as especificações de cifra temporárias (Langley, Chang, Mavrogiannopoulos, Strombergson, & Josefsson, 2015, p. 4).

[3] As normas podem ser consultadas no índice dos RFC (IETF, 2015a).

Especificação de cifra	Norma[3]
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	RFC 4492
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	RFC 5246
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	RFC 5246
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	RFC 5246
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	RFC 5246
TLS_DH_RSA_WITH_AES_256_CBC_SHA256	RFC 5289
TLS_DH_RSA_WITH_AES_256_CBC_SHA	RFC 4492
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	RFC 5289
TLS_DH_RSA_WITH_AES_128_CBC_SHA	RFC 4492
TLS_RSA_WITH_AES_256_CBC_SHA256	RFC 5246
TLS_RSA_WITH_AES_256_CBC_SHA	RFC 5246
TLS_RSA_WITH_AES_128_CBC_SHA256	RFC 5246
TLS_RSA_WITH_AES_128_CBC_SHA	RFC 5246
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	RFC 5289
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	RFC 5289
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	RFC 5246
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	RFC 5246
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RFC 5246
Para utilização com certificados DSS[4]	
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	RFC 5288
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	RFC 5288
TLS_DH_DSS_WITH_AES_256_GCM_SHA384	RFC 5288
TLS_DH_DSS_WITH_AES_128_GCM_SHA256	RFC 5288
TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384	RFC 6367
TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256	RFC 6367
TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384	RFC 6367
TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256	RFC 6367
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	RFC 5246
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	RFC 5246
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	RFC 5246
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	RFC 5246
TLS_DH_DSS_WITH_AES_256_CBC_SHA256	RFC 5246
TLS_DH_DSS_WITH_AES_256_CBC_SHA	RFC 5246
TLS_DH_DSS_WITH_AES_128_CBC_SHA256	RFC 5246
TLS_DH_DSS_WITH_AES_128_CBC_SHA	RFC 5246
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	RFC 5246
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	RFC 5246
Para utilização com certificados ECDSA	
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	RFC 5289
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	RFC 5289
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	RFC 5289
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	RFC 6367
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	RFC 6367

[4] Os certificados DSS utilizam o algoritmo DSA.

Especificação de cifra	Norma[3]
TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	RFC 6367
TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	RFC 6367
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305	ID draft-ietf-tls-chacha20-poly1305
TLS_ECDHE_ECDSA_WITH_AES_256_CCM	RFC 7251
TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	RFC 7251
TLS_ECDHE_ECDSA_WITH_AES_128_CCM	RFC 7251
TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	RFC 7251
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	RFC 4492
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	RFC 4492
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	RFC 5289
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	RFC 4492
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	RFC 5289
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	RFC 4492
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	RFC 4492
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	RFC 4492