CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
CAMPUS TIMÓTEO

Gustavo Alves Vasconcelos

UM MÉTODO PARA IMPLEMENTAÇÃO DE CERTIFICAÇÃO DIGITAL EM REDE LOCAL

Timóteo

2018

Gustavo Alves Vasconcelos

UM MÉTODO PARA IMPLEMENTAÇÃO DE CERTIFICAÇÃO DIGITAL EM REDE LOCAL

Monografia apresentada à Coordenação de Engenharia de Computação do Campus Timóteo do Centro Federal de Educação Tecnológica de Minas Gerais para obtenção do grau de Bacharel em Engenharia de Computação.

Orientador: Adilson Mendes Ricardo

Timóteo

2018

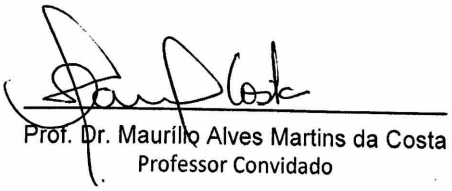
Gustavo Alves Vasconcelos

Estudo de caso: um método para implementação de certificação digital em rede local

Monografia apresentada ao Curso de Engenharia de Computação do Centro Federal de Educação Tecnológica de Minas Gerais, campus Timóteo para obtenção do título de Engenheiro de Computação.

Trabalho aprovado. Timóteo, 12 de Julho de 2018:

Prof. Me. Adilson Mendes Ricardo
Orientador



Prof. Dr. Maurílio Alves Martins da Costa
Professor Convidado

Prof. Me. Talles Quintão Pessoa
Professor Convidado

Timóteo
2018

Aos meus pais, minha namorada, meus amigos e a
todos que contribuiram para minha formação.

Agradecimentos

Primeiramente, agradeço à Deus por ter me dado sabedoria para vencer mais esta etapa da minha vida.

Agradeço aos meus pais, pelo amor, incentivo e por sempre me apoiarem durante todos esses anos.

Agradeço à minha namorada Débora, pelo companheirismo e pelo apoio.

Agradeço ao meu orientador Adilson, pela disposição, dedicação e auxílio no desenvolvimento deste trabalho.

Enfim, agradeço a todas as pessoas que fizeram parte dessa etapa decisiva em minha vida.

"Cada escolha que fazemos é uma pequena revolução."
Nobuhiro Watsuki

Resumo

O uso certificação digital para segurança da rede de computadores tem por objetivo a autenticação de uma entidade no ambiente virtual, de modo a evitar diferentes tipos de fraudes. Todo certificado é emitido por uma Autoridade Certificadora (AC), que é a responsável pela sua gerência. No Brasil, as ACs precisam de um certificado que comprove sua identidade, esse é expelido pelo Instituto Nacional de Tecnologia da Informação (ITI), o órgão responsável pela coordenação das ACs no Brasil. No entanto, com a necessidade de autenticidade em redes de áreas locais (LAN), surgiram os softwares de AC locais, o qual não necessitam da certificação do ITI. Este trabalho propõe um estudo sobre como oferecer autenticidade para servidor WEB em uma LAN, por meio da implementação de uma AC local e o uso da certificação digital. Para tal, foi implementado uma plataforma com clientes e servidores locais, para realização de testes de autenticidade. Os testes simularam três tipos de situações tendo como objetivo mostrar a efetividade do método e buscando analisar os possíveis resultados a nível cliente. Após a análise realizada foi constatado que, embora a AC local não seja tão segura quando uma AC certificada, os testes apresentaram resultados satisfatórios para autenticidade dos servidores WEB.

Palavras-chave: Certificados Digitais, Autoridade Certificadora, Autenticidade, Rede de Área Local.

Abstract

The use of digital certification for computer network security aims to authenticate an entity in the virtual environment in order to avoid different types of fraud. Each certificate is issued by a Certification Authority (CA), which is responsible for its management. In Brazil, the CAs need a certificate that proves their identity, which is expelled by the National Institute of Information Technology (ITI), the body responsible for the management of CAs in Brazil. However, with the need for authenticity in local area networks (LAN), local CA software has appeared, which does not require ITI certification. This paper proposes a study on how to offer authenticity to a WEB server in a LAN, through the implementation of a local CA and the use of digital certification. To this purpose, a platform with local clients and servers was implemented to perform authenticity tests. The tests simulated three types of situations in order to show the effectiveness of this method and to analyze the possible results at the client level. After the analysis, it was found that, although the local CA is not as secure as a certified CA, the tests presented satisfactory results for the authenticity of the WEB servers.

Keywords: Digital Certificates, Certifying Authority, Authenticity, Local Area Network.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

AC	Autoridade Certificadora
DNS	*Domain Name System*
HTML	*HyperText Markup Language*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
ICP	Infraestrutura de Chaves Públicas Brasileira
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IIS	*Internet Information Service*
IP	*Internet Protocol*
ITI	Instituto Nacional de Tecnologia da Informação
ITU	*International Telecommunication Union*
LAN	*Redes de Áreas Locais*
MD	*Message Digest*
MiTM	*Man in the Middle*
MMC	*Microsoft Management Console*
PKI	*Public Key Infrastructure*
SET	*Secure Electronic Transaction*
SSL	*Secure Socket Layer*
TSL	*Transport Layer Security*
URL	*Uniform Resource Locator*
VM	*Virtual Machine*

Sumário

1 Introdução

A evolução tecnológica tem possibilitado mudanças significativas nos cenários sociais, políticos, econômicos e culturais. Com esse avanço, destaca-se a criação e expansão das redes de computares que contribuíram para o aperfeiçoamento da troca de informação, tornando-a mais simples, rápida e barata.

De acordo com Kurose e Ross (2013), o uso das redes de computadores se tornou fundamental para a sociedade. Muitas pessoas contam, principalmente com a internet, em suas atividades profissionais, sociais e pessoais, pelas informações e serviços que essa oferece, encurtando distâncias e economizando tempo. Isso não é diferente no ambiente corporativo, segundo Tanenbaum e Wetherall (2011), toda empresa, grande ou pequena, tem uma dependência vital das informações computadorizadas, sentindo imediatamente o impacto quando os seus recursos de redes de computadores ficam indisponíveis.

De acordo com Tanenbaum e Wetherall (2011), em virtude da expansão e do aumento de serviços fornecidos pelas redes de computadores, a segurança da informação tornou-se um problema de grandes proporções, pois milhões de cidadãos começaram a utilizá-la, surgindo a necessidade de se comunicar com mensagens íntegras, autênticas e lidas apenas por pessoas autorizadas.

Kurose e Ross (2013) também enfatiza a necessidade da segurança da informação, segundo os autores, atrás de toda essa utilidade e entusiasmo das redes de computadores, existe o lado escuro, um lado no qual “vilões” tentam causar problemas em nosso cotidiano danificando nossos computadores, violando nossa privacidade e tornando inoperantes os serviços da rede dos quais dependemos.

Uma das tecnologias que veio para atender a essa necessidade foi a certificação digital. Essa tem o objetivo de evitar que adulterações, interceptações ou outros tipos de fraudes ocorram, pois essa assegura as identidades dos envolvidos na troca eletrônica de documentos, mensagens e dados (SAFRAN, 2010).

O Instituto Nacional de Tecnologia da Informação (ITI) (2017) define certificado digital como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos. Esse é gerado e assinado por uma terceira parte, ou seja, uma Autoridade Certificadora (AC), que é o encarregado de assegurar a sua identidade virtual.

As ACs são as responsáveis por diversas funções, como: emitir, expedir, distribuir, revogar e gerenciar os certificados, é ela que associa uma pessoa, processo, servidor, ou etc, a um par de chaves criptográficas, que são utilizadas para autenticação (TANENBAUM; WETHERALL, 2011). Por esses motivos essa é considerada o componente mais importante para o certificado digital. Segundo Monteiro e Mignoni (2007), as ACs são entidades de confiança que emitem certificados digitais para entidades, que precisam se identificar e garantir

suas operações no mundo digital.

Deste modo, o presente trabalho busca inicialmente identificar os métodos de autenticação virtual com certificados digitais para redes de áreas locais(LANs)[1]. Posteriormente, simular e testar em um ambiente local virtual o uso de um software de AC para a identificação dos servidores WEB, de forma a avalia essa alternativa a nível cliente com objetivo de investigar sua capacidade.

1.1 Problema e sua importância

O acesso de servidores WEB e/ou ferramentas em LANs, sem a verificação de identidade, faz com que o usuário e o ambiente fiquem vulneráveis a ataques, fraudes e prejuízos potenciais, que se dão por diferentes formas, como corrupção, desvios, espionagem e manipulação dos dados. Sendo que, em um ambiente com servidores certificados, os usuários terão maior certeza de com quem está se comunicando, dando maior tranquilidade na troca de mensagem.

Uma alternativa para resolver o problema de autenticação de servires WEB em rede LAN é a compra e utilização de certificação digital assinado por uma AC reconhecida pelo ITI. No Brasil, essas ACs precisam de uma certificação que comprove sua identidade, esse é expelido pelo ITI, o órgão responsável pela gerência das ACs no Brasil, seguindo as regras de funcionamento estabelecidas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) (Instituto Nacional de Tecnologia da Informacao, 2017). Fazendo com que o certificado emitido por essas ACs ganhe validade jurídica.

Uma outra opção é a implementação de um software de AC local para emitir e gerenciar os certificados internos. De acordo com Junior (2009), embora essas não tenham o valor jurídico estão se tornando fortes opções para usuários de LAN, pois são meios relativamente seguros, de baixo custo e rápidos para elevar o nível de autenticidade nas atividades cotidianas. Além disso, essa evita os problemas de má administração de serviços de uma AC externa, pois usuário é o próprio administrador. Nesse contexto, surge a seguinte questão: A utilização de certificados digitais emitidos por uma AC própria, eleva o nível de autencidade dos servidores WEB em redes de áreas locais(LANs)?

1.2 Objetivos

Diante do que foi exposto e da necessidade crescente do uso de certificados digitais, o objetivo geral deste trabalho é realizar um estudo de caso sobre como oferecer autenticidade para servidor WEB em uma LAN, sem o uso de uma AC externa, por meio da implementação e o uso da certificação digital. Similarmente, esse trabalho também tem como objetivo específicos:

- Implementar uma plataforma com clientes e servidores, onde o servidor WEB é certificado por AC local;

[1] *Local area network*

- Elaborar e executar testes de acesso de autenticidade no servidor WEB;
- Analisar, a nível do cliente, o resultado dos acessos ao servidor WEB com e sem a utilização de certificado digital para problema proposto.

2 Fundamentação Teórica

O presente trabalho estuda a aplicação de certificado digital em uma rede local, juntamente com melhores práticas do protocolo Camada Segura de Transporte(TLS)[1]. Desta forma, esse capítulo tem como objetivo apresentar a fundamentação teórica necessária para a compreensão do trabalho desenvolvido, abordando os conceitos de criptografia, função *hash*, assinatura digital, certificado digital, AC, TLS e Sistema de Nomes de Domínios(DNS)[2].

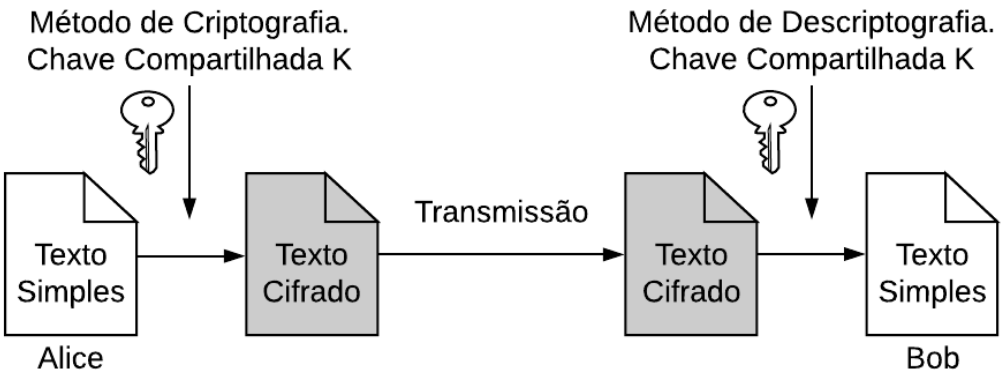
2.1 Criptografia

A palavra criptografia vem de origem grega, que significam 'escrita secreta' (TANENBAUM; WETHERALL, 2011), essa surgiu com a necessidade de maior segurança ao enviar informações sensíveis através de meios de comunicações questionáveis, isto é, em meios onde não é possível garantir que um intruso não possa interceptar o fluxo de dados para leitura ou para modifica-lo (SOARES; LEMOS; COLCHER, 1995).

As mensagens que serão criptografadas são conhecidas como texto simples (*plaintext*), essas são transformadas em um texto cifrado (*ciphertext*) após o processo de criptografia (TANENBAUM; WETHERALL, 2011).

A Figura 1, ilustra o processo de criptografia que funciona da seguinte maneira, um texto simples é aplicado a um método, algoritmo de criptografia, parametrizada por uma chave, resultando na saída o texto cifrado. Para descriptografar uma mensagem, será aplicado o mesmo procedimento acima utilizando o texto cifrado, um algoritmo de decifração e uma chave, resultando na saída o texto original (FOROUZAN, 2008).

Figura 1 – Modelo de criptografia



Fonte: Adaptado de (KUROSE; ROSS, 2013).

Para que as mensagens se tornem ilegíveis é necessário que sejam cifradas por com-

[1] *Transport Layer Security*
[2] *Domain Name System*

pleto, bit-a-bit, em um fluxo contínuo, ou divididas em blocos de n-bytes e criptografados em seguida. Estes processos de cifragem são denominados como criptografia de fluxo de dados e criptografia de blocos(MORENO; PEREIRA; CHIARAMONTE, 2005).

Na criptografia, os algoritmos são públicos e as chaves são secretas. Qualquer um pode acessar os algoritmos para cifragem/decifragem, já as chaves devem ser protegidas, pois são elas que contém o segredo da cifragem (FOROUZAN, 2008). Logo, um bom método de criptografia deve garantir que seja, senão impossível, pelo menos muito difícil que um intruso recupere a partir do texto cifrado e do conhecimento sobre o método de criptografia, o valor das chaves. Sendo isso verdade, a confidencialidade do texto transmitido é garantida, enquanto as chaves utilizadas forem secretas (SOARES; LEMOS; COLCHER, 1995).

2.1.1 Criptografia Simétrica

Na criptografia de chave simétrica, a mesma chave é compartilhada pelos participantes. O emissor usa essa chave e um algoritmo de criptografia para cifrar os dados, o receptor usa a mesma chave e o algoritmo de descriptografia correspondente para decifrar os dados. A chave é mesma para todos participantes (FOROUZAN, 2008).

A Figura 1 ilustra o funcionamento desse método de criptografia por meio da comunicação entre duas pessoas, Alice e Bob. Nesse cenário, Alice deseja se comunicar com Bob utilizando o método de criptografia de chave simétrica. Para isso, antes de iniciar a troca de mensagem é necessário que a chave simétrica seja compartilhada entre ambos, essa deve ser enviada por meio de um canal seguro, pois se outra pessoa tiver acesso a essa chave, essa também poderá fazer parte da conversa. Em seguida, quando Alice ou Bob for enviar ou receber uma mensagem um do outro, a chave compartilhada será utilizada para cifrar e decifrar o texto simples(KUROSE; ROSS, 2013).

Nota-se que os algoritmos de criptografia de chave simétrica recebem esse nome porque a mesma chave pode ser usada nas duas direções (FOROUZAN, 2008). Este processo é mais rápido se comparado à criptografia de chave assimétrica, mas continua sendo inseguro devido à distribuição centralizada, sendo necessário um canal seguro para distribuição da chave (TRINTA; MACÊDO, 1998).

Na criptografia de chave simétrica, o algoritmo usado para decifrar é o inverso do algoritmo usado para cifrar. Isso significa que, se o algoritmo para criptografar uma mensagem usa uma combinação de adição e multiplicação, o algoritmo para descriptografá-la terá uma combinação de subtração e divisão (FOROUZAN, 2008).

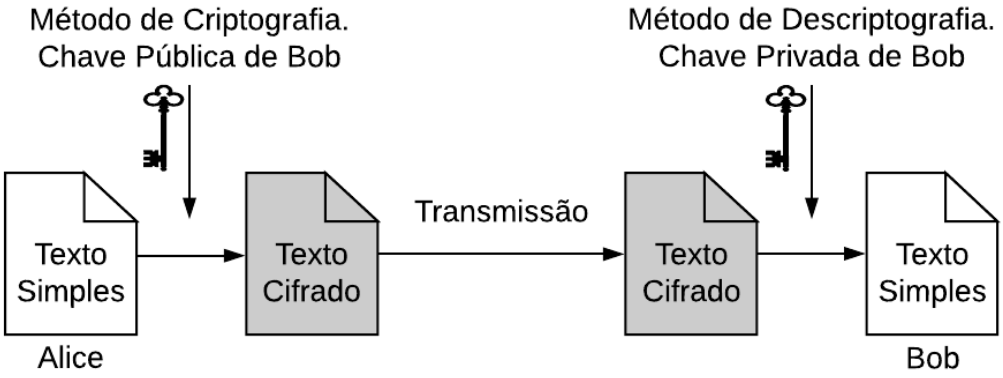
2.1.2 Criptografia Assimétrica

A criptografia de chave pública, minimiza o problema de distribuição centralizada de chaves encontrado na criptografia de chave simétrica, pois não é preciso estabelecer um canal seguro. Para tal, existem duas chaves, uma privada e outra pública. A chave privada é mantida em segredo com usuário, enquanto a chave pública é anunciada para em um diretório público (KUROSE; ROSS, 2013), permitindo que qualquer pessoa possa enviar mensagens cifradas a

partir da chave pública, as quais somente o proprietário da chave privada, referente ao par da chave pública utilizada, é capaz de decifrá-las, proporcionando autenticidade do destinatário. Além disso, a qualquer momento um usuário pode mudar sua chave privada, e publicar sua nova chave pública complementar para substituir sua antiga (STALLINGS; BROWN, 2016).

A Figura 2 apresenta um cenário onde duas pessoas, Alice e Bob, desejam se comunicar utilizando o método de criptografia por chave pública, o qual, o primeiro deseja enviar uma mensagem de forma segura ao segundo. Para isso, é necessário que Bob publique sua chave pública para que Alice ou qualquer outro que deseje comunicá-lo aplique essa chave para criptografar a mensagem. Em seguida, ao receber a mensagem enviada por Alice, Bob utiliza sua chave privada para descriptografá-la (TANENBAUM; WETHERALL, 2011).

Figura 2 – Criptografia com chaves públicas



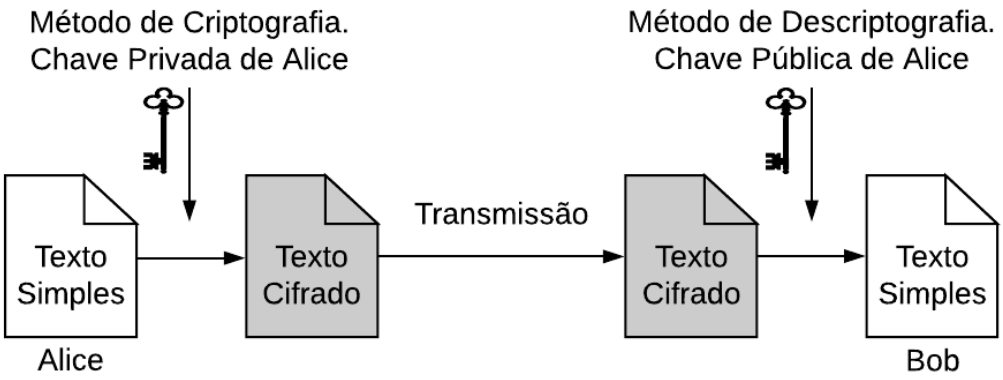
Fonte: Adaptado de (KUROSE; ROSS, 2013).

Assim, ninguém mais pode ler a mensagem criptografada, porque o sistema de criptografia é considerado sólido, sendo muito difícil derivar chave privada da chave publicamente conhecida. Para enviar uma resposta, basta o Bob fazer o mesmo que o Alice, encriptografar a mensagem utilizando a chave pública de Alice (TANENBAUM; WETHERALL, 2011).

A criptografia de chave privada, diferente da criptografia de chave pública, é direcionado para proporcionar autenticidade do emissor na comunicação e integridade da mensagem, como mostra a Figura 3.

Nesse esquema, Alice criptografa a mensagem usando sua chave privada e a envia para Bob. Em seguida, quando Bob ou qualquer outra pessoa descriptografá-la utilizando a chave pública de Alice, isso indicará que o único emissor possível é Alice, assim providenciando autenticidade a comunicação. Além disso, ninguém mais séria capaz de modificar o texto simples, porque o único que poderia ter criptografado com a chave privada do usuário emissor seria o próprio emissor, assim providenciando integridade dos dados (STALLINGS; BROWN, 2016).

Figura 3 – Criptografia com chaves privada



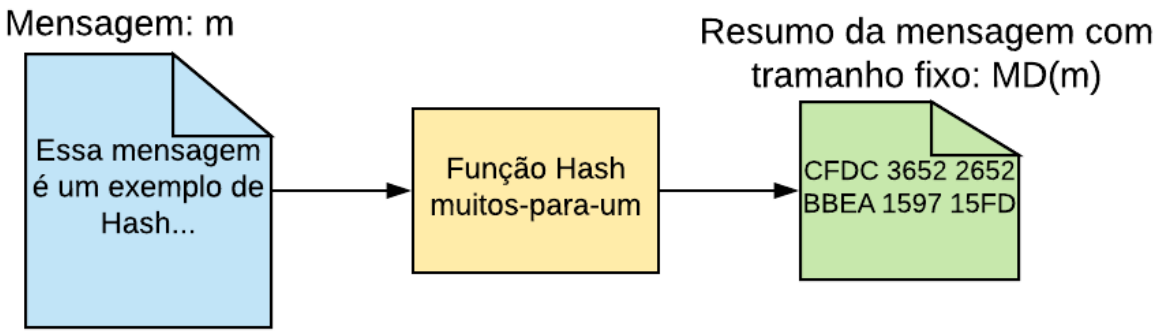
Fonte: Adaptado de (KUROSE; ROSS, 2013).

2.2 Função *Hash*

A função *hash* representada por MD (*Message Digest*), geralmente é chamada sumário da mensagem. Como mostrado na Figura 4, essa recebe uma entrada de tamanho indefinida, e calcula uma cadeia de tamanho fixo conhecida como *hash* (KUROSE; ROSS, 2013).

O código *hash* é uma função aplicada a todos os bits da mensagem e oferece a capacidade da detecção de erros: uma mudança em qualquer bit na mensagem, resulta em uma mudança no resultado da saída função *hash* (STALLINGS; BROWN, 2016).

Figura 4 – Função *hash*



Fonte: Adaptado de (KUROSE; ROSS, 2013).

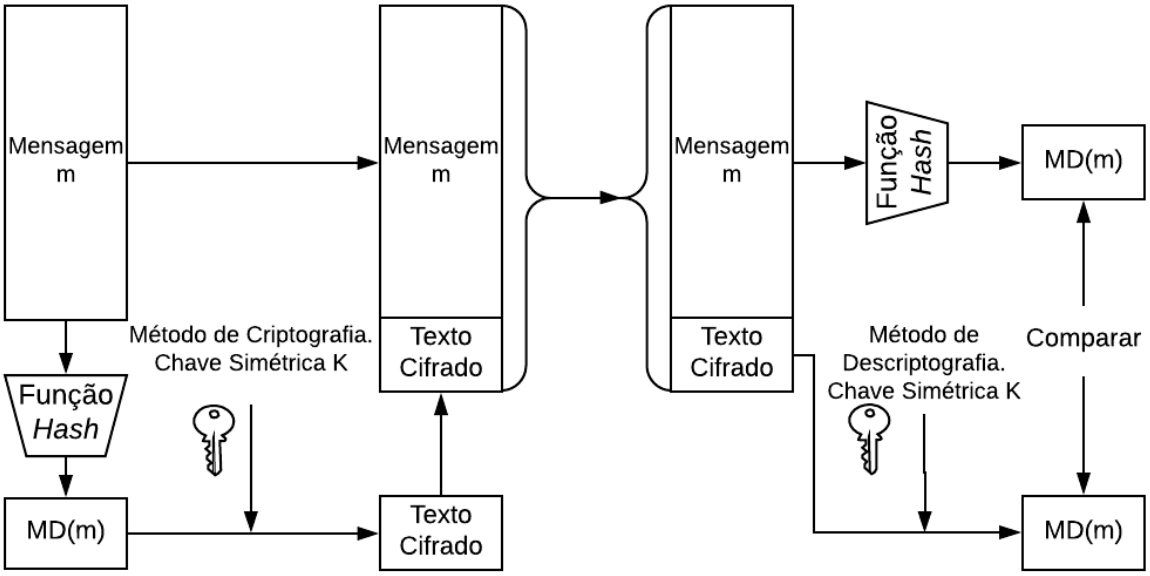
O objetivo de uma função *hash* é produzir uma *fingerprint* [3] de um arquivo, mensagem ou blocos de dados. Que será ultilizado para autenticação de mensagens e verificação da integridade de mensagens (STALLINGS; BROWN, 2016). Para isso, de acordo com Stallings e Brown (2016) função *hash* precisa ter as seguintes propriedades.

[3] Impressão digital

1. A função *hash* pode ser aplicado em texto com tamanho qualquer;
2. A função *hash* produz uma saída de comprimento fixo;
3. Se uma mensagem m for fornecido, o cálculo de MD(m) será muito fácil;
4. Para qualquer mensagem m de tamanho n, é computacionalmente inviável encontrar outro mensagem com mesmo tamanho n, diferente de m, tal que o resultando da função *hash* MD(m), seja o mesmo que MD(n).

A Figura 5 exemplifica uma maneira de autenticação de mensagem usando a função de *hash*. Nessa, a mensagem resumida (MD(m)) é cifrada usando algoritmo de criptografia de chave simétrica. O receptor recebe a mensagem, decifra, e realiza o cálculo *hash* da mensagem e, compara com a mensagem resumida do emissor. Se o valor for de MD(m) do receptor e do emissor forem iguais, e for assumido que apenas o emissor e o receptor possuem a chave de criptografia, então a autenticação é garantida (STALLINGS; BROWN, 2016).

Figura 5 – Autenticação de mensagem usando função *hash* e criptografia assimétrica

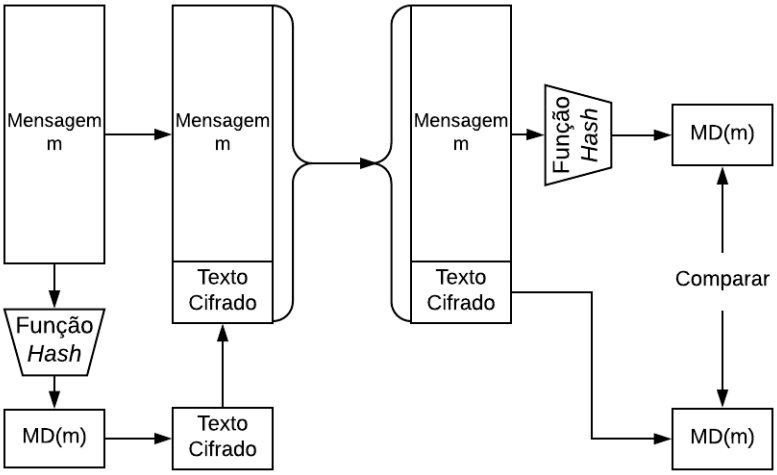


Fonte: Adaptado de (STALLINGS; BROWN, 2016).

A mensagem resumida (MD(m)) também pode ser cifrada utilizando o algoritmo de criptografia de chave pública. O algoritmo de chave pública tem duas vantagens, ele fornece tanto uma assinatura digital bem como autenticação de mensagem, e não requer uma distribuição de chaves pelas partes envolvidas (STALLINGS; BROWN, 2016).

Por último, a Figura 6, mostra uma técnica usando uma função *hash* mas não usa criptografia para autenticação de mensagem (STALLINGS; BROWN, 2016).

Figura 6 – Autenticação de mensagem usando função *hash*



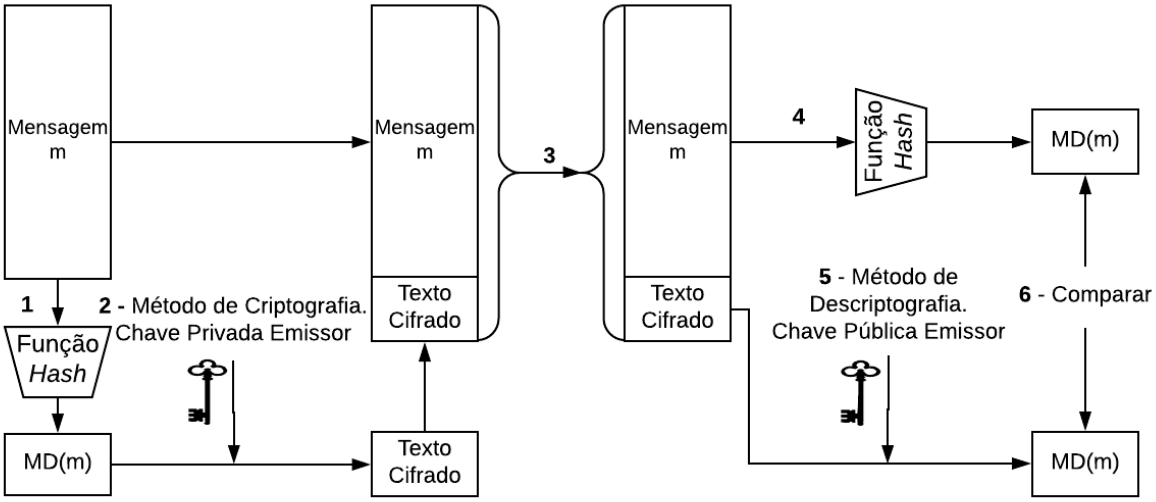
Fonte: Adaptado de (STALLINGS; BROWN, 2016).

2.3 Assinatura Digital

A assinatura digital é o mecanismo utilizado provar se o autor de um determinado documento é quem diz ser e que o documento não foi modificado/violado por terceiros de maneira acidental ou intencional (REZENDE, 2016), sendo capaz de agregar características semelhantes às obtidas ao assinar um documento utilizando papel e caneta, mas em meio eletrônico (KUROSE; ROSS, 2013).

O objetivo da assinatura digital não é garantir a confidencialidade, mas a autenticidade, integridade e o não-repúdio das mensagens (KUROSE; ROSS, 2013). Para atender essas garantias, é feito o uso da criptografia assimétrica e da função *hash*. Como pode ser visto na Figura 7, onde o processo de assinatura e verificação da mensagem é realizado da seguinte maneira.

Figura 7 – Representação processo de assinatura digital



Fonte: Adaptado de (STALLINGS; BROWN, 2016).

1. É feito o cálculo do valor da função de *hash* da mensagem, resultando em um bloco de *hash* - MD(m);
2. Em seguida, é realizado a criptografia com a chave privada do emissor do bloco de *hash*, resultando em um bloco de *hash* cifrado;
3. A mensagem original mais o bloco de *hash* cifrado em anexo, é enviada;
4. A mensagem é recebida com o bloco de *hash* cifrado em anexo, o receptor decifra o bloco de *hash* cifrado utilizando a chave pública do emissor;
5. O receptor aplica a mesma função de *hash* utilizada pelo emissor na mensagem recebido, resultando em um outro bloco de *hash*;
6. Por último, é feita comparação entre os dois blocos de *hash*, o que foi calculado pelo receptor com o recebido em anexo na mensagem. Se os valores forem o mesmo, o receptor reconhece que a mensagem foi assinada pelo emissor, pois é assumido que ninguém mais tem acesso a sua chave privada. Desse modo, nenhum outro usuário poderia ter criado um texto cifrado que seja decifrado utilizando a chave pública do emissor.

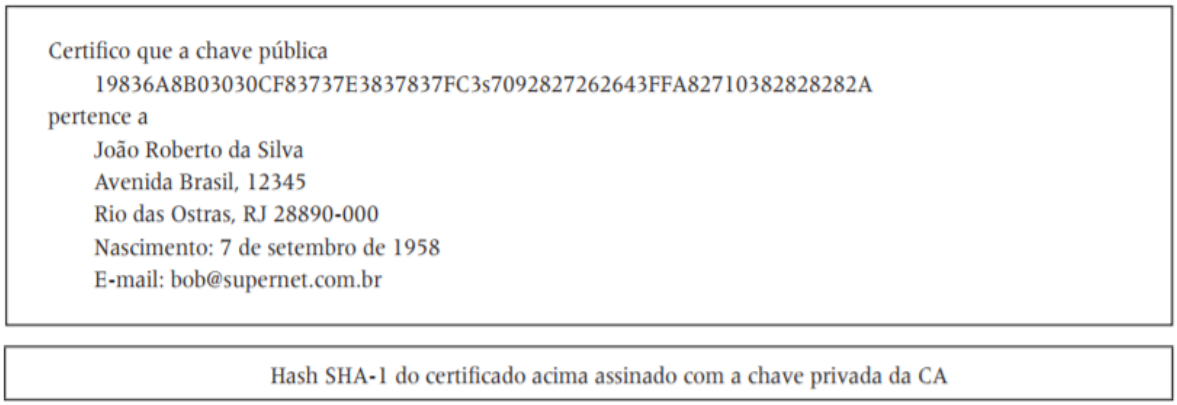
2.4 Certificado Digital e Autoridade Certificadora

O certificado digital é um documento eletrônico assinado, que contém nome, número público exclusivo chamado de chave pública e outros dados, vinculado a uma entidade específica, indivíduo, empresa, e etc, e utilizado para identificá-los no meio digital (KUROSE; ROSS, 2013). As informações contidas num certificado digital são o que possibilita colocá-lo em repositórios públicos para que terceiros possam conferir a autenticidade das assinaturas digitais que vierem examinar (JÚNIOR; SILVA, 2008).

Conforme explica Marcacini, o certificado eletrônico é uma forma, não a única, mas talvez a mais prática, de se demonstrar a titularidade da chave pública utilizada para conferir a assinatura. Pode ser entendido, sob o ângulo jurídico, como uma declaração de uma pessoa, o ente certificante, em relação à chave pública de uma outra pessoa, atestando essa titularidade (MARCACINI, 2007).

Um certificado pode ser auto-assinado ou emitido por uma AC, produzindo um par de chaves, pública e privada, para seu proprietário. A chave pública fica disposta no certificado, enquanto a chave privada deve ficar com o proprietário e em segurança, pois caso outra pessoa tenha acesso, poderá se passar pelo proprietário legítimo (REZENDE, 2016). A Figura 8 apresenta o modelo de um certificado digital assinado por uma AC.

Figura 8 – Possível Certificado Digital



Fonte: (TANENBAUM; WETHERALL, 2011).

O certificado digital passa por várias fases desde seu requerimento até o fim de sua validade. Tadano (2002) divide esse ciclo em oito fases, são elas:

1. Requerimento: é o pedido de expedição do certificado digital feito pela pessoa interessada à AC;
2. Validação do requerimento: é função da AC garantir que o requerimento seja válido e que os dados do requerente sejam corretos;
3. Emissão do certificado: é o ato de reconhecimento do título do certificado digital pelo requerente e sua emissão;
4. Aceitação do certificado pelo requerente: após emitido, o requerente deve retirá-lo da AC e confirmar a validade do certificado emitido;
5. Uso do certificado: é o período em que o certificado pode ser utilizado, sendo seu uso de total responsabilidade do requerente;
6. Suspensão do certificado digital: é o ato pelo qual o certificado se torna temporariamente inválido para operações por algum motivo especificado pela AC, como o comprometimento da chave pública;

7. Revogação do certificado: é o processo pelo qual o certificado se torna definitivamente inválido pelo comprometimento da chave privada do titular ou quando ocorrer algum fato que torne o certificado digital pouco seguro para uso. Um certificado suspenso ou revogado deve ser publicado na lista de certificados revogados (LCR) e estar sempre disponível para consulta;

8. Término da validade e renovação do certificado: o certificado digital tem um período preestabelecido de validade atribuído pela AC. Em geral, este período é de um a três anos, dependendo da importância e finalidade da chave.

Todo certificado é emitido e assinado pela AC que o criou. Essa também é responsável pela gerência do seu ciclo de fases, podendo: emitir, revogar, armazenar, renovar e distribuir. De acordo com Kurose e Ross (2013), uma AC tem as seguintes funções:

- Verificar se uma entidade (pessoa, roteador e assim por diante) é quem diz ser. Não há procedimentos obrigatórios para o modo como deve ser feita a certificação. Quando tratamos com uma AC, devemos confiar que ela tenha realizado uma verificação de identidade adequadamente rigorosa.

- Criar um certificado que vincula a chave pública da entidade à identidade verificada. O certificado contém a chave pública e a informação exclusiva que identifica mundialmente o proprietário da chave pública (por exemplo, o nome de alguém). O certificado é assinado digitalmente pela AC.

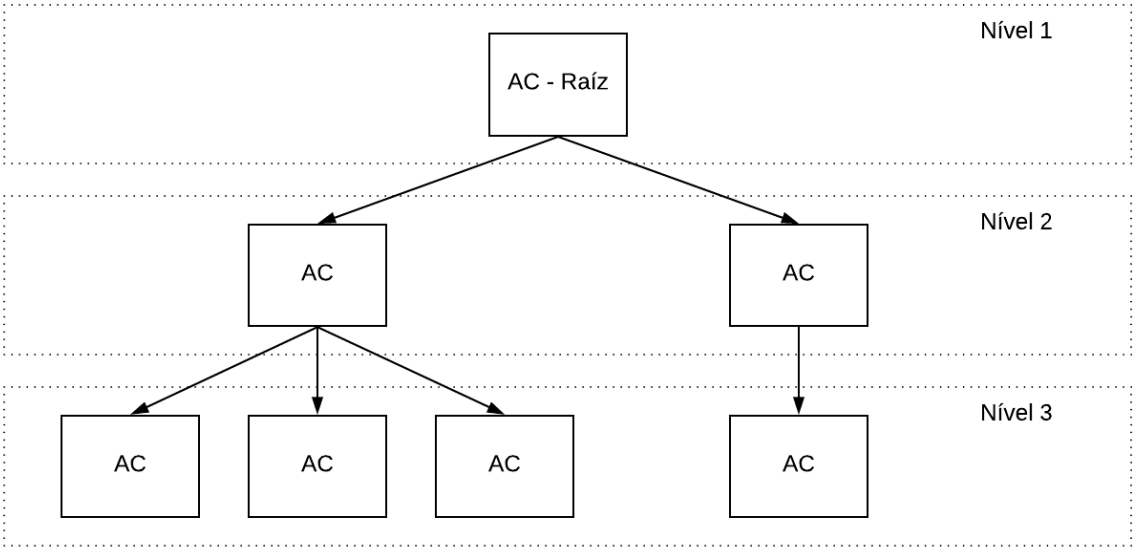
Uma analogia feita por Medeiros para explicar sobre a relação entre Certificado Digital e AC, diz: "Assim como a Carteira de Identidade é assinada por um Órgão de Segurança que lhe dá credibilidade, o certificado digital é emitido e assinado (chancelado) por uma AC digital que emite o certificado"(JÚNIOR; SILVA, 2008).

Como existe um número crescente de usuários solicitando certificados, uma única AC não é suficiente para atender a demanda de emissão e verificação de identidades, como há várias ACs atuando, há a necessidade de gerenciá-las, assim surgiu a Infraestrutura de Chave Pública(PKI)[4] (NASCIMENTO, 2009). Esta tem como função fornecer um modo de estruturar esses componentes e definir padrões para os vários documentos e protocolos (TANENBAUM; WETHERALL, 2011).

A Figura 9 ilustra uma forma particularmente simples de PKI hierárquica. Nessa existem três níveis de hierarquia, mas esse número pode variar de acordo com a necessidade. Nesse modelo, cada nível é responsável por fiscalizar o nível subsequente, por exemplo no primeiro nível temos uma AC chamada de raiz, essa é responsável por criar, revogar, armazenar, distribuir certificados, atualizar o par de chaves utilizados (quando expirados ou caso sejam comprometida) e fiscalizar para todas ACs do segundo nível, do mesmo modo, as ACs segundo nível são responsáveis pelas do terceiro, e assim por diante (TANENBAUM; WETHERALL, 2011).

[4] *Public Key Infrastructure*

Figura 9 – Hierarquia PKI



Fonte: Adaptado de (TANENBAUM; WETHERALL, 2011).

No caso específico do Brasil, o governo criou uma infraestrutura de chaves públicas composta por ACs organizadas de maneira hierárquica denominada ICP-Brasil (NASCIMENTO, 2009). Essa é responsável por disponibilizar os certificados digitais que são classificados quanto à sua aplicabilidade e quanto aos requisitos de segurança de proteção da chave privativa (Instituto Nacional de Tecnologia da Informação, 2013).

Por existir diferentes tipos de certificados, a ITU (*International Telecommunication Union*[5]) junto com a IETF (*Internet Engineering Task Force*[6]) desenvolveram o modelo X.509, como um padrão de certificado digital que vincula um nome à uma chave pública e tem por objetivo fornecer serviços de autenticação (NASCIMENTO, 2009). Os principais campos desse padrão e suas respectivas descrições estão listados na Tabela 1.

Segue alguns exemplos de softwares para implementação de uma AC local, sem certificação do ICP-Brasil:

- Código aberto OpenSSL: Software para emissão de certificado desenvolvido pela OpenSSL;
- Código aberto OpenCA: Software de autoridade de certificação desenvolvido pela OpenCA;
- Código aberto EJBCA: Software de autoridade de certificação desenvolvido pela PrimeKey Solutions AB;
- *Active Directory Certificate Services*: Software de autoridade de certificação desenvolvido pela Microsoft;

[5] União Internacional de Telecomunicações
[6] Força-tarefa de engenharia da internet

Tabela 1 – Campos básicos padrão X.509

Campo	Significado
Versão	Identifica a versão do formato do certificado.
Número de série	Este número, somado ao nome da AC, identifica o certificado de forma exclusiva.
Identificador	Algoritmo usado para assinar o certificado.
Nome do emissor	Nome da AC.
Período de validade	Períodos inicial e final de validade.
Nome do sujeito	Nome da entidade cuja a chave está sendo certificada.
Chave pública	A chave pública da entidade certificada e o algoritmo utilizado.
Identidade do emissor	Uma identidade opcional que identifica de forma exclusiva o emissor do certificado.
Identidade do sujeito	Uma identidade opcional que identifica de forma exclusiva a entidade certificada.
Extensões	Muitas extensões foram definidas.
Assinatura	A assinatura do certificado (assinado pela chave privada da AC)

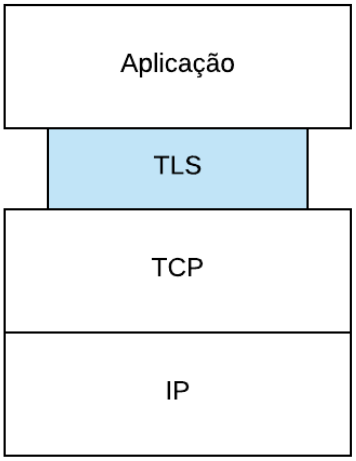
Fonte: Adaptado de (TANENBAUM; WETHERALL, 2011).

2.5 Protocolo TLS

O TLS é um padrão de internet que surgiu a partir do SSL(*Secure Sockets Layer*)[7], à fim de garantir uma comunicação ponto-a-ponto confiável. Esse pode ser implementando tanto nos navegadores quanto nos servidores WEB, oferecendo serviços de segurança como, autenticação do servidor, confidencialidade, integridade e autenticidade das mensagens enviadas (STALLINGS; BROWN, 2016).

O TLS é projetado para fazer uso do TCP para fornecer um serviço de entrega segura para os protocolos de aplicação. Isso acontece porque o TLS por proteger o TCP, ele pode ser empregado por qualquer aplicação que execute o TCP (FOROUZAN, 2008). A Figura 10 mostra o uso do TLS dentro do modelo de camadas de rede do TCP/IP, que embora resida tecnicamente na camada de aplicação, do ponto de vista do desenvolvedor, ele é um protocolo de transporte que provê serviços do TCP (STALLINGS; BROWN, 2016).

Figura 10 – Modelo TCP/IP com TLS



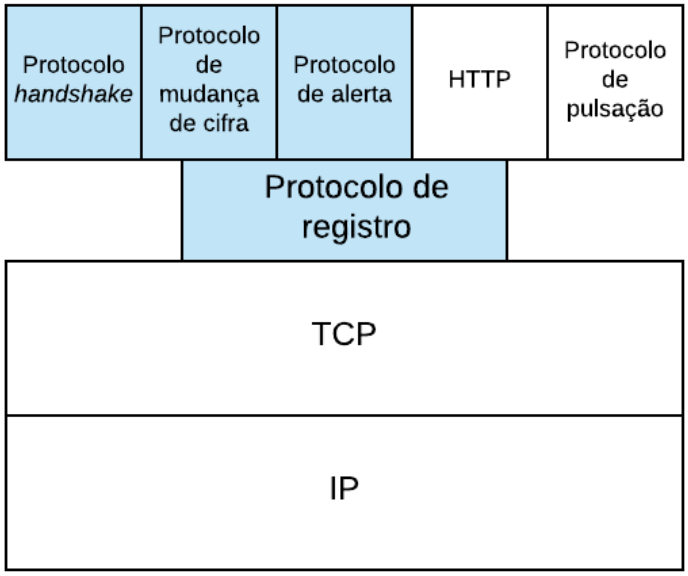
Fonte: Adaptado de (FOROUZAN, 2008).

[7] Camada Segura de Sockets

Para melhor entendimento do funcionamento do TLS é necessário entender os conceitos de conexão e sessão. A conexão TLS é utilizada em conexão ponto-a-ponto para fornece o tipo adequado de serviço para uma comunicação, sendo que cada conexão está relacionada à uma sessão. Já a sessão TLS, é utilizada em uma conexão cliente-servidor, durante o protocolo *handshake*. São elas que definem os os respectivos parâmetros de segurança compartilhados por várias conexões (STALLINGS; BROWN, 2016).

Como ilustrado na Figura 11 o TLS não é um protocolo único, mas sim duas camadas de protocolos, formada pelo protocolo de registro, protocolo *handshake*, protocolo de mudança de cifra, protocolo de alerta.

Figura 11 – Protocolos TLS



Fonte: Adaptado de (STALLINGS; BROWN, 2016).

O protocolo de registro TLS é utilizado para assegurar a integridade e confidencialidade das informações à serem enviadas para protocolos da camada superior que opera com o TLS (STALLINGS; BROWN, 2016).

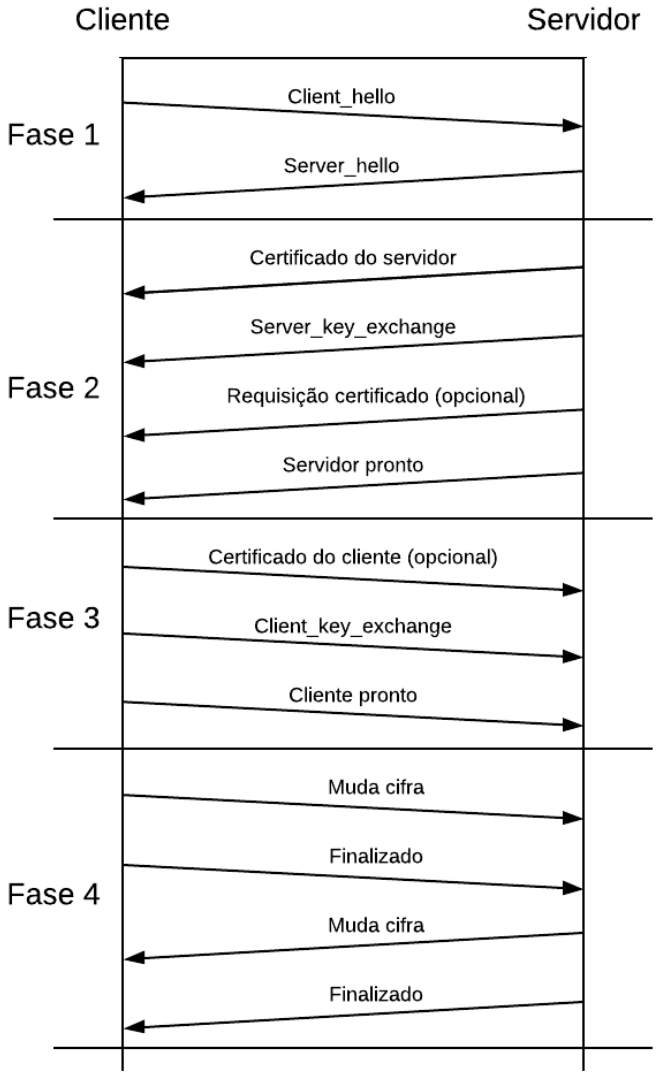
Já o protocolo de mudança de cifra é o mais simples. Esse consiste em apenas uma mensagem com um único *byte* com o valor 1, contendo como único propósito, indicar que um estado pendente seja copiado para o estado atual fazendo com que o conjunto de cifras utilizado nessa conexão seja atualizado (STALLINGS; BROWN, 2016).

O protocolo de alerta é responsável por enviar alertas às partes relacionadas na comunicação que está utilizando o TLS. Cada mensagem desse protocolo consiste contém dois campos de um *byte* cada. O primeiro *byte* é responsável por indicar o tipo de alerta, sendo o valor um para aviso(1) ou dois para alerta fatal(2). Sendo que, se a mensagem for um alerta fatal a conexão é encerrada imediatamente. Já o segundo *byte* é responsável por indicar qual o tipo de alerta, assim esse contém o valor do código que indica a descrição do alerta (STALLINGS; BROWN, 2016).

A parte mais complexa e importante do TLS é o protocolo *handshake*. Esse protocolo é o responsável por negociar os parâmetros de segurança que serão utilizados na conexão, e pela autenticação do servidor e cliente, sendo o último opcional (STALLINGS; BROWN, 2016).

O protocolo *handshake* é usando antes que qualquer dado de aplicação seja transmitido, e consiste em uma série de mensagens trocadas entre o cliente e o servidor, divididas em quatro fases, usadas para estabelecer uma conexão segura, como mostra a figura 12.

Figura 12 – Representação protocolo *handshake*



Fonte: Adaptado de (STALLINGS; BROWN, 2016).

A primeira fase é responsável por definir alguns parâmetros de segurança e iniciar a conexão entre o cliente e o servidor. Essa é iniciada pelo cliente que envia para o servidor uma mensagem "client_hello" com uma requisição de conexão, na qual possui seus parâmetros de configurações que são: o conjunto de cifras, versão do protocolo, um número aleatório, um ID de sessão e algoritmos de compressão (STALLINGS; BROWN, 2016).

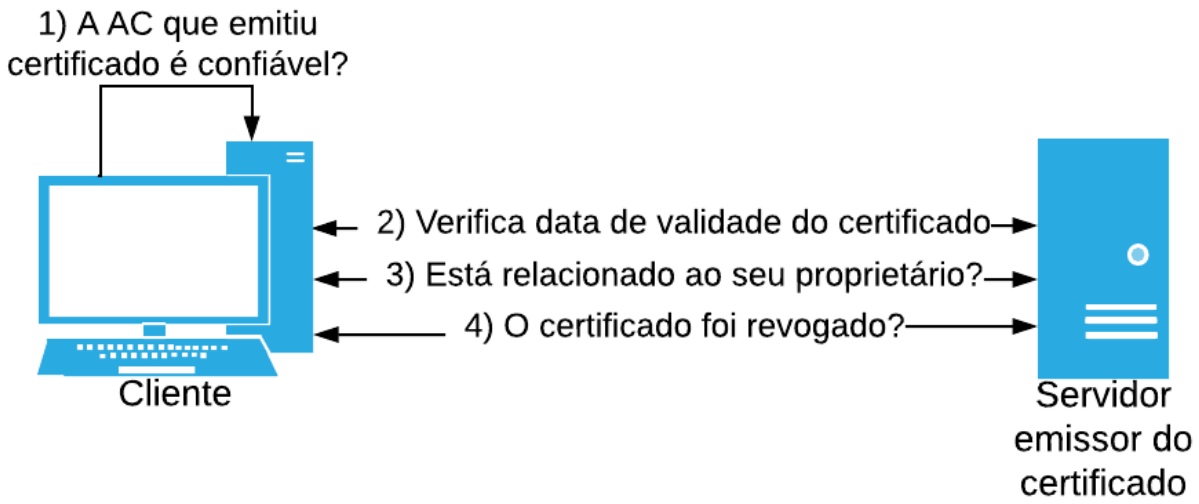
Após enviar a mensagem, o cliente aguarda a pela resposta "server_hello" possuindo a melhor configuração para estabelecer uma conexão segura entre eles, de acordo com os parâmetros enviados pelo cliente. Sendo que, essa resposta abrange os mesmos parâmetros enviados pelo cliente (STALLINGS; BROWN, 2016).

A segunda fase depende do método de autenticação, nesse trabalho será abordado apenas a autenticação pela certificação digital. Assim, o servidor envia o seu certificado, no formato padrão X.509, para que o cliente possa autenticá-lo. Em alguns casos, o servidor pode exigir o cliente que o envie um certificado (STALLINGS; BROWN, 2016).

Antes de finalizar, o servidor pode ou não, dependendo do algoritmo de troca de chave negociado, enviar a mensagem "Server_Key_Exchange" com informações necessárias para que o cliente também tenha condições de gerar a chave secreta à ser utilizada pelo protocolo de registro. Em seguida, o servido envia uma mensagem "Server_done" e aguarda pela resposta do cliente (MACEDO, 2008).

Na terceira fase, o cliente verifica se o certificado digital enviado pelo servidor, é válido, confiável e de fato, está relacionado ao seu proprietário (MACEDO, 2008). Também é verificado o período de validade e informações adicionais, como por exemplo, se o certificado já foi revogado, o processo pode ser visualizado na Figura 13.

Figura 13 – Verificação certificado digital



Fonte: Elaborado pelo autor.

Além disso, é verificado se parâmetros do "server_hello" é válido, e também, dependendo do algoritmo de troca de chave negociado anteriormente, enviar a mensagem "Server_Key_Exchange" para contribuir na criação da chave (STALLINGS; BROWN, 2016).

Na última fase, o cliente gera sua chave a ser utilizada pelo protocolo de registro, a partir das informações trocadas nas mensagens de "Server_Key_Exchange" e "Server_Key_Exchange". Em seguida, envia uma mensagem "Muda cifra" ao servidor para informá-lo de que o conjunto de cifras à ser utilizado deve ser atualizado. Para isso, seu estado pendente é copiado e se tornar atual. Feito isso, o cliente envia uma mensagem para "Finalizado" encerrar sua parte no

protocolo *handshake* (STALLINGS; BROWN, 2016).

Em resposta a essas duas mensagens, o servidor envia seu próprio "Muda cifra" e "Finalizado", indicando que copiou o seu estado pendente para estado atual, e encerrou sua parte no protocolo *handshake*. Nesse ponto, o cliente e servidor está pronto para trocar dados de aplicação de forma segura (STALLINGS; BROWN, 2016).

2.6 Sistema de Nomes de Domínios (DNS)

Criado em 1983, o DNS surgiu com objetivo de mapear nomes de *hosts* em endereços IP. A essência do DNS é a criação de um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura (TANENBAUM; WETHERALL, 2011).

O procedimento de tradução de um nome em endereço IP começa quando um programa aplicativo chama um resolvedor e repassa o nome como parâmetro. O resolvedor realizar uma consulta com o nome recebido em um servidor DNS local, que retorna o endereço IP ao resolvedor. Este, em seguida, retorna o endereço IP ao programa aplicativo que fez a chamada (TANENBAUM; WETHERALL, 2011).

Para gerenciar a um grande conjunto de nomes que está em mudança constante, o DNS é divido em domínios. Todo domínio pode ser divido em subdomínios, ou possuir um único *host*, ou então pode representar uma empresa possuindo milhares de *hosts* (TANENBAUM; WETHERALL, 2011).

Todo domínio, pode ter um conjunto de registros de recursos associado a ele. Esses registros são usados para mapear os domínios, assim quando o DNS recebe um nome de domínio do resolvedor, ele busca pelos registros de recursos associados àquele nome (TANENBAUM; WETHERALL, 2011).

Um registro de recurso é formado por cinco campos, são eles:

- Nome domínio: Informa o domínio ao qual esse registro se aplica. Este campo é utilizado para satisfazer as consultas sobre um determinado tipo de registro;
- Tempo de vida: Fornece uma indicação da estabilidade do registro;
- Classe: Especifica a qual classe o registro presente no campo valor pertence. Na prática esse campo sempre será representado pela classe IN, pois essa classe representa um registro de internet;
- Tipo: Informa qual é o tipo do registro. A Tabela 2 mostra os tipos mais comuns de registro;
- Valor: O valor que será usado para preencher cada campo, podendo ser um número, um nome de domínio ou uma string, dependendo do tipo de registro.

Tabela 2 – Tipos de registro no DNS

Tipo	Significado	Valor
SOA	Início de autoridade	Parâmetros para essa zona
A	Endereço IPv4 de um *host*	Inteiro 32 bits
AAAA	Endereço IPv6 de um *host*	Inteiro 128 bits
MX	Troca de mensagem de correio	Prioridade, domínio disposto a aceitar correio eletrônico
NS	Servidor de nomes	Nome de um servidor para este domínio
CNAME	Nome canônico	Nome do domínio
PTR	Ponteiro	Nome alternativo de um endereço IP

Fonte: (TANENBAUM; WETHERALL, 2011).

Um registro SOA fornece dados descritos pela autoridade do domínio autoridade do domínio, ou seja, a entidade responsável por seus registros oficiais. Assim é fornecido, o nome da principal fonte de informações sobre a zona do servidor de nomes, o endereço de correio eletrônico do administrador, um número de série exclusivo e diversos flags e timeouts (TANENBAUM; WETHERALL, 2011).

O tipo de registro A contém o um nome, e o endereço IPv4 de 32 bits de algum *host*. Já o registro AAAA correspondente ao nome e a um endereço IPv6 de 128 bits. Além disso, cada *host* deve ter pelo menos um endereço IP. Sendo que, alguns podem têm dois ou mais registros de recurso do tipo A ou AAAA. Consequentemente, o DNS pode retornar vários endereços para um único nome (TANENBAUM; WETHERALL, 2011).

O tipo de registro MX especifica o nome do *host* preparado para aceitar mensagens de correio eletrônico para o domínio especificado (TANENBAUM; WETHERALL, 2011). Registros MX permitem que os nomes de *host* de servidores de correio tenham apelidos simples (KUROSE; ROSS, 2013).

Outro tipo de registro é o NS, esse especifica um servidor de nomes para o domínio ou subdomínio. Esse registro é usado para encaminhar consultas DNS ao longo da cadeia de consultas (KUROSE; ROSS, 2013).

Os registros CNAME permitem a criação de nomes alternativos, ou seja, um o segundo nome ou apelido para um registro de domínio (TANENBAUM; WETHERALL, 2011).

O PTR também é um tipo de registro que indica outro nome. No entanto, esse depende da interpretação do contexto no qual se encontra. Na prática, esse é utilizado na pesquisa inversa, o qual segue o caminho oposto da pesquisa direta no DNS normal, pois traduz endereços IP em nomes de domínio. (TANENBAUM; WETHERALL, 2011).

Sobre a organização do DNS, esse é composto de zonas não superpostas. Cada zona está associada a um ou mais *host*, que mantêm o banco de dados para essa zona. Para melhorar a confiabilidade, alguns dos *host* podem estar localizados fora da zona. (TANENBAUM; WETHERALL, 2011).

3 Trabalhos Relacionados

Os certificados digitais têm sido amplamente utilizados para o processamento de dados e para a troca de mensagens e documentos entre cidadãos, governo e empresas, pois capaz de garantir capaz de garantir autenticidade e não-repúdio às informações eletrônicas.

No caso especifico de certificados digitais em redes locais, existem softwares para criação de ACs internas onde o usuário ou a empresa é o responsável por administrá-la, sendo encarregado pela gerência dos certificados apenas dessa rede, podendo disponibilizar os diferentes tipos de certificado dependendo de sua necessidade.

Assim, sabendo-se da extensão dessa tecnologia e com intuito de buscar trabalhos mais pertinentes ao problema proposto, foi realizado uma pesquisa sobre a certificação digital. Assim, foram selecionados alguns trabalhos com propósito de apresentar de forma prática as vantagens do uso dessa tecnologia em diferentes áreas.

3.0.1 Certificação Digital

Em seu trabalho, Macedo (2008) faz um estudo sobre certificação digital mostrando seu funcionamento e como essa é gerenciado no Brasil. Nesse é apresentado os tipos de certificados pessoais tais como e-CPF e certificados de email, e-CNPJ, e o passo a passo para obtê-los. Também, é abordado os conceitos de segurança sobre TLS, e métodos de identificação para um *website* seguro. Assim, Macedo (2008) mostra a importância do certificado digital, e como esse vem ganhando espaço em diversos setores para segurança da troca de informação.

3.0.2 Certificação digital: Análise da Aplicação da Certificação Digital, nos Escritórios de Contabilidade da Cidade de Balsas-MA

Sousa (2010) realiza um estudo sobre a certificação digital e suas aplicações para o ambiente de contabilidade. Assim, foi feito uma pesquisa descritiva-quantitativa com os profissionais de contabilidade atuantes na cidade de Balsas, a fim de verificar o impacto da certificação digital na área contábil foi realizada.

Nesse trabalho, foi utilizado como método de coleta de dados, o questionário, que foi aplicado a profissionais de empresas de contabilidade da cidade de Balsas. Sendo que, o questionário foi respondido pelo contador responsável pelo escritório.

Por fim, foi concluido que houve evolução tecnológica principalmente nos serviços da receita federal, e que o crescimento da tecnologia da informação veio para trazer muitos benefícios para todos os profissionais. No entanto, os impactos financeiros e estruturais nas empresas ainda são pequenos pelo motivo de estarem em fase de adaptação e implementação da tecnologia.

3.0.3 Os mais recentes ataques de segurança SSL: origens, implementação, avaliação e contramedidas sugeridas

Wassim (2011) apresenta uma breve visão geral dos ataques realizados na implementação do SSL e analisa mais detalhadamente os ataques recentes que exploram os serviços que o SSL usa. Nesse, foram explorados os cinco ataques que têm como alvo o SSL, são eles: *sniffing* ao SSL, certificado de colisão MD5, *stripping* ao SSL, prefixo SSL Null e o ataque ao protocolo de status de certificado *online*(OCSP). Sendo a maioria deles ataques do tipo *Man in the Middle*[1] (MitM).

Em seguida, foi discutido as origens de cada ataque citado acima e explicado o ambiente típico que permite que tais ataques ocorram, mostrando que muitos dos ataques comerciais sobre SSL é baseada na exploração de vulnerabilidades de design. Na maioria das ocasiões não é o protocolo de segurança em si, mas sim o design inadequado de modelos de confiança e navegadores da WEB que constituem as principais fontes de perigosos ataques como o MitM (WASSIM, 2011).

No estudo apresentado por Wassim (2011), foi implementado e testado situações com cada um dos ataques citados e realizado uma extensa avaliação sobre a taxa de sucesso desses quando vários navegadores são usados. Os navegadores que considerados foram: o *Internet Explorer*(IE), o Mozilla Firefox, o Opera, o Safari e o Chrome. Na avaliação dos navegadores, Wassim (2011) mostrou que de todos os ataques citados anteriormente, exceto *Sniffing* ao SSL, podem ser executados em quase todos os navegadores. Expondo a vulnerabilidade do design dos navegadores para segurança SSL.

3.0.4 Certificação Digital: Importância e Aplicabilidade

Lolato e Kaufmann (2014) realiza uma contextualização sobre as aplicabilidades da certificação digital nos cenários nacional e internacional. O escopo desse trabalho buscou abordar especificamente a aplicação e a segurança aplicadas à tecnologia utilizada para agilizar os processos que utilizam a certificação digital. Para isso, foram realizados testes de validação buscando garantir a segurança empregada aos documentos digitais, nesses foram adotados aos padrões da ICP-Brasil. Assim, Lolato e Kaufmann (2014) mostra de forma geral as mudanças positivas que está nova tecnologia vem proporcionando aos negócios e às pessoas, e também, as implicações relacionadas à segurança das informações e como ela pode ser garantida pelo processo tecnológico da certificação digital.

3.0.5 Análise do estado da arte

Pode-se visualizar que o uso da certificação digital está crescendo junto com a evolução da comunicação, e vem sendo aplicado em diversas áreas com o objetivo de prover maior segurança na troca de informação. Também foi mostrado os mais diversos tipos de ataques que uma comunicação TLS está sujeita e como a utilização de uma melhor prática de

[1] Homem no Meio - O ataque MitM, é quando o invasor se posiciona entre duas partes que tentam comunicar-se, intercepta mensagens enviadas e depois se passa por uma das partes envolvidas (MALENKOVICH, 2013).

segurança para a configuração dos certificados e o conhecimento da comunicação segura do navegador, pelo usuário, é importante para o aumento da segurança.

No entanto, diferente do que o presente trabalho propõe, as análises dos trabalhos apresentados foram baseadas no certificado emitido por uma AC registrada pelo ITI, sendo que, a autenticidade também é necessária em alguns casos onde a opção da compra do certificado não é uma opção adequada.

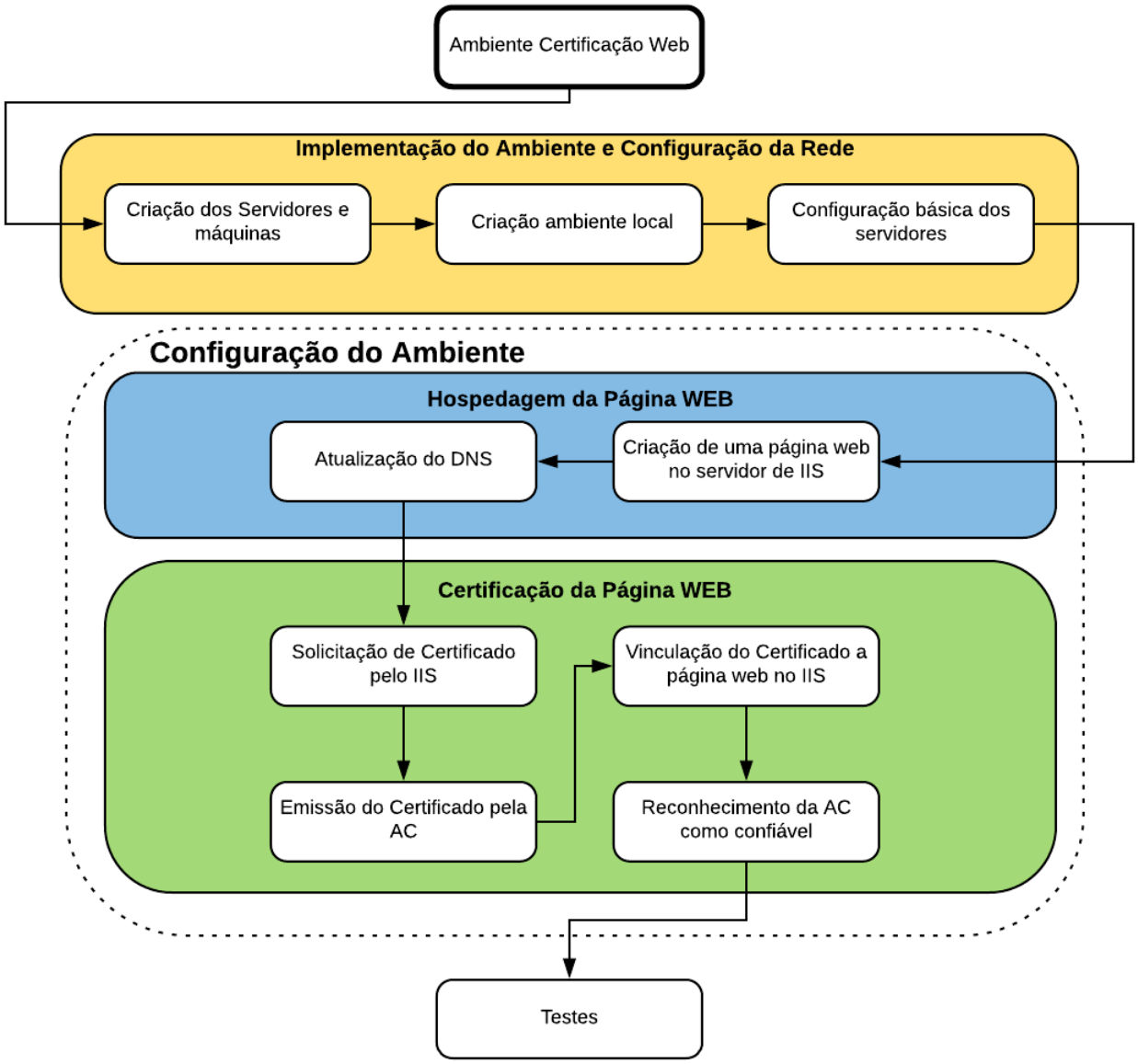
4 Materiais e Métodos

Esse trabalho é classificado como um estudo de caso, que segundo Godoy (1995) é uma pesquisa cujo o seu objeto é a análise profunda de um ambiente. Assim, tomando como base todo referencial teórico e estado da arte, foi implementado um ambiente local virtual com uma AC própria e feito um estudo sobre o uso da certificação digital para autenticação dos servidores WEB. O procedimento metodológico para o desenvolvimento deste trabalho foi dividido em três partes:

1. Levantamento e análise de tecnologias;
2. Implementação do ambiente;
3. Realização de testes.

O fluxograma da Figura 14 mostra uma visão geral desse trabalho. Todas as fases do fluxograma serão descritas nas próximas seções, com o objetivo de esclarecer o procedimento para o desenvolvimento deste trabalho.

Figura 14 – Fluxograma do trabalho de implementação e configuração do ambiente



Fonte: Elaborado pelo autor.

4.1 Levantamento e análise de tecnologias

Na primeira etapa desse trabalho foi realizado o levantamento, análise e escolha das tecnologias utilizadas para resolver o problema proposto. Essa talvez seja uma das etapas mais importantes do trabalho, pois uma escolha errada poderia levar tanto ao atraso do tempo de desenvolvimento até mudanças no objetivo do trabalho.

O estudo destes materiais, o referencial teórico e os trabalhos relacionados, possibilitaram um maior entendimento sobre certificação digital, tanto na parte teórica, quanto o seu funcionamento prático, auxiliando nas escolhas das tecnologias que foram utilizadas para resolução do problema. Após realizar o levantamento e a análise, foi feito a seleção, buscando

a melhor opção para se chegar à solução, com esse pensamento utilizou-se os seguintes critérios:

1. Simplicidade - facilidade de compreensão;
2. Custo - o preço do produto;
3. Qualidade - custo/benefício.

Levando em consideração os critérios anteriores, optou-se por realizar o estudo em um ambiente virtual, em função do custo de implementação para o trabalho de pesquisa. Desse modo, utilizou-se o software de virtualização Oracle VM VirtualBox, por ser simples, gratuito e de código aberto (VANOVER; HALETKY, 2010), além de atender a todas necessidades desse trabalho.

Para escolha dos sistemas operacionais dos servidores do ambiente proposto, o Windows Server 2012-r2 foi adotado. A motivação dessa escolha se deu pela simplicidade, facilidade de obtenção e o suporte para o software (OAKS, 2016). Além de conter as funções e recursos necessários para implementação da rede LAN proposta, como o DNS, Serviço de Informação da Internet(IIS)[1] e AC. Assim, simplificando e agilizando o processo de implementação.

Para a máquina dos testes, utilizou-se o sistema operacional Windows 7, motivado pela simplicidade, facilidade de uso e por ser um dos sistemas operacionais mais populares e utilizados no mundo (TOLHURST, 2013).

Para a escolha do navegador para realização dos testes, optou-se por utilizar um mais econômico em relação à recursos de *hardware*, uma vez que foi implementado um ambiente virtual com várias VMs em uma só máquina, o consumo de memória RAM e CPU se tornou a condição de escolha. Logo, optou-se pelo *Internet Explorer 11* já que esse exige menos recursos de *hardware* do computador do que as páginas equivalentes no Chrome ou no Firefox (ELLIS; COX, 2018).

Antes do início da implementação, definiu-se o número de servidores segregando as funções necessárias, motivado pela organização da rede, por isso foi determinado que seriam utilizados três servidores, são eles:

- ServDNS - DNS - Para a tradução do nome de domínios para endereço IP;
- ServIIS - IIS - Para hospedagem das páginas WEB da rede local;
- ServAC - AC - Para a gerência dos certificados digitais.

Para melhores práticas de segurança da comunicação entre usuário e servidor WEB, as configurações utilizadas para emissão dos certificados foram baseadas na análise feita por Ristic (2010) sobre o uso seguro do TLS, assim o presente trabalho utilizou:

[1] *Internet Information Service*

- A Chave privada com tamanho de 2048-bits;
- O Algoritmo de *Hash* SHA256;
- O Certificado emitido por servidor válido e confiável.

4.2 Implementação do ambiente

Para facilitar o entendimento, esta etapa foi dividida em duas partes. A primeira parte aborda a criação da LAN, nela é exemplificado a instalação do ambiente local virtual, a instalação dos servidores e as configurações das funções e recursos específicos de cada um, a instalação da máquina de teste, e por último a configuração de rede.

A segunda parte é a mais importante, pois trata a configuração do ambiente proposto para realizações dos testes, nela são mostrados os procedimentos para a criação e certificação de uma página WEB hospedada em um servidor.

4.2.1 Criação do ambiente proposto e configuração da rede interna

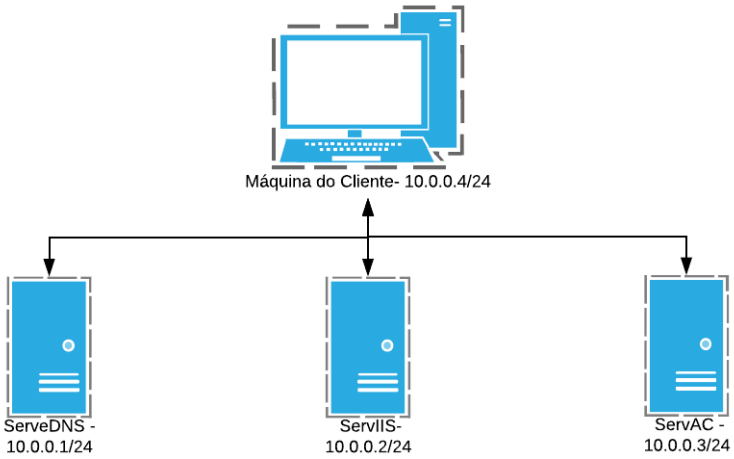
Para processo de criação do ambiente proposto foi utilizado o virtualizador escolhido, o Oracle VM VirtualBox. Nesse foram criados as quatro máquinas virtuais(VMs)[2] em um ambiente interno local virtual, são elas: os três servidores listados anteriormente utilizando o Windows-Server 2012-2, e uma máquina usuário com Windows 7 para a realização dos testes.

A configuração de rede interna virtual foi possível graças a opção de *internal network*[3] do virtualizador, que tem como função fazer com que todo o tráfego fique restrito à uma rede interna, onde somente as VMs selecionadas ficarão visíveis entre elas, e onde nem mesmo o próprio hospedeiro às enxergará.

A fim de atender as especificações de uma LAN, foi necessário configurar a rede interna, onde foi utilizado a faixa de IP 10.0.0.1 com a máscara 255.255.255.0/24. Após a configuração da rede, foi feito a configuração básica dos servidores, onde os servidores foram nomeados, e suas funções e recursos foram adicionadas. O passo-a-passo exemplificado o processo de adição de recursos de cada servidor está disponível no apêndice A, B e C. A Figura 15 ilustra o ambiente em conformidade com a configuração da LAN proposta, e a tabela 3 apresenta o resumo das configurações de cada uma das VMs.

[2] *Virtual machines*
[3] Rede interna

Figura 15 – Ambiente proposto



Fonte: Elaborado pelo autor.

Tabela 3 – Configurações das máquinas virtuais

Máquina Virtual	Nome	Sistema Operacional	IP	Serviço
Servidor 1	ServDNS	Windows Server 2012-2	10.0.0.1/24	DNS
Servidor 2	ServIIS	Windows Server 2012-2	10.0.0.2/24	IIS
Servidor 3	ServAC	Windows Server 2012-2	10.0.0.3/24	AC
Cliente	Cliente	Windows 7	10.0.0.4/24	Testes

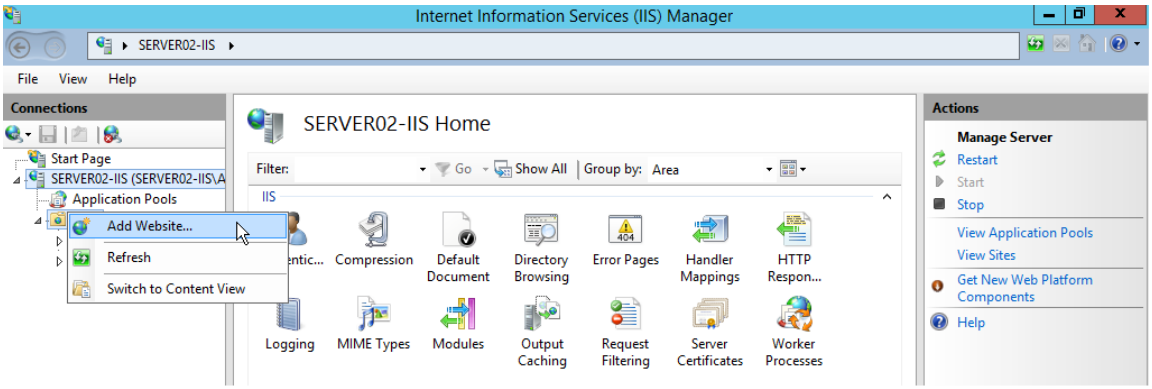
Fonte: Elaborado pelo autor

4.2.2 Configuração do ambiente proposto

Para configurar o ambiente, inicialmente foi necessário criar um arquivo com extensão HTML, ou seja, uma página WEB para ser hospedada e certificada, essa foi chamada de "index.html".

A hospedagem é feita pelo ServIIS, para isso utilizou-se o console de gerenciamento do IIS, onde foi adicionado um novo *site* a pasta de *Sites* do IIS, como mostra na Figura 16.

Figura 16 – Adição novo *Site*



Fonte: Elaborado pelo autor.

Para completar a criação foi necessário preencher o formulário com as informações da página WEB, são elas:

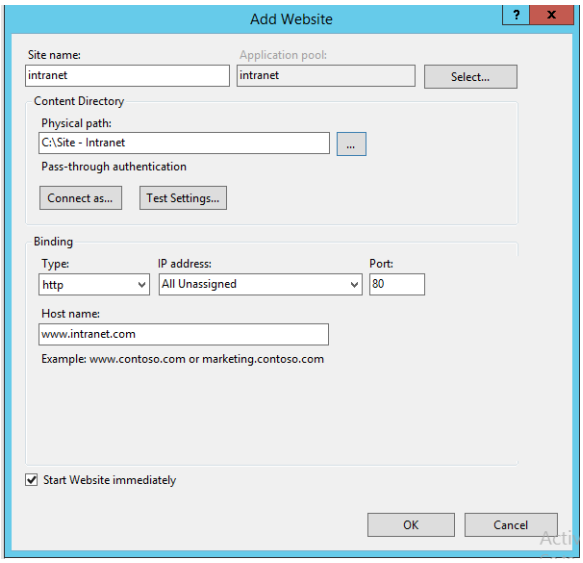
- *Site name* : Nome do *site* no IIS;
- *Application pool*: Exibe o *pool* de aplicativos selecionado para o *site*;
- *Physical path*: O caminho físico onde o conteúdo do *site* está armazenado;
- *Test Settings*: Avalia se as configurações de caminho são válidas;
- *Type*: tipo de conexão HTTP ou HTTPS;
- IP address: IP do servidor onde *Site* está armazenado;
- *Port*: A porta de comunicação do *site*;
- *Host* name: O nome do *host*, também conhecidos como nome de domínio;

O formulário é preenchido com os dados da página WEB pode ser visualizado na Figura 17.

Para que a página hospedada fosse acessada pelo nome de domínio (URL) foi necessário atualizar o DNS do ServDNS. Para esse estudo foi criado uma zona de pesquisa direta. O nome dado à zona criada no DNS deve ser o mesmo que o nome do domínio que se deseja utilizar, por esse motivo a zona foi nomeada como "intranet.com", desta forma, qualquer *host* dessa zona incluirá ao seu final o nome desse domínio.

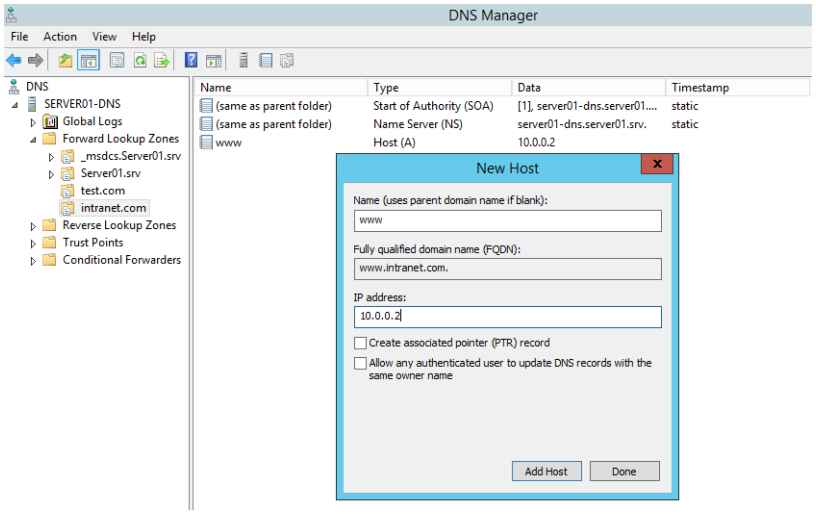
Na configuração da zona, para adicionar informações sobre do *host* nesse domínio, foi criado um registro do tipo HOST(A) com o nome do registro igual ao nome do *host* usado durante a criação de um *site* no IIS, "www.intranet.com", e com o endereço IP do *host*, o ServIIS, 10.0.0.2/24. Feito essas configurações, já foi possível realizar o acesso via URL. A Figura 18 mostra como é feito essa adição do novo *host* a um domínio no DNS.

Figura 17 – Configurações do *site*



Fonte: Elaborado pelo autor.

Figura 18 – Adição do *host* a zona de pesquisa direta



Fonte: Elaborado pelo autor.

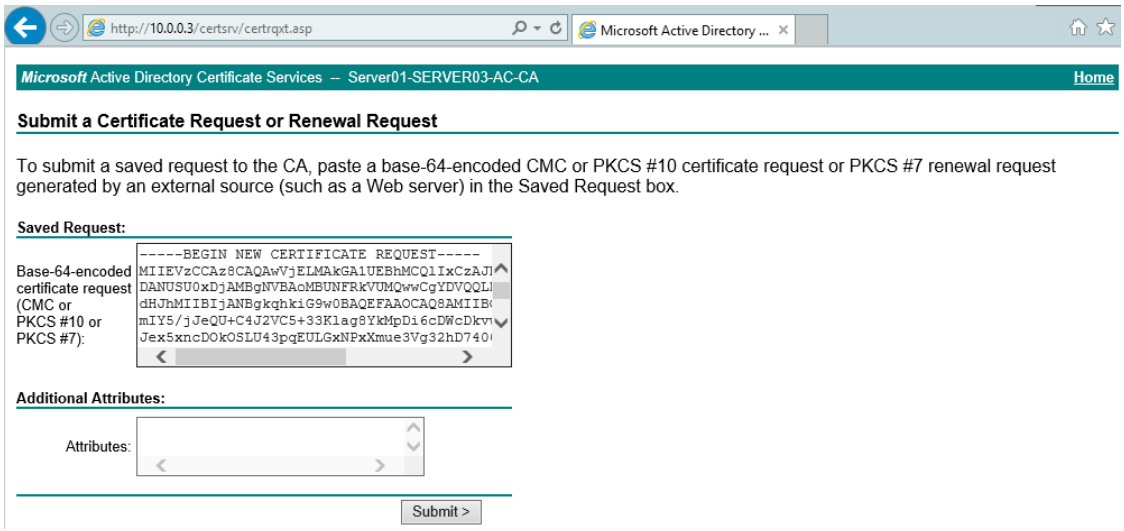
A última parte dessa etapa é a certificação da página WEB que ocorre em quatro fases, são elas: a solicitação, a emissão, vinculação, e o reconhecimento do certificado.

Para a realização da solicitação do certificado, primeiro foi criado uma requisição no console de gerenciamento do IIS contendo um texto codificada com informações da página WEB e o tipo de criptografia da chave privada do certificado, que foi enviado para AC através do Servidor de Certificado acessado via navegador, como é mostrado na Figura 19.

Feito a requisição, um processo foi aberto no servidor de certificado, de modo que, o ServIIS ao acessá-lo, pode visualizar as requisições enviadas e checar os seus status.

A emissão do certificado requisitado foi feita pela AC do ServAC, feito isso, o certificado

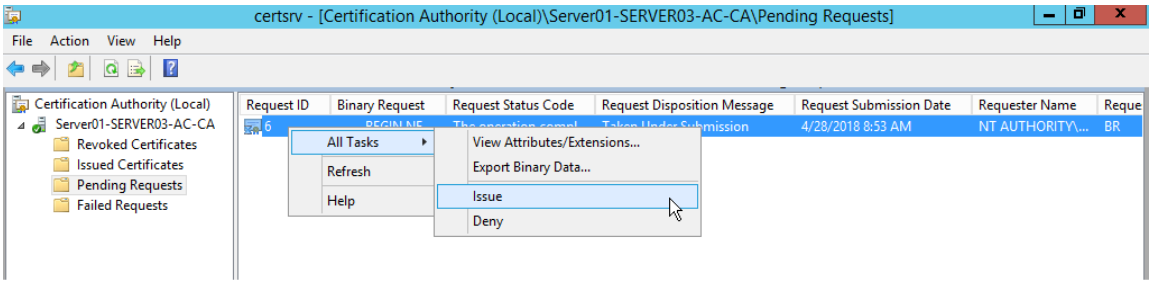
Figura 19 – Serviço de requisição



Fonte: Elaborado pelo autor.

foi assinado pela AC e adicionado a uma lista de certificados emitidos. Na Figura 20 pode ser visualizado os diretórios de uma AC, e a como é feito a emissão do certificado.

Figura 20 – Emissão certificado

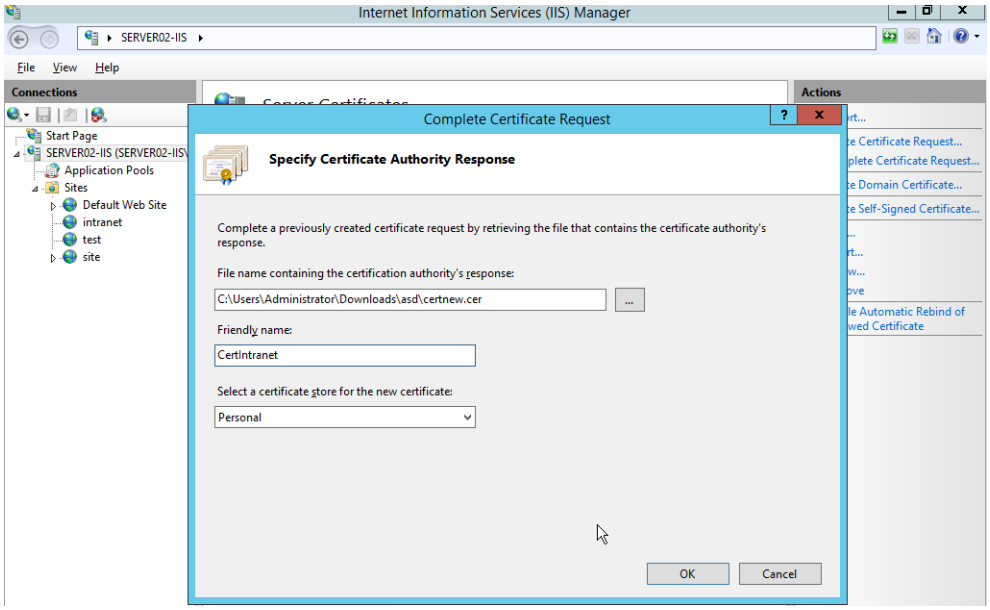


Fonte: Elaborado pelo autor.

Após a emissão do certificado, dois arquivos ficaram disponíveis no processo de requisição do ServISS no Servidor de Certificados: um com extensão .cer e o outro .p7b. O arquivo .cer contendo o certificado assinado com sua chave privada, e o arquivo .p7b o certificado assinado sem a chave privada e a cadeia de certificados com ACs Intermediárias. Em seguida, o arquivo .cer foi baixado manualmente pelo ServIIS em sua máquina e utilizado na conclusão da requisição do certificado, feita no gerenciador do IIS usando o arquivo e um nome para identifica-lo no IIS. A Figura 21 demonstra como é feito esse processo.

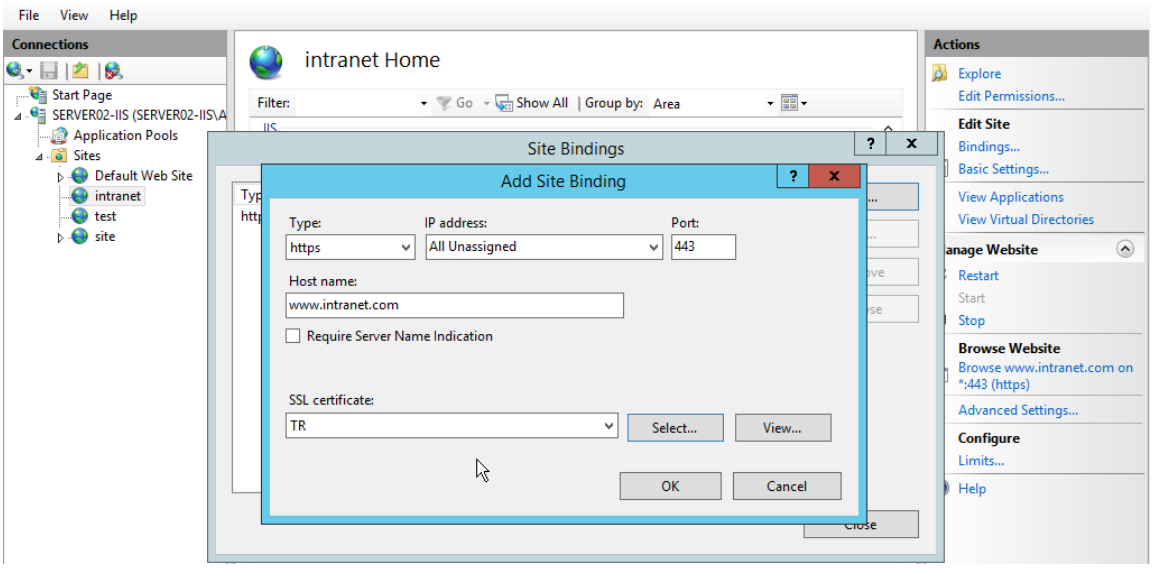
Para associar o certificado à página WEB, foi criado um novo vínculo do tipo HTTPS no *site* da página WEB, no console de gerenciamento do IIS, utilizando o certificado adicionado anteriormente. Em seguida, foi necessário remover o vínculo do tipo HTTP para que não existisse ambiguidade. A Figura 22 mostra as informações utilizados para criação de um novo vínculo.

Figura 21 – Adição novo certificado ao IIS



Fonte: Elaborado pelo autor.

Figura 22 – Vinculação certificado à página WEB

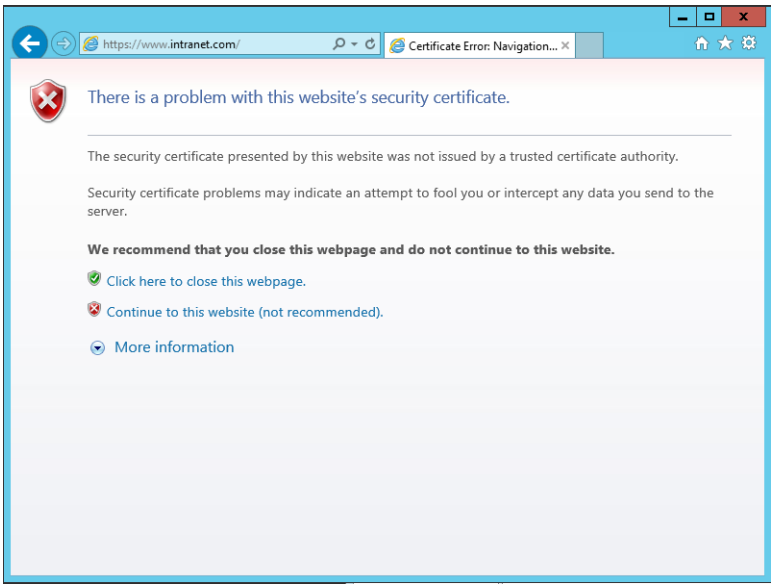


Fonte: Elaborado pelo autor.

Na última parte dessa etapa foi necessário fazer o reconhecimento da AC que emitiu o certificado da página WEB nas máquinas da rede interna. Para que, a mensagem de segurança, como na Figura 23, não surgisse quando o usuário acessasse à página WEB através de alguma máquina sem reconhecimento da AC.

Para realizar o reconhecimento da AC que emitiu o certificado da página WEB foi necessário adicioná-la à lista de autoridades confiáveis do Windows, que se encontra no *Mi-*

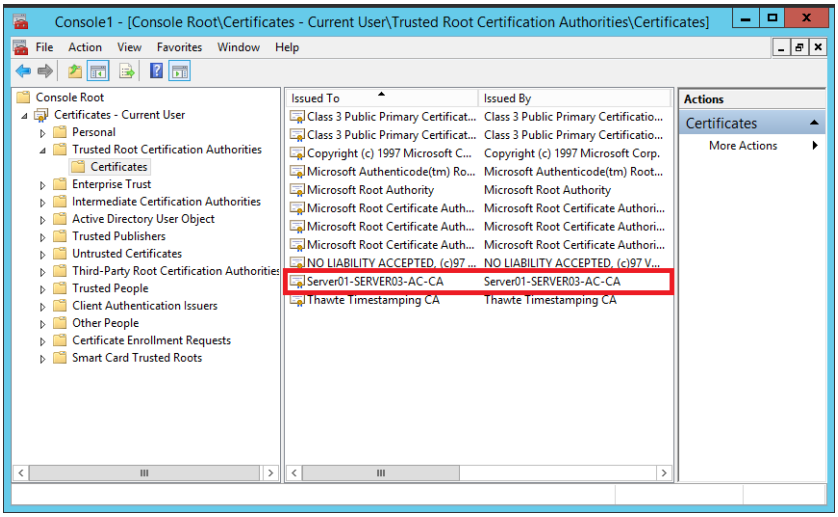
Figura 23 – Mensagem segurança



Fonte: Elaborado pelo autor.

crosoft Management Console[4](MMC), ou no caso da utilização de um *Active Directory* (AD), adicionar no Console de Gerenciamento de Diretiva de Grupo. Isso é necessário, porque os navegadores utilizam essa lista como referência para confiar ou não em um certificado de uma página WEB. Desse modo, após acessar o MMC foi adicionado o *Snap-in* de certificados da máquina, e na pasta de autoridade certificados confiáveis instalado o arquivo .p7b, emitido pela AC anteriormente. A Figura 24 mostra o certificado da AC do ServAC adicionado à lista de AC confiáveis do Windows.

Figura 24 – Lista de ACs confiáveis



Fonte: Elaborado pelo autor.

[4] Console de Gerenciamento da Microsoft

4.3 Testes

Com o objetivo de avaliar o uso da certificação digital para a autenticação do servidor WEB na LAN, a nível cliente, foram realizados testes utilizando o ambiente implementado em três diferentes situações. Essas situações têm o intuito de ilustrar os diferentes possíveis resultados para a visão do cliente após alguma ocorrência, seja ela acidental ou não, e também mostrar as vantagens desse método para a autenticidade da LAN, são elas:

- Situação 1 - Invasão no DNS;
- Situação 2 - Invasão da AC;
- Situação 3 - Invasão no DNS e na AC.

Em cada uma das situações acima, foi feito o acesso à página WEB "www.intranet.com"e comparado com as bases obtidas no cenário padrão, sem a invasão. Para obtenção dos dados, foram observadas três condições simples de segurança que estão presentes em servidores WEB com certificados. Essas foram selecionadas a partir do artigo escrito por Weeks (2017), que apresenta condições de verificação de uma página WEB, e do tutorial criado por Olenski (2017), que mostra como verificar detalhes de um certificado TLS no *Internet Explorer 11*. Logo, se em alguma das situações todas as condições forem satisfeitas, significa que a certificação não pode garantir a autenticidade para aquela situação.

Desse modo, buscou-se analisar os dados obtidos e compreender os limites da certificação para autenticação do servidor WEB no ambiente proposto utilizando o navegador *Internet Explorer 11*. Uma observação a ser feita sobre estas condições é que a primeira é válida para qualquer servidor, já a segunda e terceira varia de navegador para navegador. Segue abaixo as condições usadas para realizar as comparações:

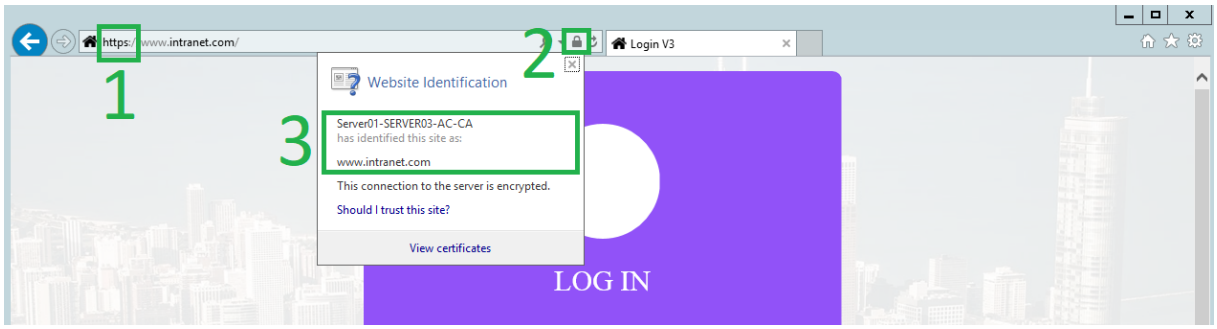
1. O Tipo da página WEB deve ser HTTPS;
2. O Certificado da página WEB deve ser assinado pelo ServAC e ser válido.
3. O Cadeado da página WEB deve estar "fechado";

A primeira é a página WEB ser do tipo HTTPS, denotando que essa tem um certificado digital para assegurar sua identidade.

Para a segunda condição é necessário que a primeira seja satisfeita, nessa é feito a verificação de quem emitiu o certificado da página e sua data de validade, para isso basta do clicar no cadeado da página WEB.

Por último o cadeado deve ser "fechado" indicando que o navegador reconhece e confia na AC que assinou o certificado daquela página WEB. A Figura 25 destaca em verde onde cada uma das condições estão localizadas.

Figura 25 – Acesso à página satisfazendo as condições



Fonte: Elaborado pelo autor.

Finalmente, o ambiente virtual foi criado e executado em um computador com processador Intel(R) Core(TM) i7-6700M com 2.8 GHz de frequência, 8 GB de memória RAM e o sistema operacional Windows 10 Home (64 bits).

5 Resultados

Este capítulo apresenta os resultados obtidos através da realização do presente trabalho. Assim, ele descreve os testes de comparação realizados entre as situações sem e com invasão citadas anteriormente. Por fim, é realizada uma análise dos resultados obtidos investigando as restrições da implementação de certificação do Servidor WEB em uma LAN.

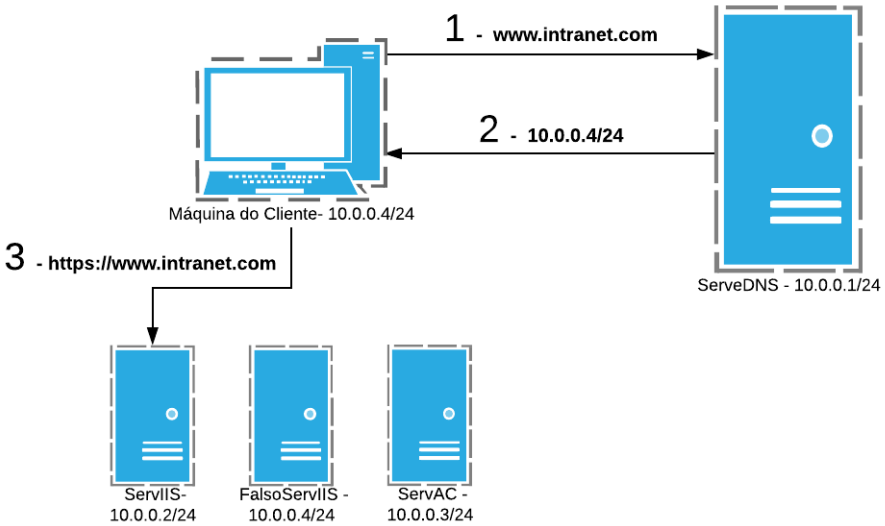
Para simulação das situações abaixo, foram criadas duas VMs para simular os servidores de AC e IIS do invasor. Este foi nomeada de FalsoServISS com IP 10.0.0.4/24, e aquela de FalsoServAC com IP 10.0.0.5/24.

5.1 Situação 1 - Invasão no DNS

A primeira simulação foi projetada com a finalidade de avaliar o comportamento do ambiente proposto para quando ocorrer uma invasão no DNS, alterando o IP do *host* da página WEB e o redirecionamento para outro servidor IIS.

Para tal, foi criado uma página WEB para o invasor, idêntica a página "www.intranet.com" para ser hospedada pelo FalsoServIIS. Sendo que, os testes foram realizados com a página do invasor do tipo HTTP e HTTPS, com certificado assinado pelo FalsoServAC. A Figura 26 ilustra fluxos para o acesso da página WEB "www.intranet.com" sem a mudança no DNS.

Figura 26 – Fluxo desejado

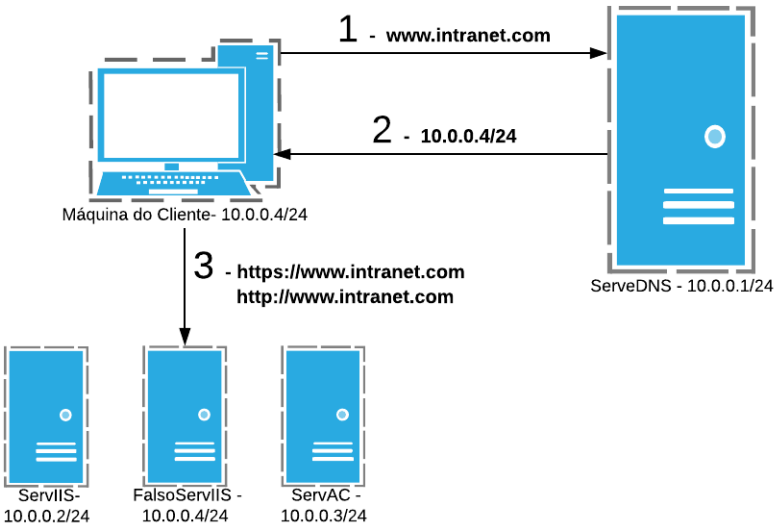


Fonte: Elaborado pelo autor.

Em um primeiro momento, para realização dos testes foi feito a alteração na zona "intranet.com" no DNS, nessa foi criado um novo HOST(A) para redirecionar o nome de domínio da página WEB "www.intranet.com" para o IP do FalsoServIIS, e posteriormente, foi excluindo

o HOST(A) antigo que redirecionava para o ServIIS. A Figura 27 ilustra o fluxo para o acesso da página WEB "www.intranet.com" com adulteração no DNS.

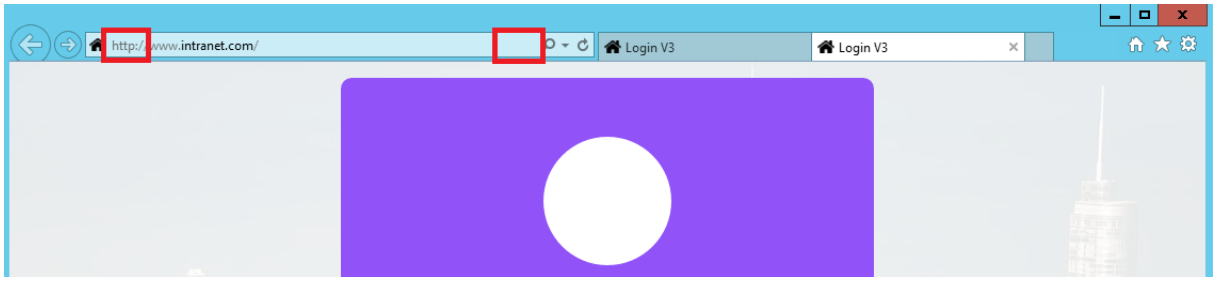
Figura 27 – Fluxo após troca IP host no DNS



Fonte: Elaborado pelo autor.

Em seguida, foi feito o acesso à URL "www.intranet.com", o qual foi redirecionado para o FalsoServIIS pelo DNS, e verificado as três condições citadas anteriormente para autenticação da página WEB. No teste das condições para página do tipo HTTP, nenhuma das condições foram satisfeitas, como pode ser visto na Figura 28 que mostra o resultado do acesso página WEB do tipo HTTP do invasor após o acesso. Também é importante ressaltar que a comunicação sem certificado para autenticação, do tipo HTTP, faz com que o servidor WEB fique mais vulnerável à ataques, como foi mostrado no capítulo 2, isso acontece, pois, o cliente não pode ter a certeza absoluta de que está se conectando ao servidor verdadeiro (DIERKS, 2009).

Figura 28 – Situação 1 - Acesso página HTTP

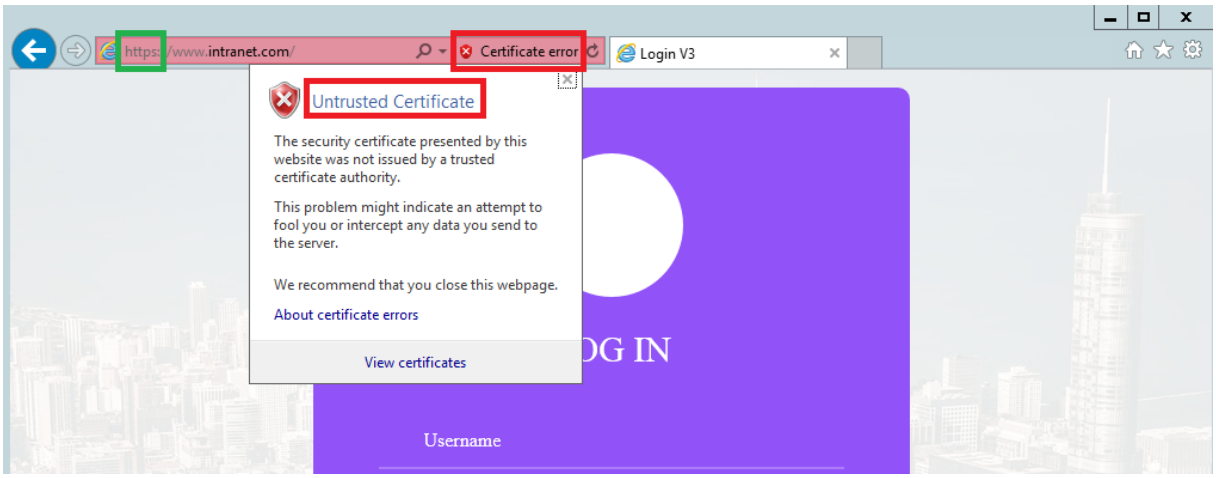


Fonte: Elaborado pelo autor.

No teste com página do tipo HTTPS, as condições de número dois e três não foram satisfeitas, pois o navegador não reconheceu o certificado da página WEB do invasor como confiável, pois esse foi emitido por uma AC não identificada como segura pela máquina, por

esse motivo uma mensagem de segurança igual à mostrada na Figura 23 aparece. O resultado para o teste com página HTTPS pode ser visto na Figura 29 onde é mostrado quais condições foram e quais não foram satifeitas.

Figura 29 – Situação 1 - Acesso página HTTPs



Fonte: Elaborado pelo autor

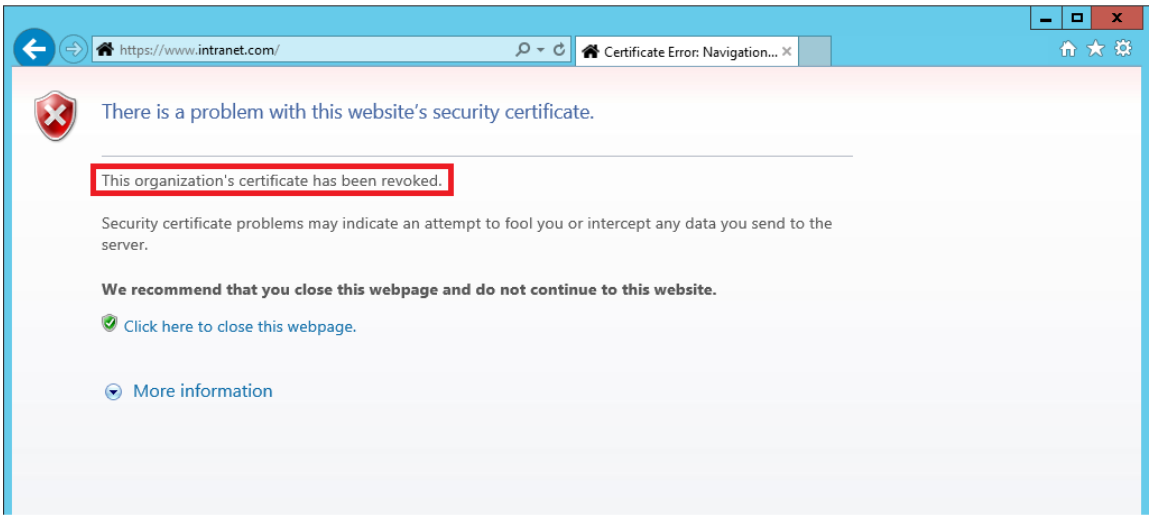
5.2 Situação 2 - Invasão da AC

A segunda situação foi projetada com finalidade de avaliar o impacto da emissão e/ou revogação dos certificados sem o reconhecimento dos administradores. Nessa, o invasor pode emitir certificados, e/ou revogar os certificados existentes na AC. Para tal, foram analisadas as duas perspectivas no ambiente local proposto, a primeira foi a emissão de um certificado pela AC para o FalsoServIIS, a segunda a revogação do certificado do ServISS na AC.

Para a emissão de um certificado para uma página WEB hospedada pelo FalsoServIIS, foi realizado o mesmo processo de certificação mostrado na seção anterior. No entanto, mesmo que essa satisfaça as três condições de acesso por ser certificada por uma AC confiável do ambiente, o DNS não reconhece e redireciona o IP do servidor do invasor para que os usuários possam acessá-lo. Sendo assim, mesmo com um certificado emitido pelo ServAC, o invasor não consegue redirecionar o acesso para o FalsoServIIS sem modificar o DNS.

Já com a revogação do certificado emitido para o ServIIS, o acesso dos usuário à esse é suspenso, isso devido a propriedade do TLS de verificação de identidade do servidor realizada pelo cliente, que verifica se o certificado do servidor e a identificação pública são válidos, o fluxo de verificação é mostrado na Figura 13. Desta forma, com a revogação do certificado o usuário não conseguirá acessar à página WEB do servIIS, a figura 30 mostra a mensagem de erro de segurança da página WEB após a tentativa de acesso à página "www.intranet.com" com o certificado revogado e a página suspensa.

Figura 30 – Situação 2 - Tentativa de acesso após revogação do certificado



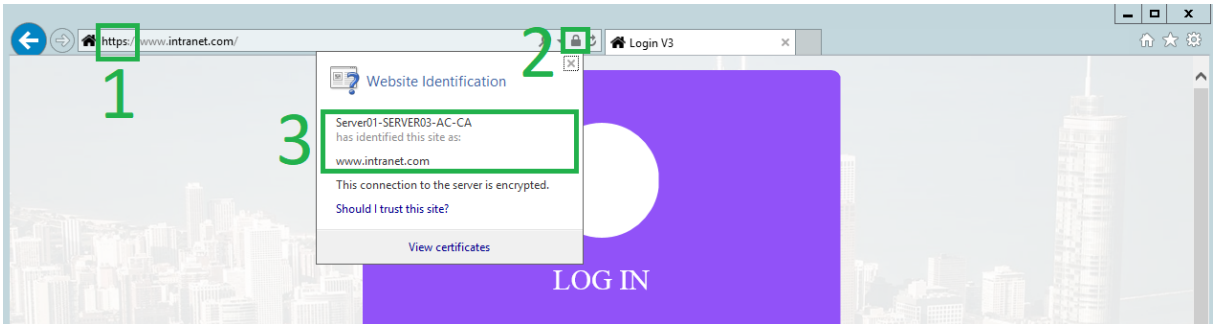
Fonte: Elaborado pelo autor.

5.3 Situação 3 - Invasão na AC e DNS

A última situação tem como objetivo analisar o pior cenário de invasão para o ambiente com AC própria, fazendo a junção da primeira e segunda situação. Para tal, também foi criado uma página WEB para o invasor, idêntica a página "www.intranet.com", o qual foi hospedada pelo FalsoServIIS, com o tipo HTTPS com certificado do ServAC.

Nesse cenário, o IP do *host* no DNS é redirecionado para o FalsoServIIS, como foi mostrado na primeira situação. Além disso, a página WEB hospedada pelo FalsoServIIS foi certificada pelo ServAC, o qual o ambiente proposto considera como uma AC confiável, como foi apresentado na segunda situação. O resultado do teste de acesso à página WEB é exposto na Figura 31 que mostra que todas as condições foram satisfeitas, consequentemente a certificação digital de uma página WEB utilizando uma AC própria não pode garatir a autenticidade do ambiente para essa situação.

Figura 31 – Situação 3 - Acesso página HTTPs



Fonte: Elaborado pelo autor.

5.4 Análise dos Resultados

Esta seção apresenta uma análise dos resultados descritos neste capítulo. Os resultados obtidos através dos testes das situações, relatados nas seções 5.1, 5.2 e 5.3, avaliam o ambiente implementado no capítulo 4. Quanto aos testes realizados, foi abordado apenas a visão do cliente. Esse trabalho não considera as questões de segurança no TLS, pois tem como pressuposto a implementação de um ambiente com melhores práticas de segurança para a comunicação entre usuário e servidor WEB. No presente trabalho, essas foram baseadas na análise feita por Ristic (2010) sobre o uso seguro do TLS, mostradas com capítulo 4.

A primeira situação testou a influência do DNS no ambiente local proposto. Os resultados apresentados foram bastante interessantes, pois o navegador conseguiu identificar a ocorrência do redirecionamento no DNS, sem a necessidade de ferramentas adicionais, só a nível cliente, como mostra a Figura 29. Tal fato, pode ser explicado pelo uso do certificado digital e pelas configurações do ambiente implementado, que permitiu ao navegador reconhecer como não confiável o certificado utilizado na página WEB do invasor, desse modo, identificando uma violação ou abuso interno no DNS.

A segunda situação, por sua vez avaliou a importância da AC para autenticidade do ambiente. Por se tratar do responsável dos certificados digitais, os resultados foram obtidos a partir de testes realizados com emissão e revogação de certificados sem reconhecimento do administrador. A análise desse cenário, permitiu identificar alguns pontos importantes.

De modo geral, a emissão de certificado feita por uma AC confiável para um servidor WEB, desconhecido pelo DNS, não o fez ser inserido no ambiente. Consequentemente, os testes realizados a nível cliente não foram suficientes para avaliar essa ocorrência. Um fato importante observado nessa situação é que o DNS interno ofereceu segurança para o cliente, uma vez que, o controle dos nomes de domínios e os respectivos IPs é interno, diferente dos DNS do ambiente WAN.

Na revogação de um certificado já emitido pela AC confiável, diferente do anterior, foi possível identificar uma ocorrência de violação ou falha no ambiente, pois resultou na indisponibilidade da página WEB vinculada ao certificado revogado, após a verificação do certificado, como mostrado na Figura 30.

A terceira situação demonstrou um cenário onde a autenticidade é corrompida de modo que não foi possível detectar nenhuma ocorrência de ataque, a nível de cliente, apenas com os testes realizados, como relatado na Figura 31.

É importante destacar também que esses resultados são válidos apenas para as situações com servidores certificados cadastrados no DNS interno de uma LAN, pois o uso do DNS também auxiliou para a identificação dos servidores da rede. Diferente de uma situação de rede de longa distância(WAN)[1], onde o DNS utilizado normalmente é público. Assim, se uma AC externa for invadida já é suficiente para corromper autenticidade dos certificados emitidos por ela, pois o usuário não conseguirá diferenciar se o certificado é válido ou não. No entanto, a segurança oferecida por uma AC externa é superior a uma AC interna.

[1] *Wide Area Network*

6 Conclusão

A partir dos estudos e das pesquisas realizadas a respeito do certificado digital, o presente trabalho foi elaborado com a proposta de realizar um estudo de caso sobre a implementação e o uso da certificação digital, emitida por uma AC interna, para a autenticação dos servidores WEB de uma LAN. Para tal, foi implementado um ambiente virtual com servidores de DNS, IIS e AC, onde foram criados e realizado testes de autenticidade a nível do cliente. Com os resultados obtidos nos testes foi possível avaliar o método de certificação digital para o caso proposto. Permitindo assim, que o objetivo geral do trabalho fosse alcançado.

A utilização desse método além de ser simples e fácil de implementar, trouxe vantagens para a segurança do usuário e da rede. Os testes realizados apresentaram resultados satisfatórios para a segurança do usuário e do ambiente tanto no cenário com a invasão no DNS, quanto com a invasão da AC. Assim, a implementação de uma AC interna mostrou os mesmos benefícios de uma AC externa. No entanto, quando comparado as duas, a diferença se encontra unicamente na segurança da entidade, onde a AC externa, por sua vez, é uma entidade criada para oferecer segurança e autenticidade aos certificados emitidos, diferente da AC interna que é utilizada apenas para auxiliar na segurança da rede.

Diante disso, o presente trabalho realizou um estudo sobre um método para prover autenticidade para os servidores WEB de uma LAN utilizando a certificação digital emitida por uma AC interna. Sendo uma alternativa viável por oferecer segurança de baixo custo para ambientes, no qual não é acessível a opção da compra de um certificado de uma AC externa.

Devido ao conteúdo extenso de segurança da computação e certificação digital, podem ser exploradas do presente trabalho em futuros estudos os módulos que não foram contemplados neste trabalho. Dentre essas, estão:

- A implementação desse método em um ambiente real;
- Adaptar o método para certificação de usuários para autenticação e controle na rede;
- Avaliar e comparar os softwares de ACs.

Referências

DIERKS, T. *The Transport Layer Security (TLS) Protocol Version 1.2*. 2009. Acessado em 26 de julho de 2018. Disponível em: <https://tools.ietf.org/pdf/rfc5246.pdf>. Citado na página 49.

ELLIS, C.; COX, A. *The best web browser 2018: faster and more secure*. 2018. Acessado em 26 de julho de 2018. Disponível em: <https://www.techradar.com/news/the-best-web-browser>. Citado na página 38.

FOROUZAN, B. A. *Protocolo TPC/IP*: 3ªedição. São Paulo: McGrawHill, 2008. Citado nas páginas 17, 18 e 27.

GODOY, A. S. Pesquisa qualitativa tipos fundamentais. *Revista de Administração de Empresas*, São Paulo, SP, v. 35, n. 3, p. 20–29, 1995. Citado na página 36.

Instituto Nacional de Tecnologia da Informacao. *Certificação Digital*. 2017. Acessado em 26 de julho de 2018. Disponível em: <http://www.iti.gov.br/certificado-digital>. Citado na página 15.

Instituto Nacional de Tecnologia da Informação. *Certificação Digital*. 2013. Acessado em 26 de julho de 2018. Disponível em: <http://www.beneficioscd.com.br/cartilha_online/?pagina=oq04>. Citado na página 26.

Instituto Nacional de Tecnologia da Informação (ITI). *Certificação Digital*. 2017. Acessado em 26 de julho de 2018. Disponível em: <http://www.iti.gov.br/certificado-digital>. Citado na página 14.

JUNIOR, J. H. *Certificado Digital*. 2009. Curso de Especialização em Redes e Segurança de Sistemas, PUCPR (Universidade Católica do Paraná) , Curitiba, Brasil. Citado na página 15.

JÚNIOR, M.; SILVA, F. M. da. *Certificação digital no Poder Judiciário do Estado do Ceará*. 2008. Trabalho de Conclusão de Curso(Especialista em Administração Judiciária), UVA (Universidade Estadual Vale do Acaraú) , Fortaleza, Brasil. Citado nas páginas 23 e 25.

KUROSE, J. F.; ROSS, K. W. *Redes de Computadores e a Internet*: 6ªedição. São Paulo: Pearson, 2013. Citado nas páginas 14, 17, 18, 19, 20, 22, 23, 25 e 32.

LOLATO, T.; KAUFMANN, E. R. Certificação digital: Importância e aplicabilidade. *Unoesc Ciência - ACET*, Joaçaba, SC, v. 5, n. 1, p. 39–52, 2014. Citado na página 34.

MACEDO, S. X. de. Certificação digital. 2008. Projeto Final de Especialista em Desenvolvimento de Sistemas para Web, Universidade Estadual de Maringá, Paraná, Brasil. Citado nas páginas 30 e 33.

MALENKOVICH, S. *O que é um Ataque Man-in-the-Middle?* 2013. Acessado em 26 de julho de 2018. Disponível em: <https://www.kaspersky.com.br/blog/what-is-a-man-in-the-middle-attack/462/>. Citado na página 34.

MARCACINI, A. T. R. *Certificação Eletrônica na Legislação Brasileira Atual*. 2007. Acessado em 26 de julho de 2018. Disponível em: <http://www.buscalegis.ufsc.br/revistas/files/anexos/27423-27433-1-PB.pdf>. Citado na página 24.

MONTEIRO, E. S.; MIGNONI, M. E. *Certificados Digitais: Conceitos e Práticas*: 1ªedição. Rio de Janeiro: Brasport, 2007. Citado na página 14.

MORENO, E. D.; PEREIRA, F. D.; CHIARAMONTE, R. B. *Criptografia em Software e Hardware*. São Paulo: Novatec, 2005. Citado na página 18.

NASCIMENTO, A. C. do. *Criptografica e Infraestrutura de Chaves Públicas*. 2009. <http://home.ufam.edu.br/regina_silva/CEGSIC/Textos%20Base/Criptografia_e_ICP.pdf>. Acessado em 26 de julho de 2018. Citado nas páginas 25 e 26.

OAKS, A. *Mac, Windows, or Linux? How to choose the best operating system for your business*. 2016. Acessado em 26 de julho de 2018. Disponível em: <https://www.itproportal.com/2016/08/18/mac-windows-or-linux-how-to-choose-the-best-operating-system-for-your-business/>. Citado na página 38.

OLENSKI, J. *How to View SSL Certificate Details in Each Browser and What You Can Learn*. 2017. Acessado em 26 de julho de 2018. Disponível em: <https://www.globalsign.com/en/blog/how-to-view-ssl-certificate-details/#ie>. Citado na página 46.

REZENDE, L. A. *Avaliação de Segurança do uso de TLS em Estações Servidoras na Rede da Universidade Federal de Goiás*. Goiás: [s.n.], 2016. Projeto Final de Curso de Ciência da Computação. Acessado em 26 de julho de 2018. Disponível em: <http://dcc.catalao.ufg.br/up/498/o/LorenaAparecidaRezende2016.pdf>. Citado nas páginas 22 e 24.

RISTIC, I. Internet ssl survey 2010. *Black Hat Technical Security Conference*, Las Vegas, EUA, 2010. Acessado em 26 de julho de 2018. Disponível em: <https://media.blackhat.com/bh-us-10/presentations/Ristic/BlackHat-USA-2010-Ristic-Qualys-SSL-Survey-HTTP-Rating-Guide-slides.pdf>. Citado nas páginas 38 e 52.

SAFRAN. *Entendendo a Certificação Digital*. 2010. Acessado em 26 de julho de 2018. Disponível em: <http://www.taskshop.com.br/task/paginas/SAG100.pdf>. Citado na página 14.

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. *Redes de computadores*: 2ªedição. São Paulo: Elservier, 1995. Citado nas páginas 17 e 18.

SOUSA, L. S. de. Certificação digital: Análise da aplicação da certificação digital, nos escritórios de contabilidade da cidade de balsas-ma. 2010. Projeto de Conclusão de Curso para Sistemas de Informação, UNIBALSAS, Maranhão, Brasil. Citado na página 33.

STALLINGS, W.; BROWN, L. *Computer Security, Principles and Practice*: 3ªedição. Hoboken, NJ: Pearson, 2016. Citado nas páginas 19, 20, 21, 22, 23, 27, 28, 29, 30 e 31.

TADANO, K. Y. *Certificação digital no Poder Judiciário do Estado do Ceará*. 2002. Trabalho de Conclusão de Curso(Bacharel em Ciência da Computação), UFMT (Universidade Federal do Mato Grosso, Cuiabá, Brasil. Citado na página 24.

TANENBAUM, A. S.; WETHERALL, D. *Redes de computadores*: 5ªedição. São Paulo: Pearson, 2011. Citado nas páginas 14, 17, 19, 24, 25, 26, 27, 31 e 32.

TOLHURST, C. *Windows or OS X? How to Choose the Best Operating System for Your Business*. 2013. Acessado em 26 de julho de 2018. Disponível em: <https://www.business.org/it/operating-systems/windows-or-osx-how-to-choose-the-best-operating-system-for-your-business/>. Citado na página 38.

TRINTA, F. A. M.; MACÊDO, R. C. de. *Um Estudo sobre Criptografia e Assinatura Digital*. Pernambuco: [s.n.], 1998. Departamento de Informática, Universidade Federal de Pernambuco. Acessado em 26 de julho de 2018. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Citado na página 18.

VANOVER, R.; HALETKY, E. *VMware vs. VirtualBox: Which is better for host-based virtualization?* 2010. Acessado em 26 de julho de 2018. Disponível em: <https://searchservervirtualization.techtarget.com/feature/VMware-Workstation-vs-VirtualBox>. Citado na página 38.

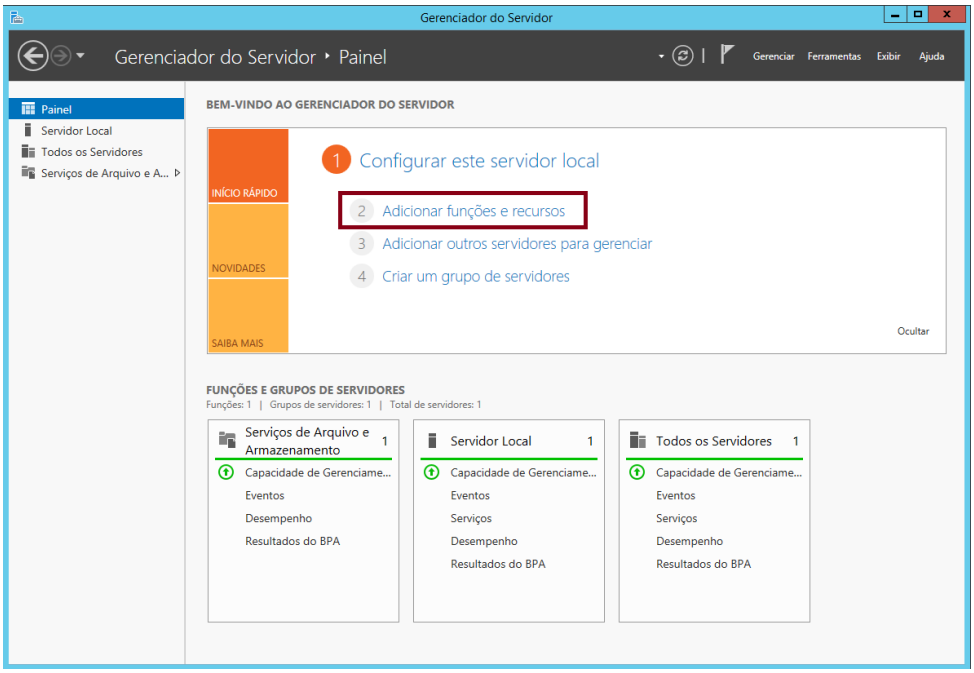
WASSIM, E. The most recent ssl security attacks: origins, implementation, evaluation, and suggested countermeasures. *Security and Communication Networks*, v. 5, n. 1, p. 113–124, 2011. Acessado em 26 de julho de 2018. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.295>. Citado na página 34.

WEEKS, C. *How to check if a website is safe*. 2017. Acessado em 26 de julho de 2018. Disponível em: <https://www.avg.com/en/signal/website-safety>. Citado na página 46.

Apêndices

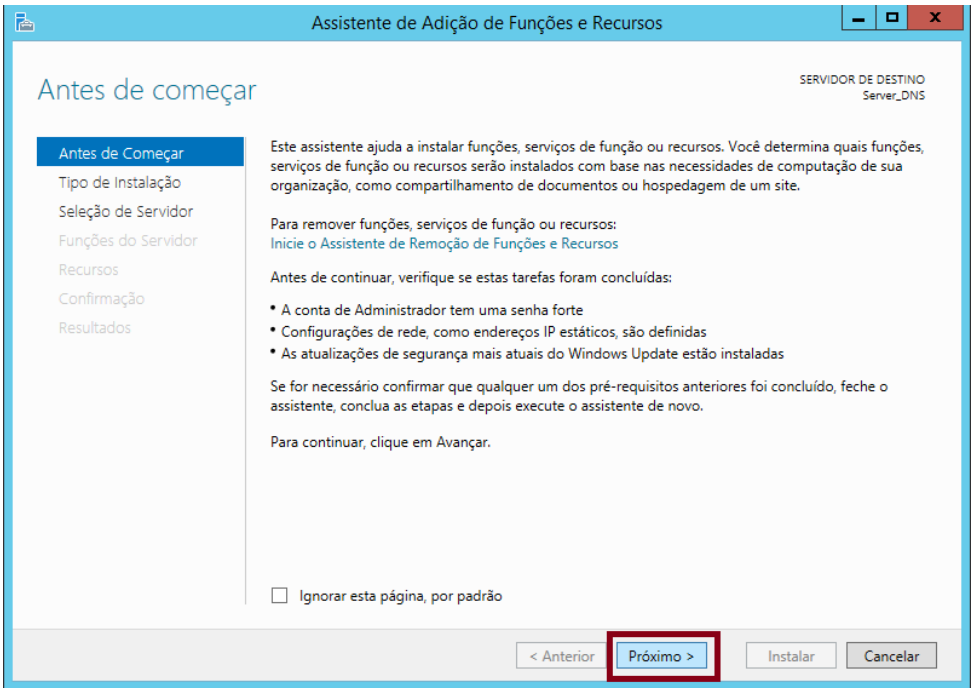
APÊNDICE A – Instalação e Configuração do Servidor de DNS

Figura 32 – Adição de funções e recursos no Gestor de Servidor



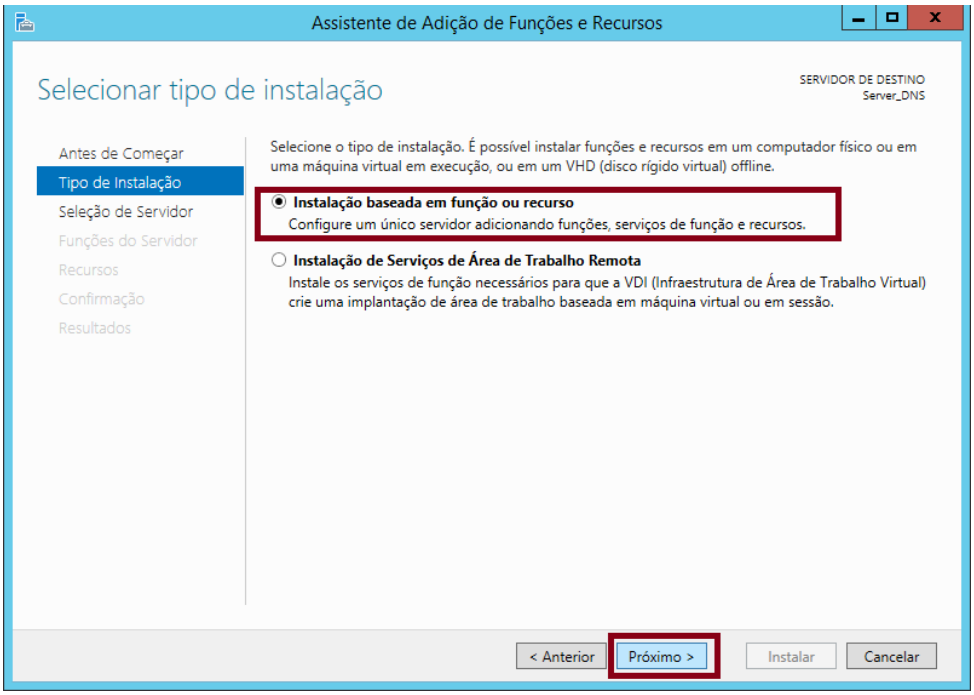
Fonte: Elaborado pelo autor.

Figura 33 – Confirmação dos pré-requisitos para instalação



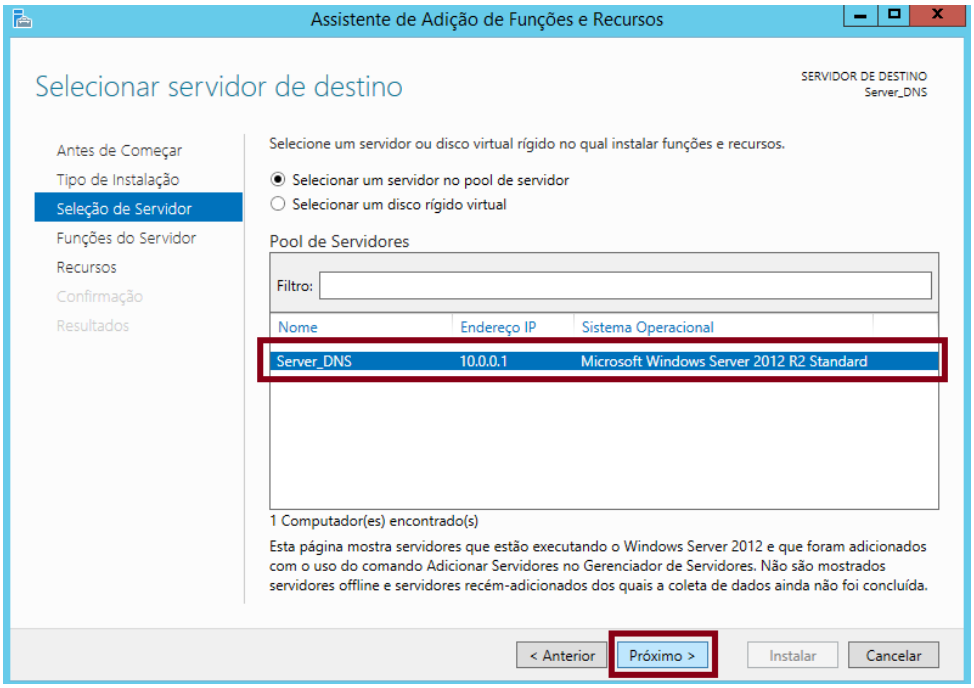
Fonte: Elaborado pelo autor.

Figura 34 – Seleção do tipo de instalação para o DNS



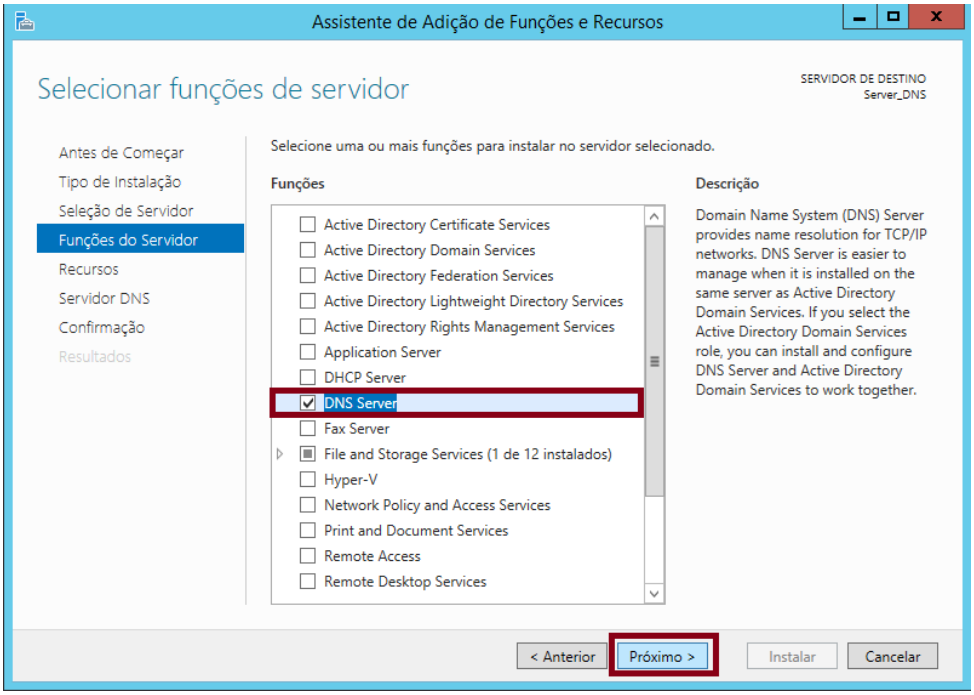
Fonte: Elaborado pelo autor.

Figura 35 – Seleção do servidor onde será instalado o DNS



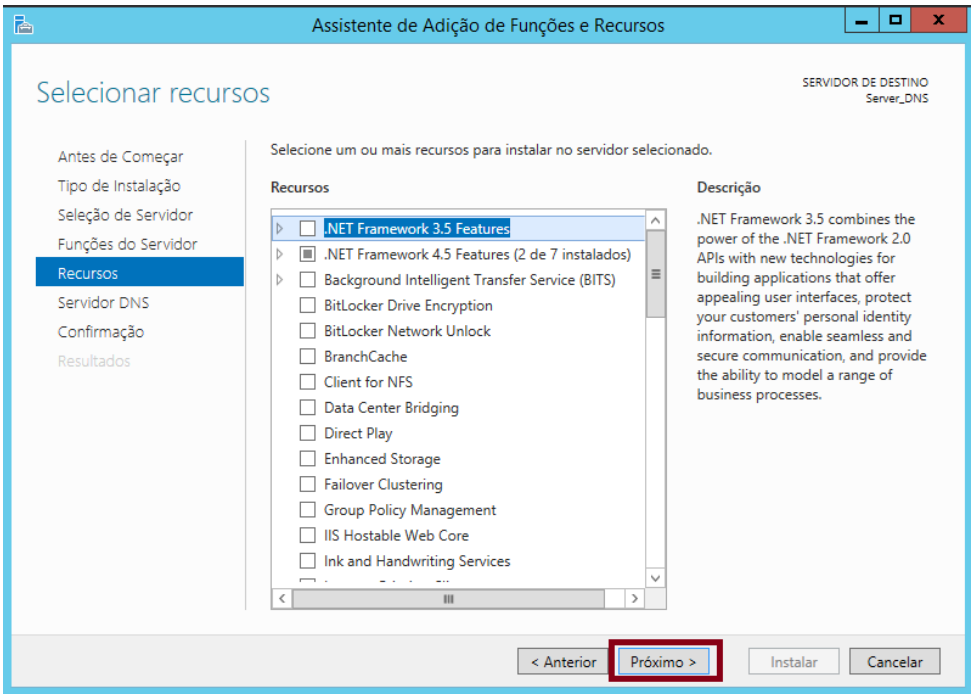
Fonte: Elaborado pelo autor.

Figura 36 – Seleção da função do DNS



Fonte: Elaborado pelo autor.

Figura 37 – Seleção de outros recursos para serem instalados no mesmo servidor que o DNS

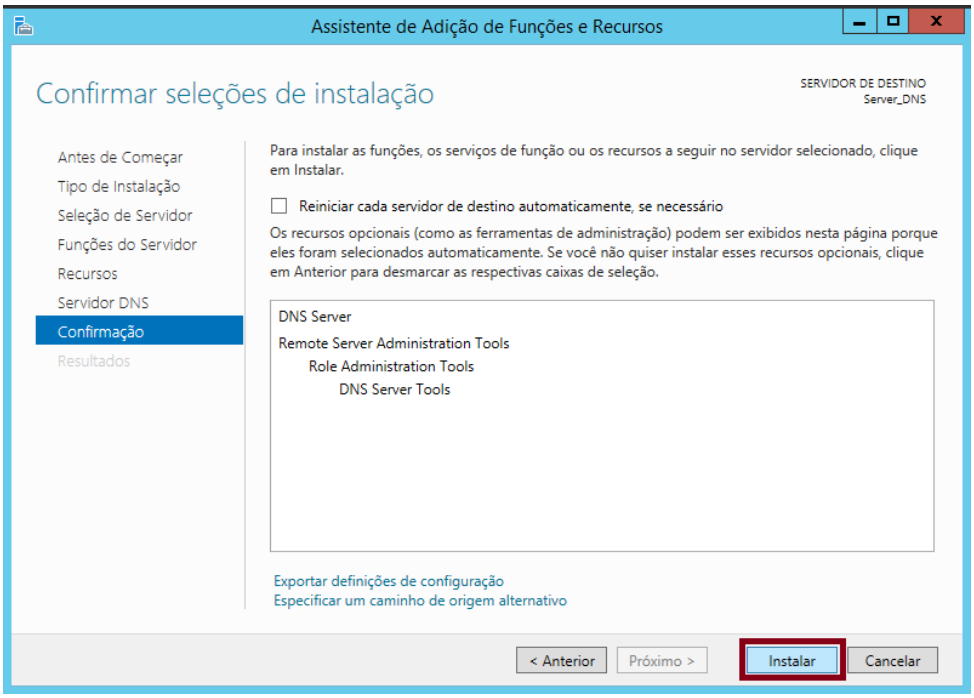


Fonte: Elaborado pelo autor.

Figura 38 – Observações sobre a instalação do DNS

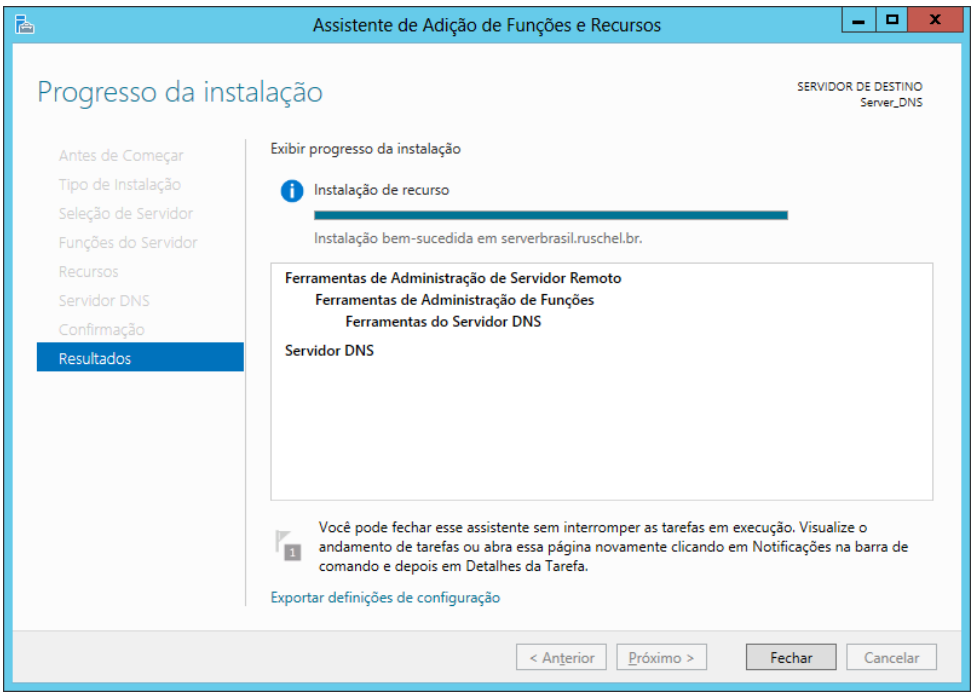
Fonte: Elaborado pelo autor.

Figura 39 – Confirmação das funções ou recursos que serão instalados



Fonte: Elaborado pelo autor.

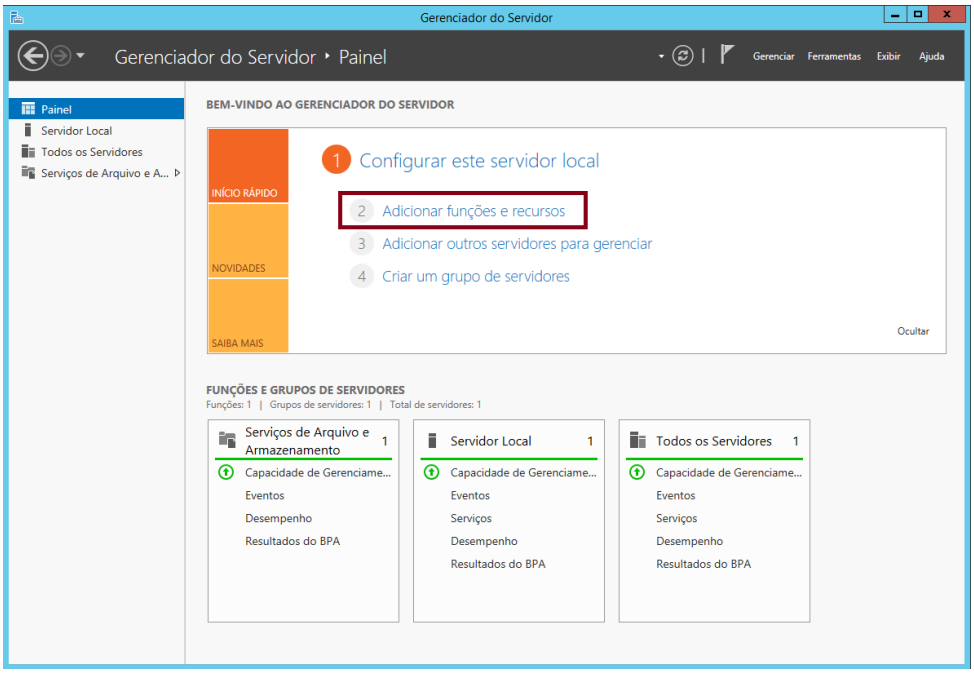
Figura 40 – Conclusão da instalação



Fonte: Elaborado pelo autor.

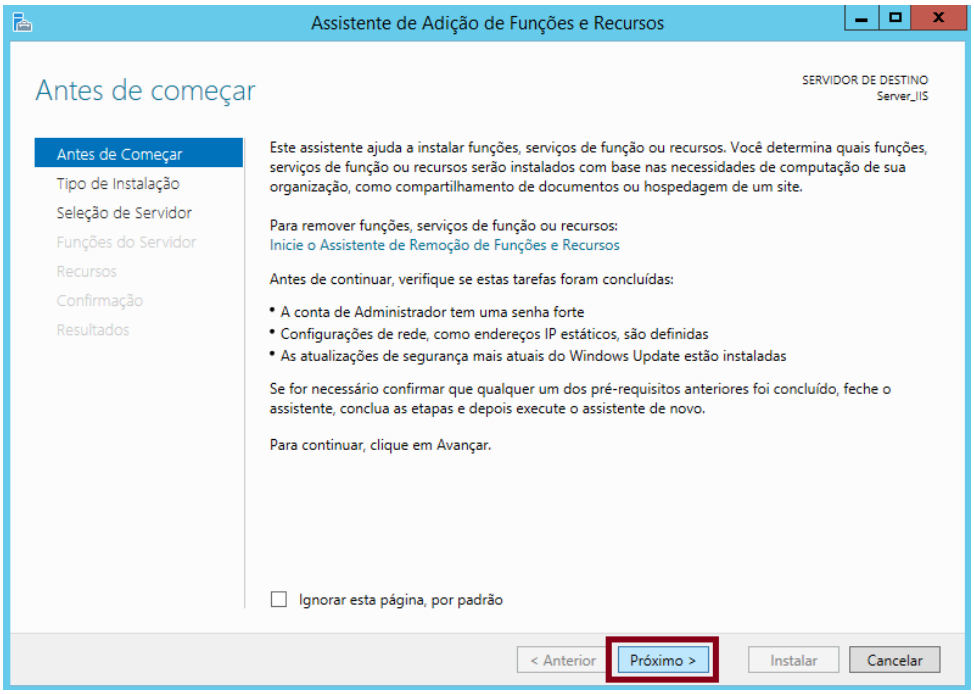
APÊNDICE B – Instalação e Configuração do Servidor de IIS

Figura 41 – Adição de funções e recursos no Gestor de Servidor



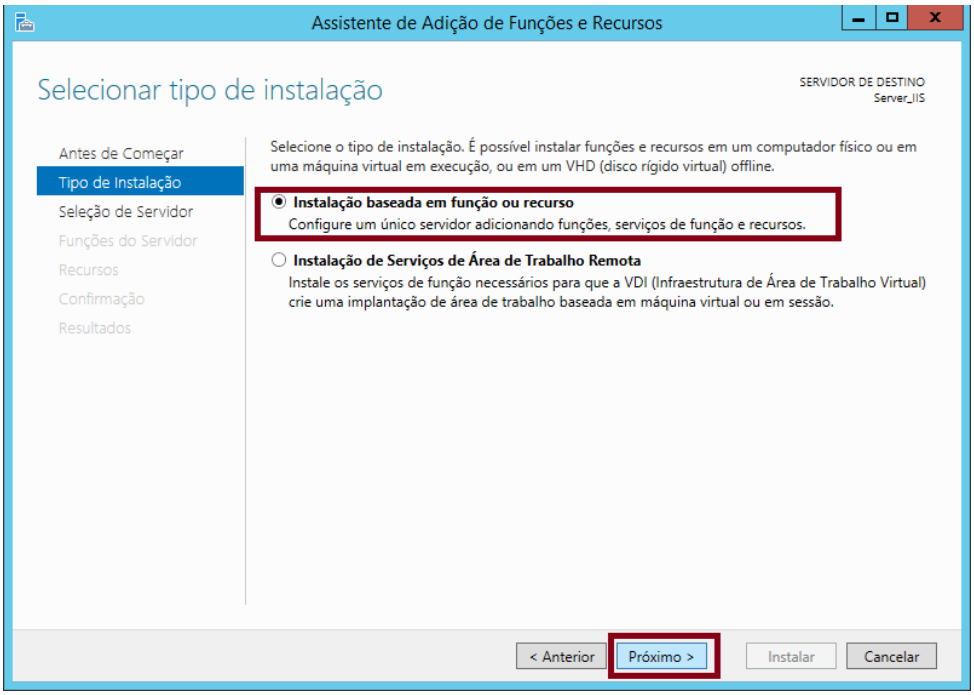
Fonte: Elaborado pelo autor.

Figura 42 – Confirmação dos pré-requisitos para instalação



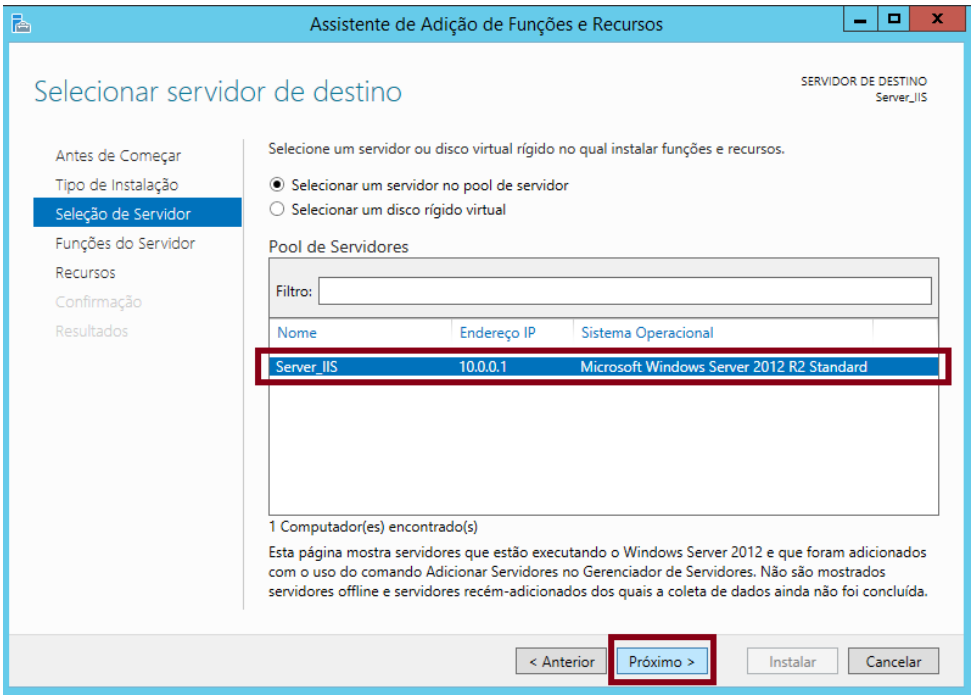
Fonte: Elaborado pelo autor.

Figura 43 – Seleção do tipo de instalação para o IIS



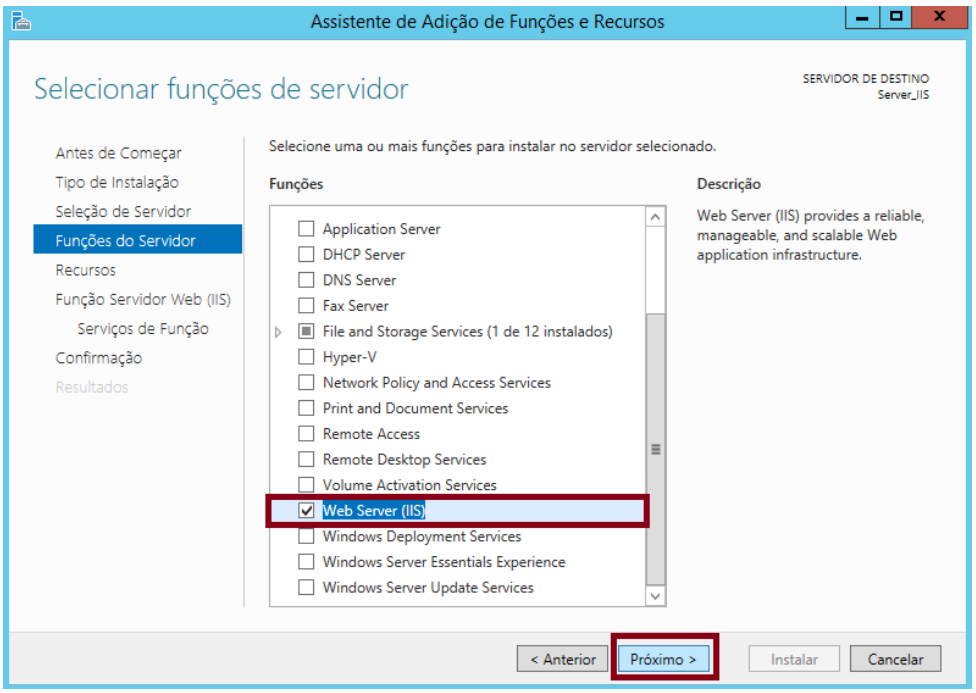
Fonte: Elaborado pelo autor.

Figura 44 – Seleção do servidor onde será instalado o DNS



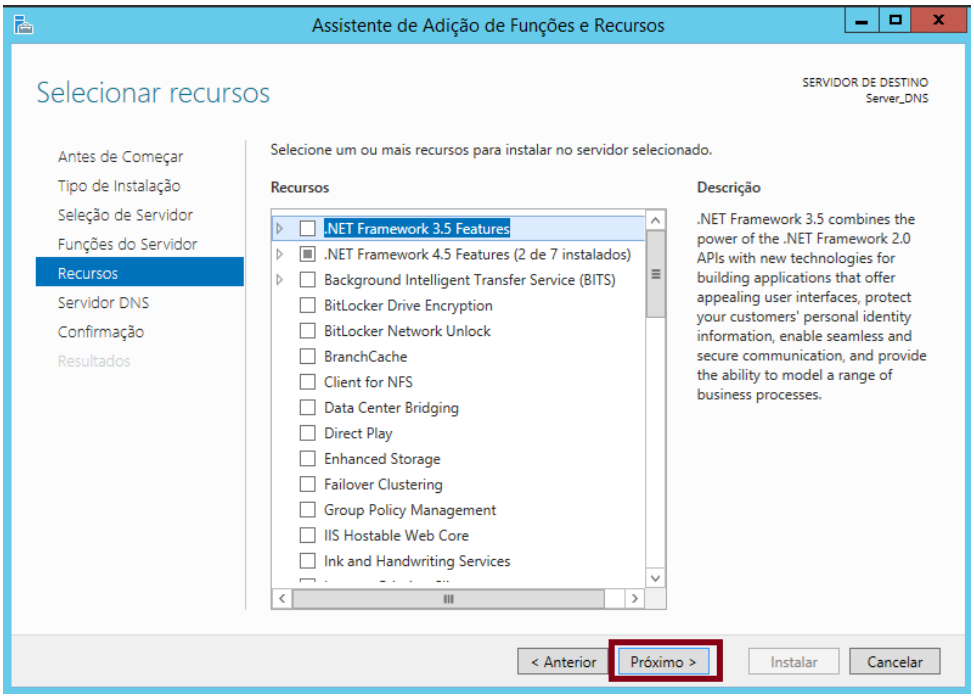
Fonte: Elaborado pelo autor.

Figura 45 – Seleção da função do IIS



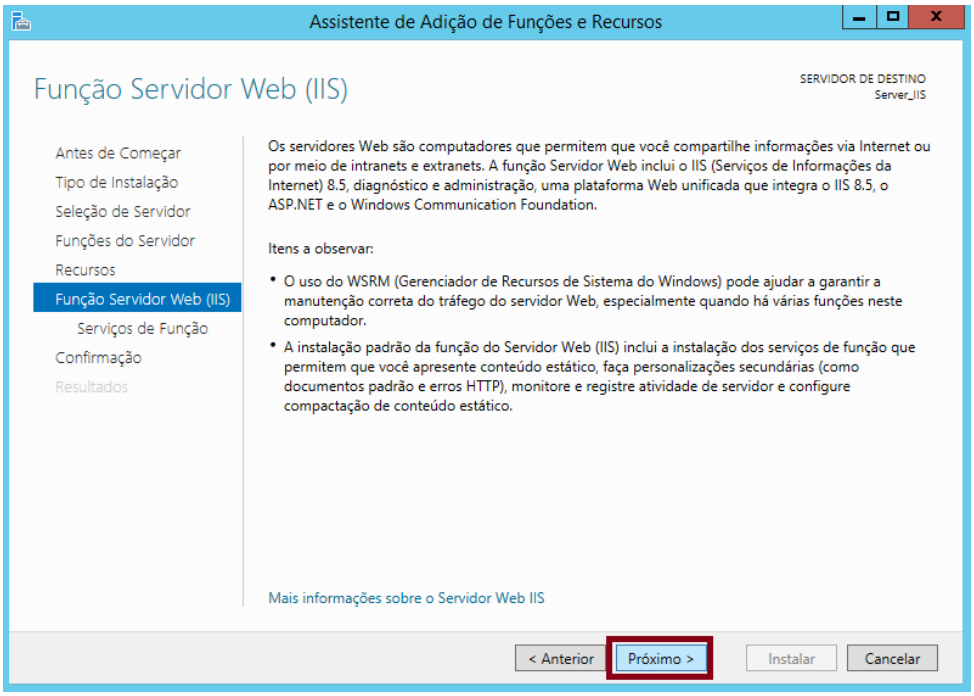
Fonte: Elaborado pelo autor.

Figura 46 – Seleção de outros recursos para serem instalados no mesmo servidor que o IIS



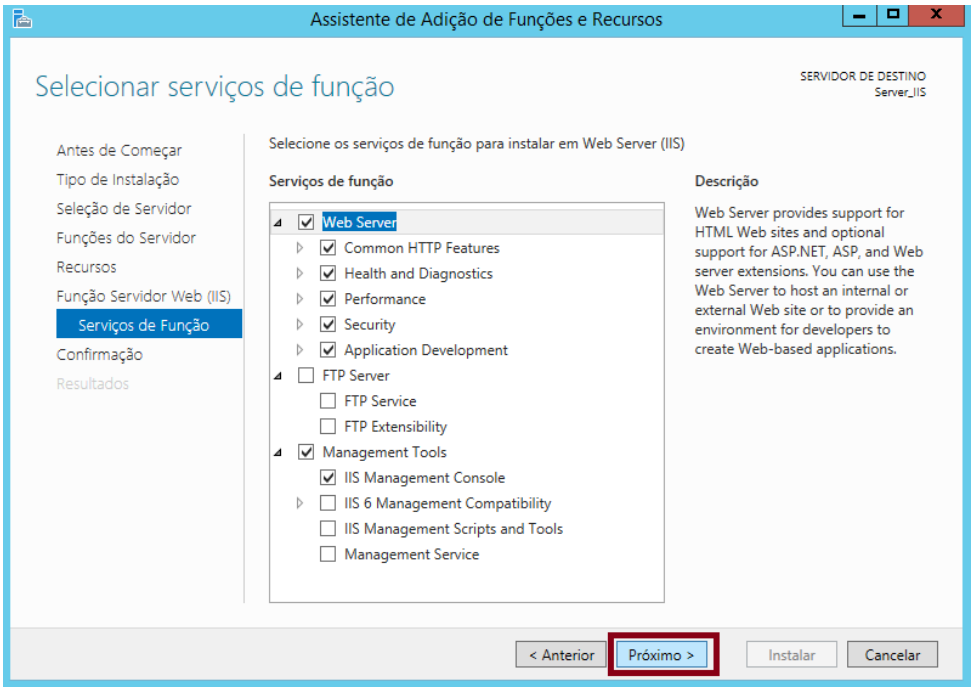
Fonte: Elaborado pelo autor.

Figura 47 – Observações sobre a instalação do IIS



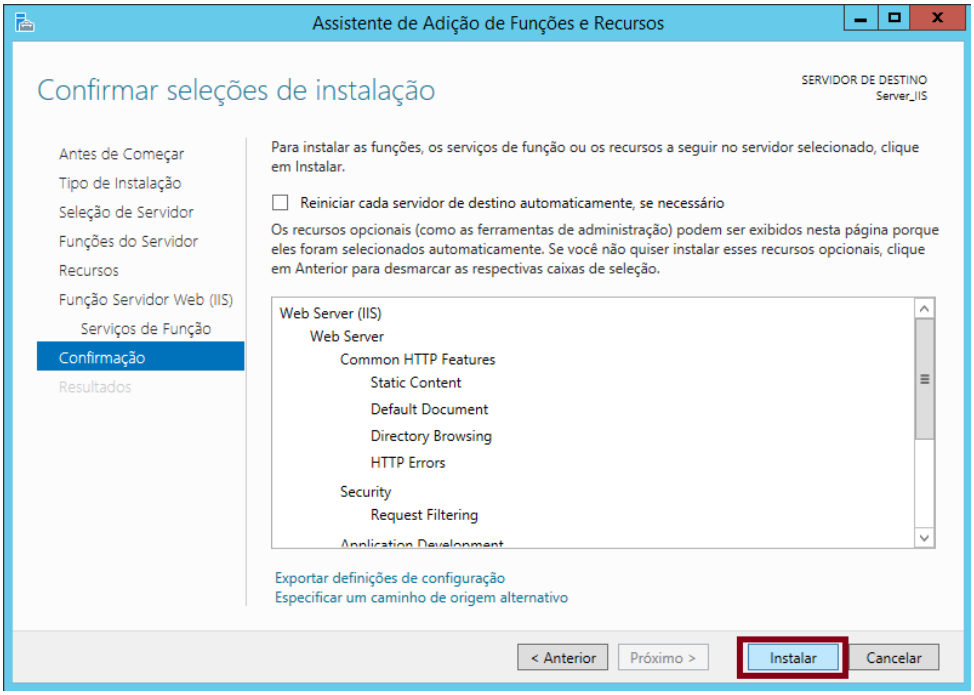
Fonte: Elaborado pelo autor.

Figura 48 – Seleção dos serviços adicionais para o IIS



Fonte: Elaborado pelo autor.

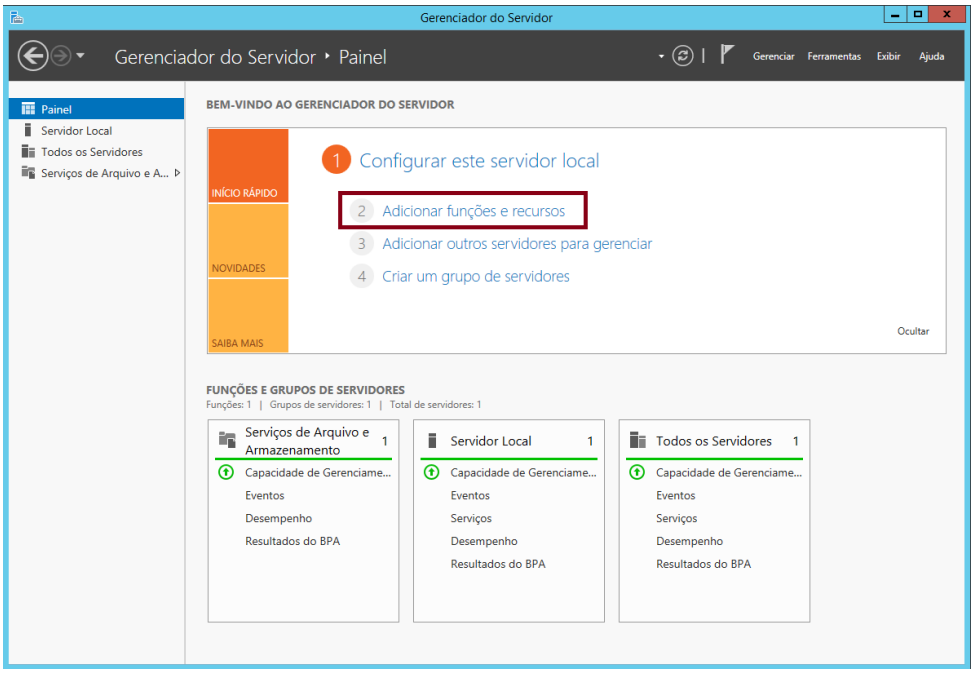
Figura 49 – Confirmação das funções ou recursos que serão instalados



Fonte: Elaborado pelo autor.

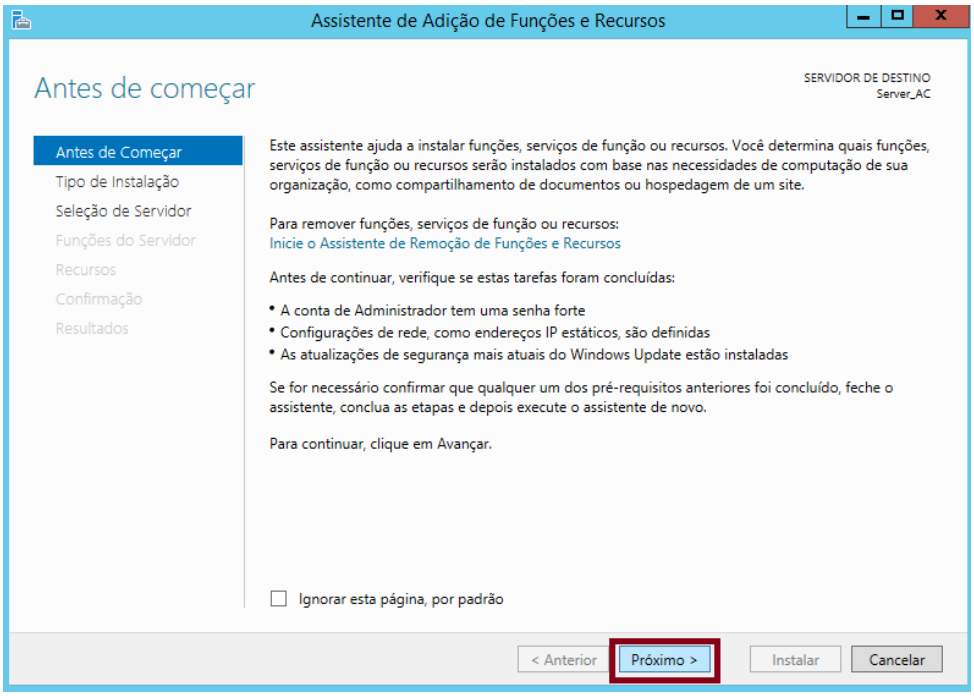
APÊNDICE C – Instalação e Configuração da AC

Figura 50 – Adição de funções e recursos no Gestor de Servidor



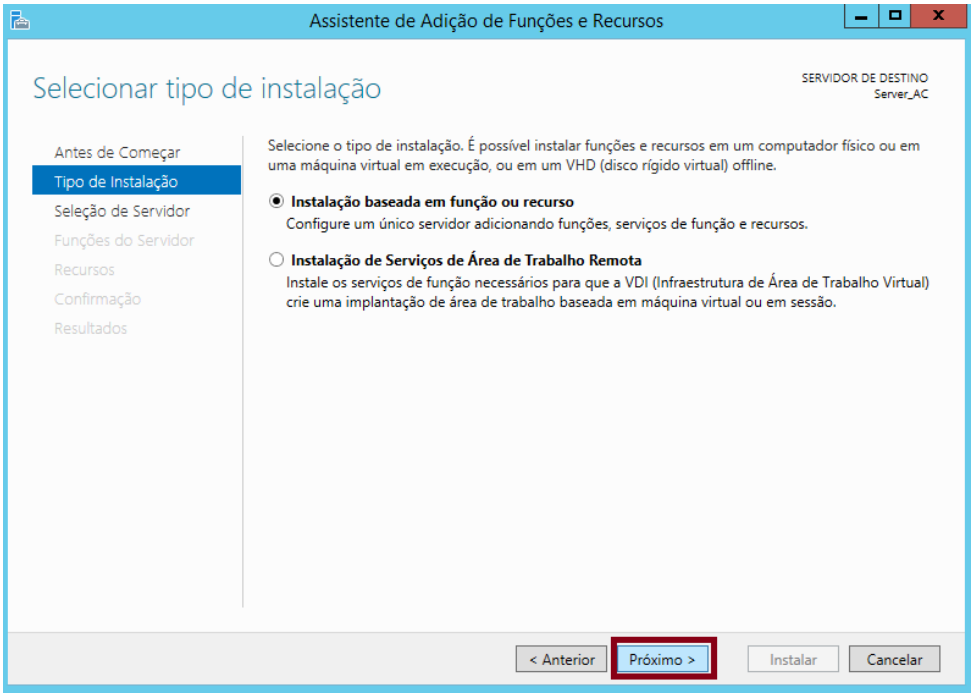
Fonte: Elaborado pelo autor.

Figura 51 – Confirmação dos pré-requisitos para instalação



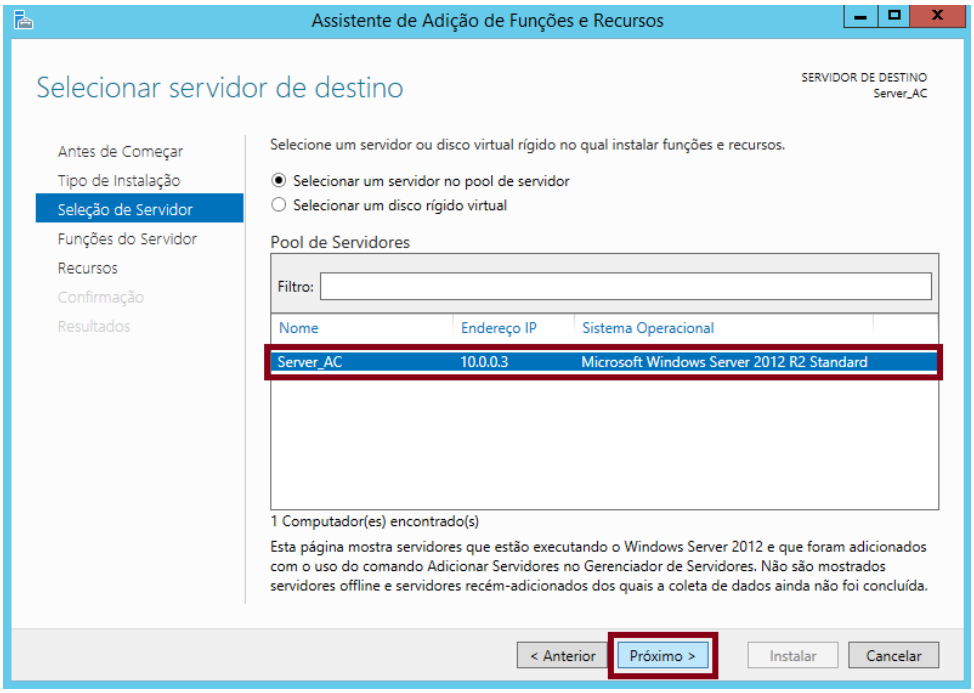
Fonte: Elaborado pelo autor.

Figura 52 – Seleção do tipo de instalação para o AC



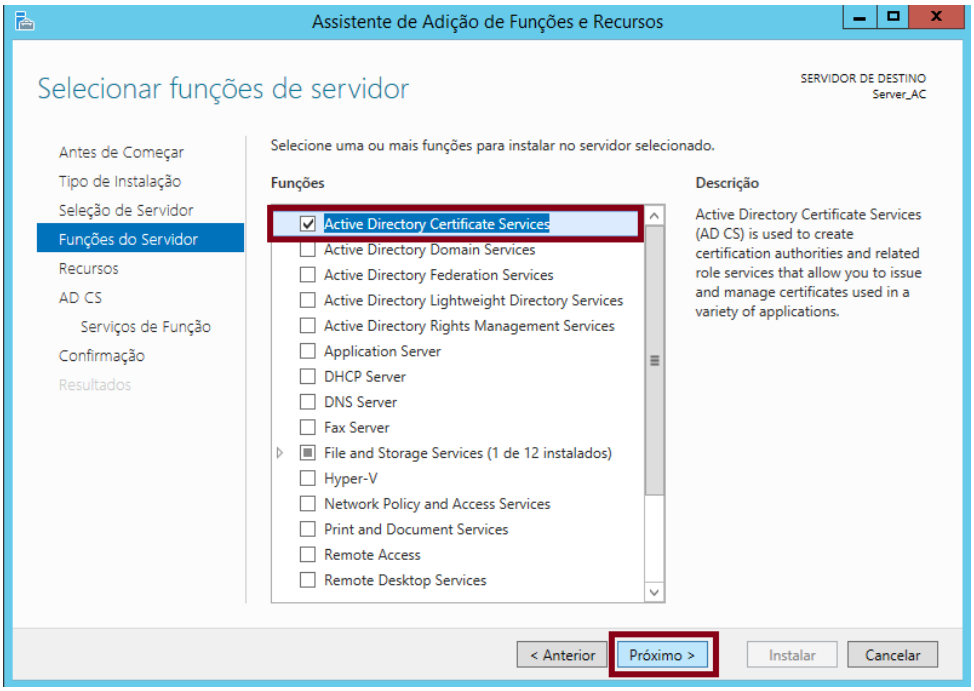
Fonte: Elaborado pelo autor.

Figura 53 – Seleção do servidor onde será instalado a AC



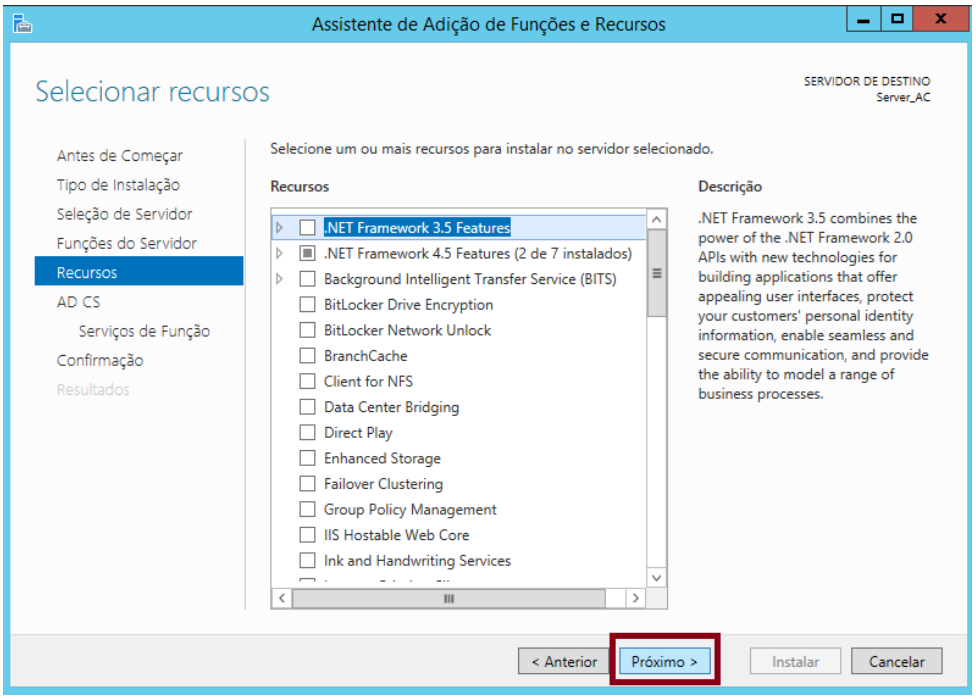
Fonte: Elaborado pelo autor.

Figura 54 – Seleção da função de AC



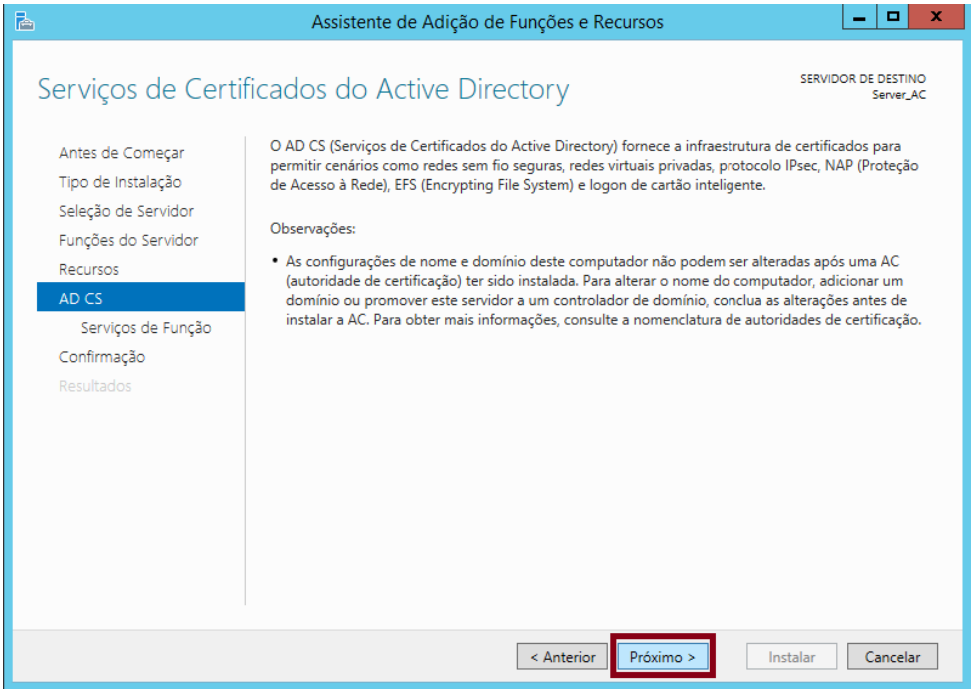
Fonte: Elaborado pelo autor.

Figura 55 – Seleção de outros recursos para serem instalados no mesmo servidor que a AC



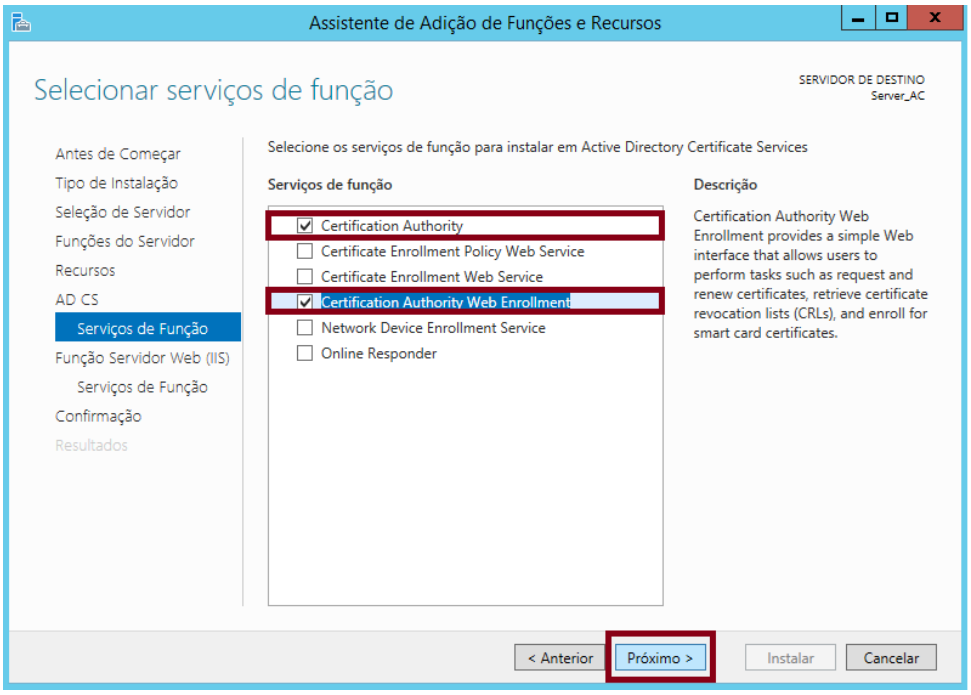
Fonte: Elaborado pelo autor.

Figura 56 – Observações sobre a instalação da AC



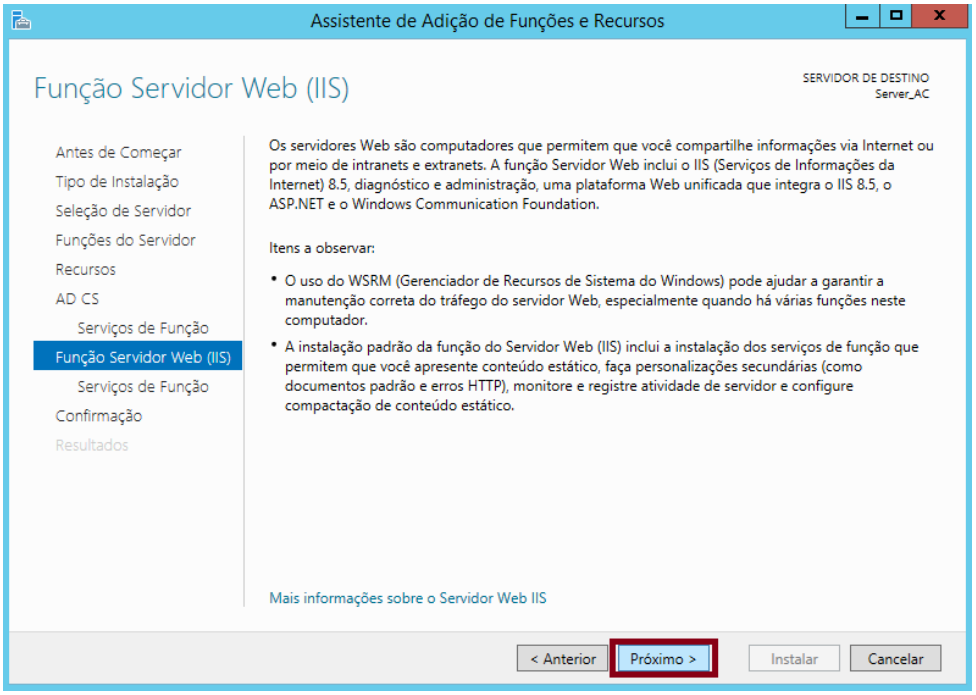
Fonte: Elaborado pelo autor.

Figura 57 – Seleção dos serviços para serem instalados na função da AC



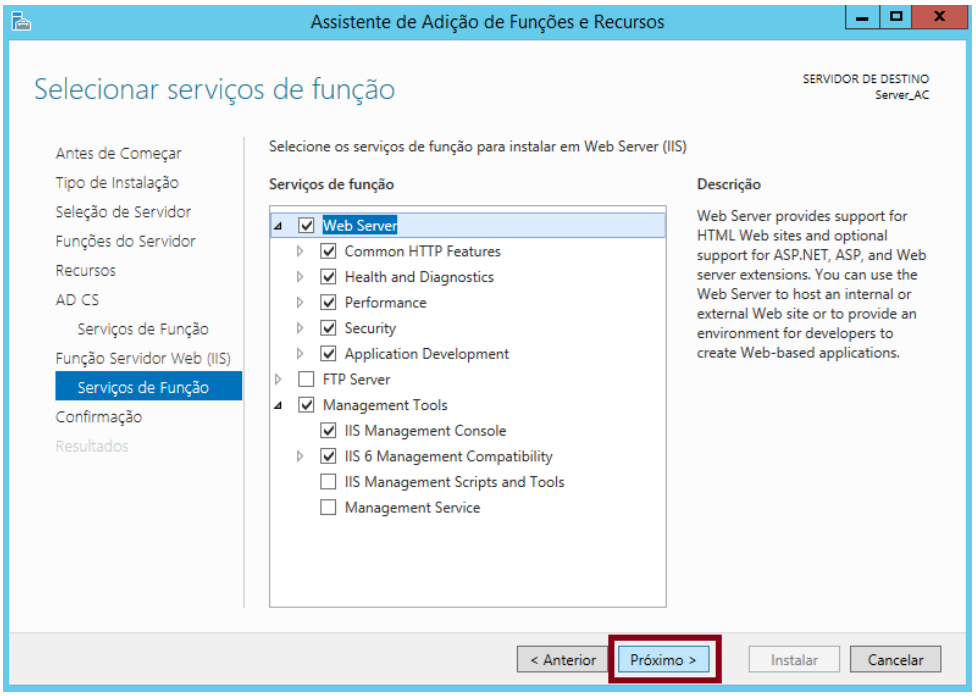
Fonte: Elaborado pelo autor.

Figura 58 – Observações sobre o serviço no ambiente WEB oferecido pela AC



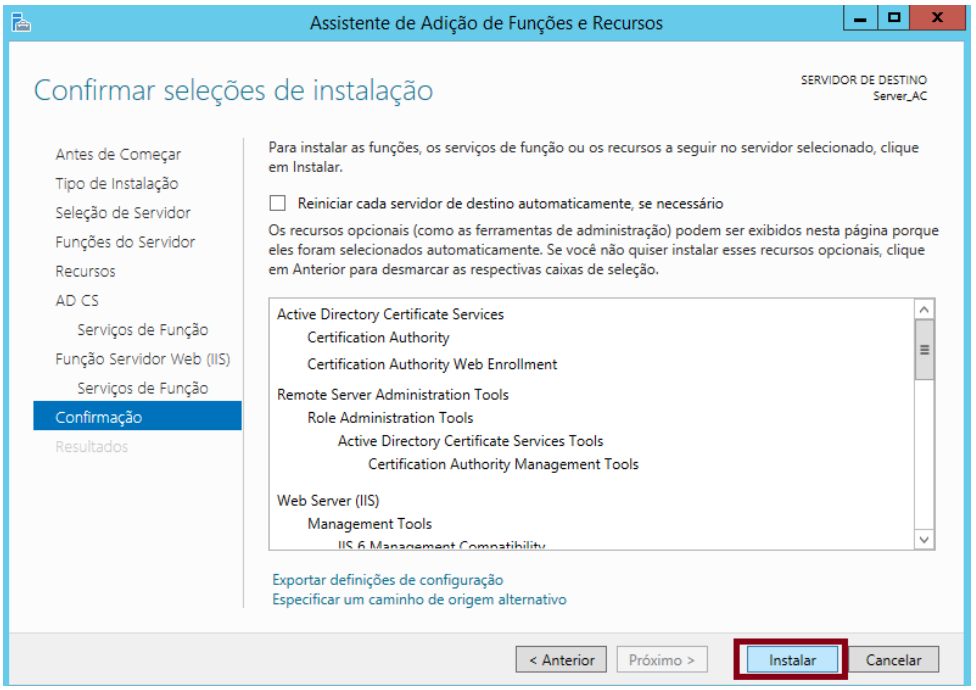
Fonte: Elaborado pelo autor.

Figura 59 – Seleção dos serviços adicionais para AC



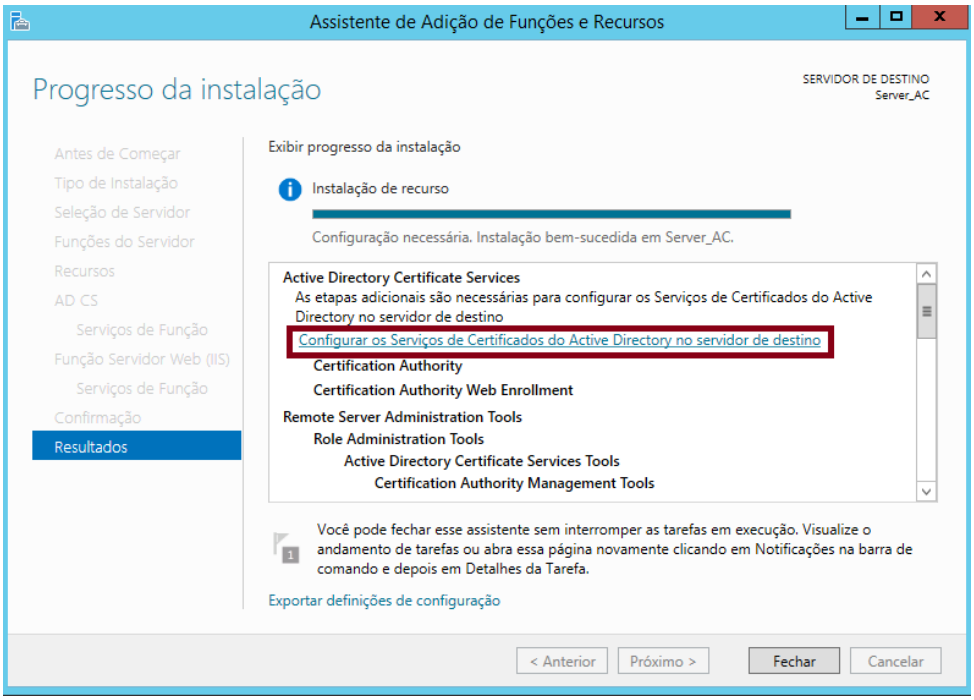
Fonte: Elaborado pelo autor.

Figura 60 – Confirmação das funções ou recursos que serão instalados



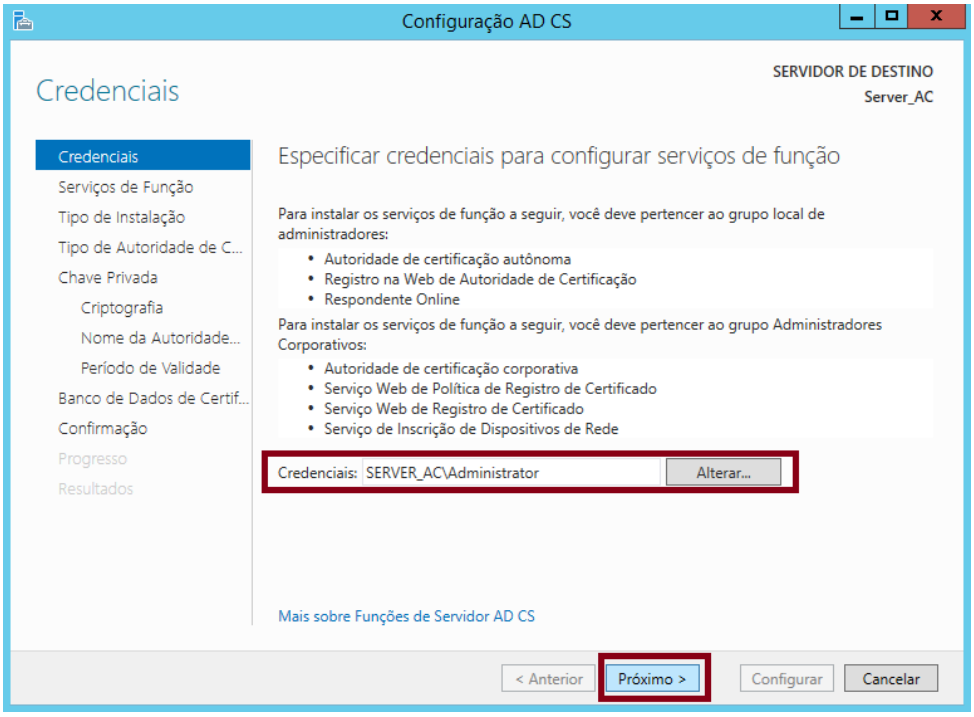
Fonte: Elaborado pelo autor.

Figura 61 – Configuração da AC



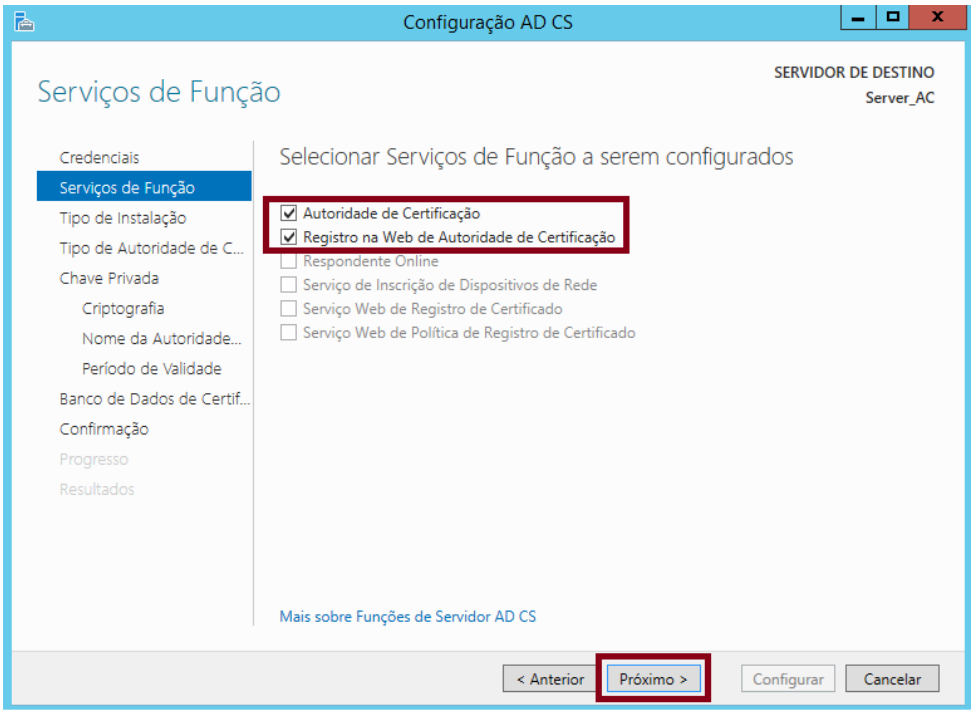
Fonte: Elaborado pelo autor.

Figura 62 – Especificação das credenciais da AC



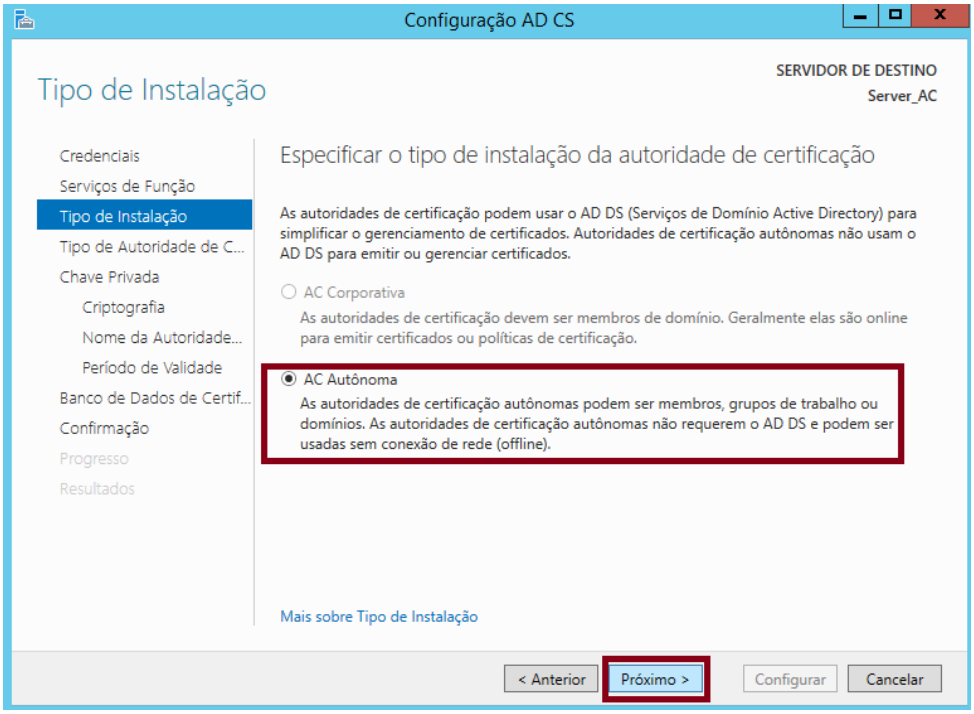
Fonte: Elaborado pelo autor.

Figura 63 – Seleção dos serviços da AC que serão configurados



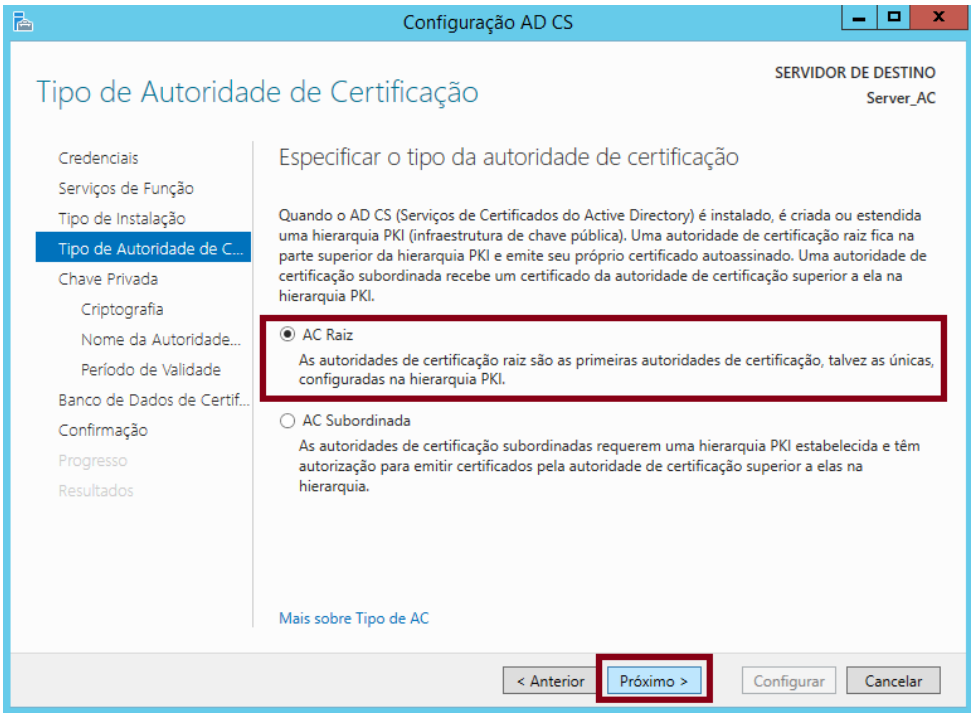
Fonte: Elaborado pelo autor.

Figura 64 – Especificação do tipo de instalação da AC



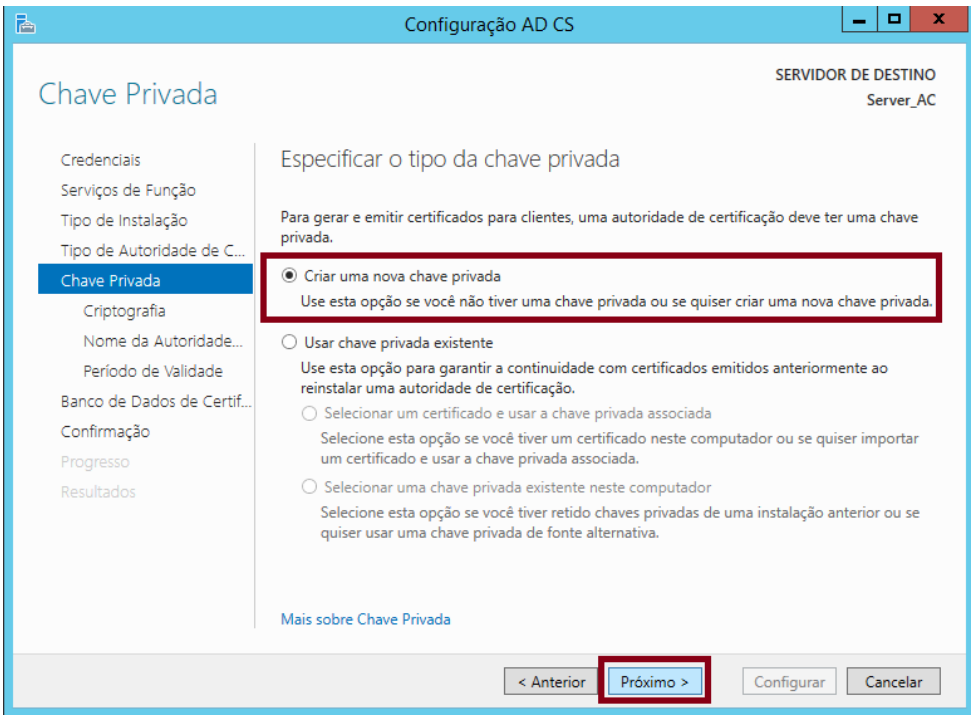
Fonte: Elaborado pelo autor.

Figura 65 – Especificação do tipo de AC



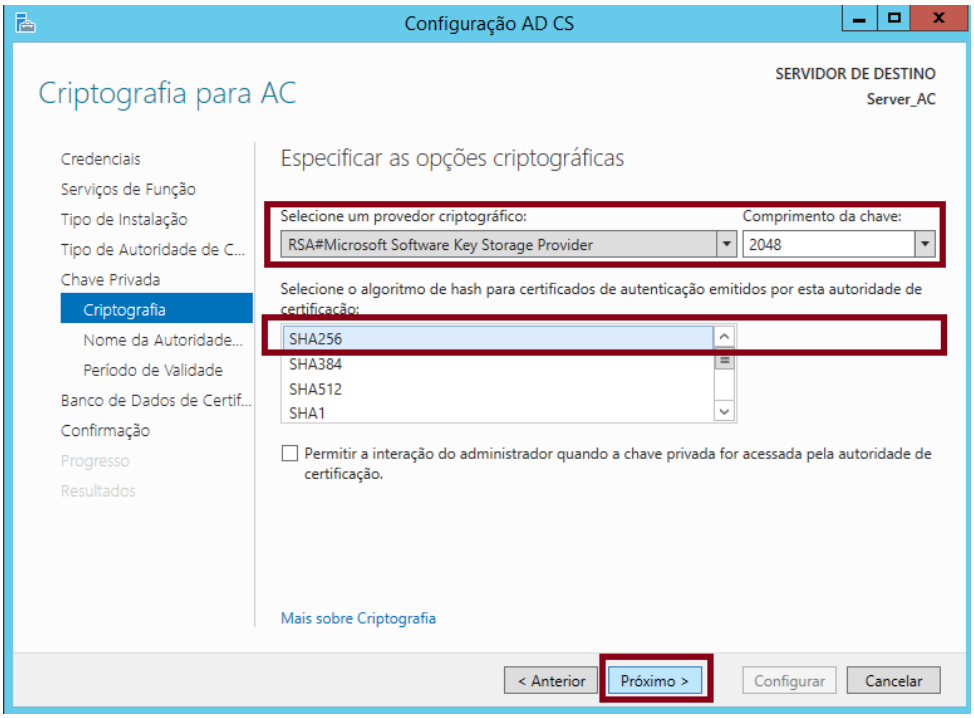
Fonte: Elaborado pelo autor.

Figura 66 – Especificação do tipo da chave privada da AC



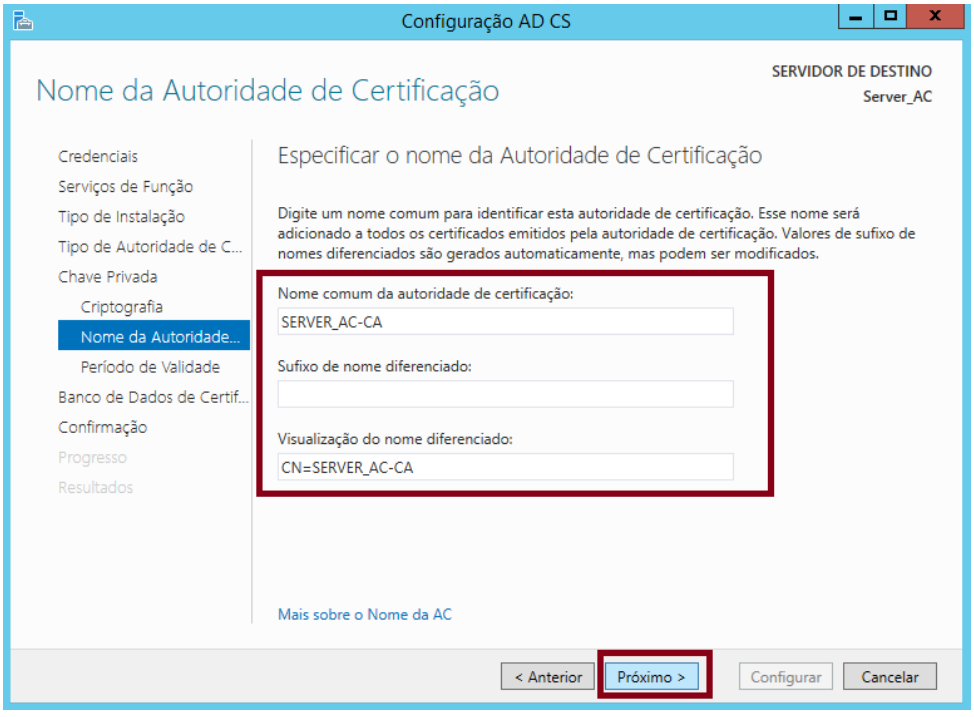
Fonte: Elaborado pelo autor.

Figura 67 – Especificação criptográfica da nova chave privada



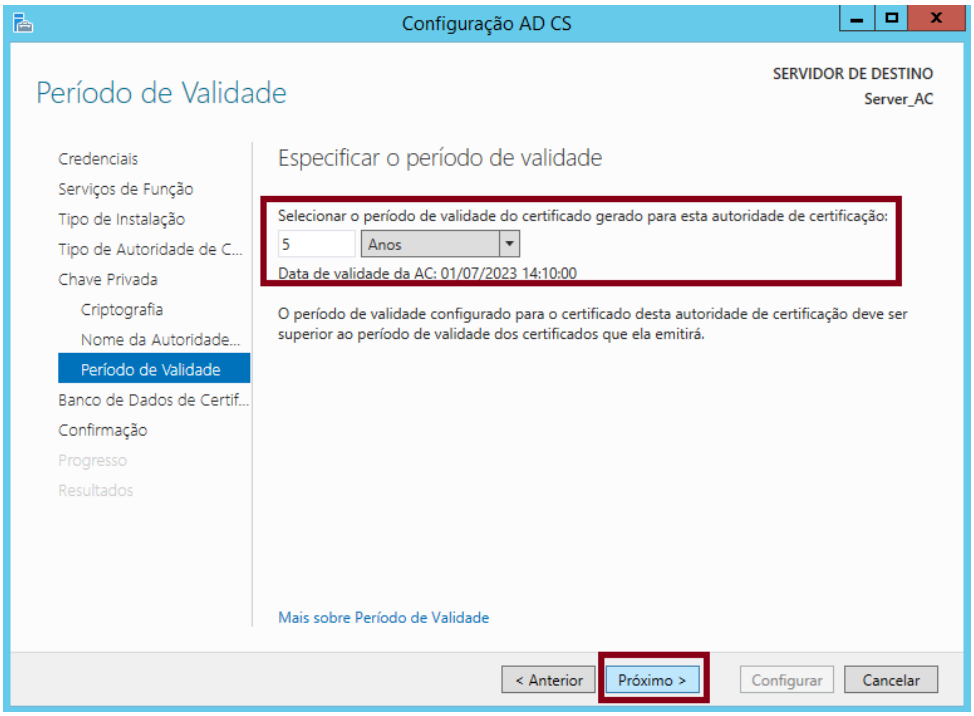
Fonte: Elaborado pelo autor.

Figura 68 – Especificação do nome da AC



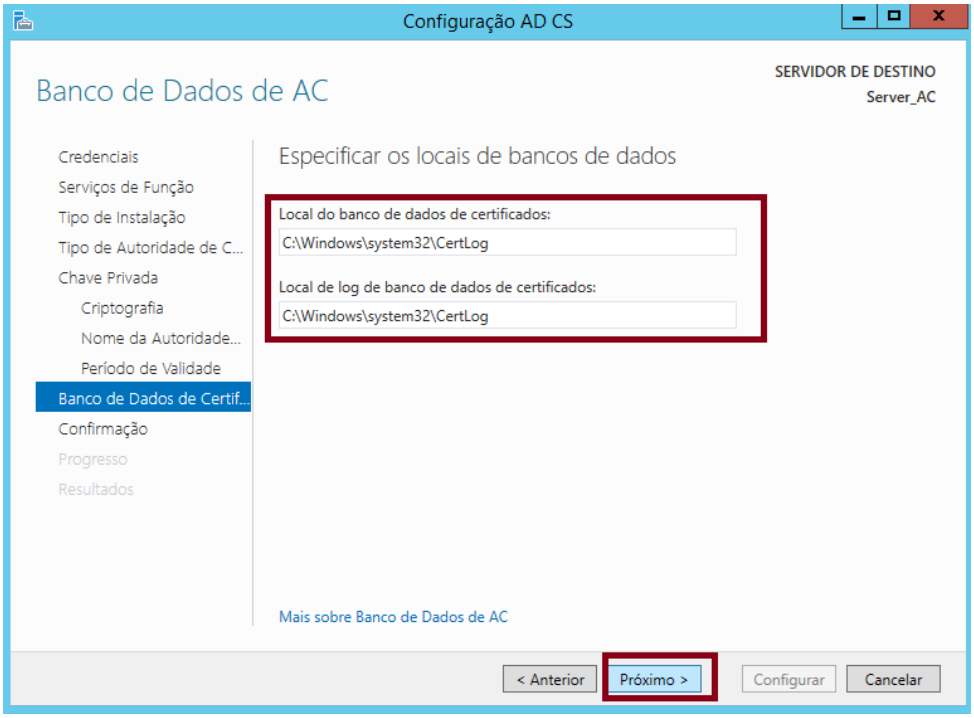
Fonte: Elaborado pelo autor.

Figura 69 – Especificação do período de validade dos certificados emitidos por essa AC



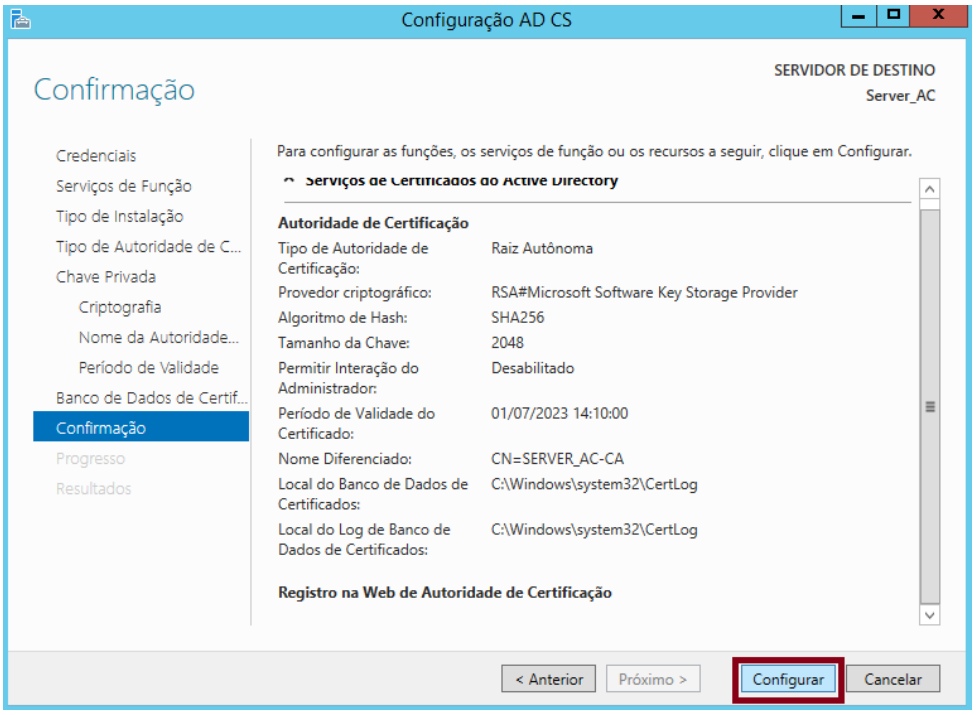
Fonte: Elaborado pelo autor.

Figura 70 – Especificação banco de dados da AC



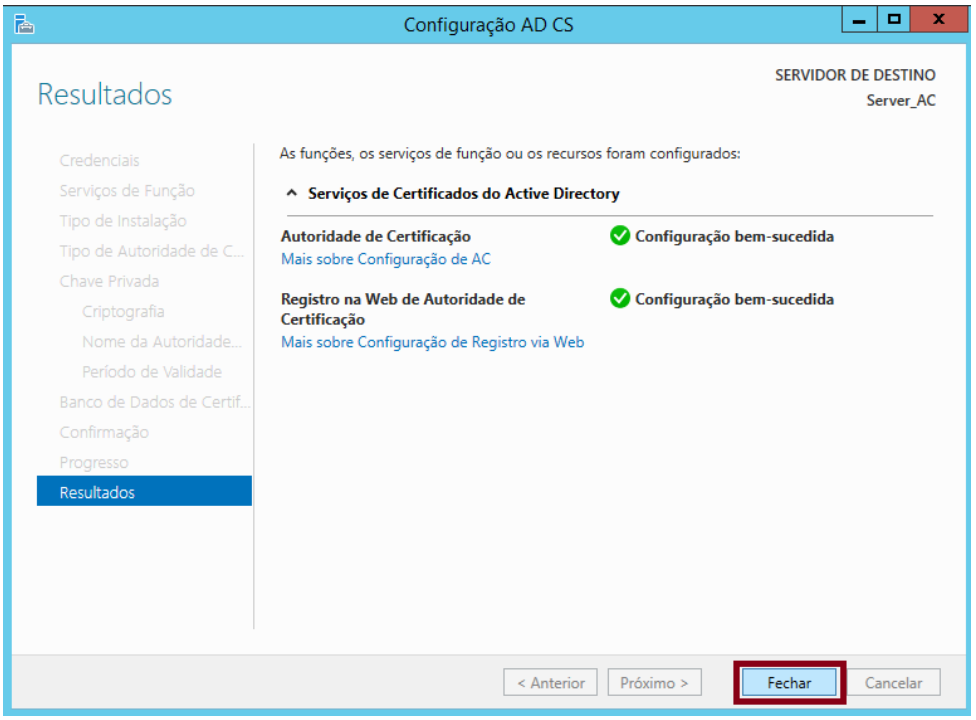
Fonte: Elaborado pelo autor.

Figura 71 – Confirmação das funções ou recursos que serão configuradas



Fonte: Elaborado pelo autor.

Figura 72 – Funções ou recursos que foram configurados



Fonte: Elaborado pelo autor.