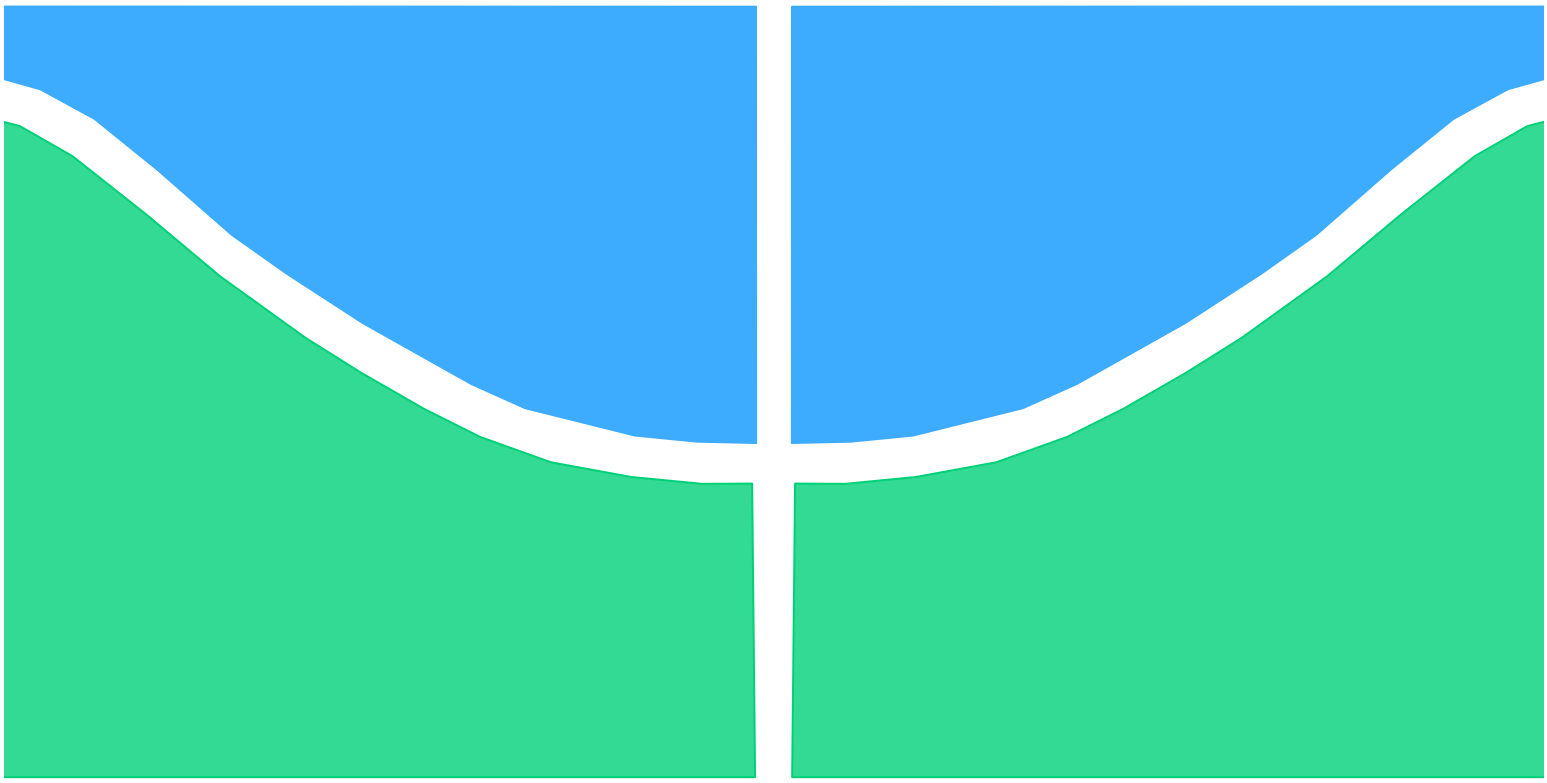

TRABALHO DE GRADUAÇÃO

GUIA DE RECOMENDAÇÕES DE SEGURANÇA PARA O DESENVOLVIMENTO DE WEB SERVICES PARA A ADMINISTRAÇÃO PÚBLICA FEDERAL

Rodolfo Augusto Mota Ribeiro
Yuiti Oki Niyama

Brasília, 11 de dezembro de 2013

UNIVERSIDADE DE BRASILIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

GUIA DE RECOMENDAÇÕES DE SEGURANÇA PARA O DESENVOLVIMENTO DE WEB SERVICES PARA A ADMINISTRAÇÃO PÚBLICA FEDERAL

Rodolfo Augusto Mota Ribeiro
Yuiti Oki Niyama

Orientador: Prof. Dr. Edgar Costa Oliveira

Relatório submetido como requisito parcial para obtenção
do grau de Engenheiro de Redes de Comunicações.

Banca Examinadora

Prof. Dr. Edgard Costa Oliveira (Orientador)	_____
Prof. Dr. Rafael Timóteo S. Jr., UnB/ Dep. Eng. Elétrica	_____
Prof. Dr. Flávio Elias Gomes de Deus, UnB/ Dep. Eng. Elétrica	_____

Dedicatória(s)

Dedico esta monografia ao meu filho que mesmo quando ainda estava na barriga de sua mãe, me ajudou a crescer como pessoa e agora seu terno sorriso alegra meus dias mais cansativos e árduos, tornando-os mais divertidos. Obrigado por me trazer tanta felicidade e por fazer parte da minha vida. Papai te ama.

Yuiti Oki Niyama

Dedico este trabalho a uma mulher guerreira que sempre acreditou nos meus sonhos, me deu forças e lutou pela minha formação. Mesmo nos momentos mais difíceis ela esteve ao meu lado me aconselhando e fornecendo energia para continuar. Obrigado Mãe por me gerar, educar e fortalecer.

Rodolfo Augusto Mota Ribeiro

Agradecimentos

Agradeço a Deus e aos Espíritos de luz que sempre estiveram comigo em toda jornada acadêmica, ao meu irmão Vinícius que despertou em mim o desejo para o estudo nesta Universidade e à Anne que sempre acreditou em mim e continuamente me estimulou a continuar e seguir até o fim.
Agradeço também a todos os professores que estiveram presentes durante todo o período acadêmico, que com seus esforços estimulam a formação de grandes profissionais nesta Universidade. Em especial, agradeço ao professor Dr. Edgard Costa Oliveira pelo excelente trabalho de orientação para a elaboração deste trabalho. Por fim, agradeço ao meu parceiro nesta pesquisa, Yuiti, que não mediu esforços, mesmo nos momentos mais difíceis, para a construção deste trabalho.

Rodolfo Augusto Mota Ribeiro

Em primeiro lugar agradeço a minha mãe por ter me ajudado e acreditado em mim, ao meu pai que me auxiliou nos momentos de incertezas do projeto, a mãe do meu filho pelo apoio e carinho e ao mais novo membro da família, meu filho, que me deu ânimo para a realização deste trabalho.
Agradeço também aos professores que me acompanharam nesta jornada, em especial ao exemplar Prof. Dr. Edgar Costa Oliveira, por ter orientado a elaboração desta monografia.
Aos meus amigos, por poder contar sempre com eles e ao grande Rodolfo Mota, meu parceiro na construção desta pesquisa.

Yuiti Oki Niyama

RESUMO

Os sistemas distribuídos tem se destacado na estratégia de negócios de corporações e entidades governamentais. O presente texto apresenta uma proposta de desenvolvimento seguro de Web Services para a Administração Pública Federal, tendo em vista a necessidade de um modelo confiável que contemple as carências atuais do Governo. Foi realizada a análise e fusão de documentos relacionados a implementação de sistemas e apresentado um guia de recomendações para a construção e projeto de uma arquitetura segura de Web Service, que complemente o planejamento e gestão da segurança da informação para essas aplicações.

ABSTRACT

The distributed systems have excelled in business corporations and government entities strategy. This paper presents a proposal of a secure Web Services development for the federal government, considering the need for a reliable model that reflects the current needs of the government. Analysis and merging of documents related to the implementation of systems was performed and presented a guide of recommendations for the design and construction of a secure architecture for Web Service, that complements the planning and management of information security for these applications.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIAÇÕES

Siglas

ABNT	Associação Brasileira de Normas Técnicas
AH	Authentication Header
APF	Administração Pública Federal
API	Application Programming Interface
ARP	Address Resolution Protocol
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
DTD	Document Type Definition
ESP	Encapsulating Security Payload
HTTP	Hypertext Transfer Protocol
ICP	Infraestrutura de Chaves Públicas
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
ITU-T	ITU Telecommunication Standardization Sector
JSON	JavaScript Object Notation
MAC	Message Authentication Code
NBR	Norma Brasileira
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OSI	Open Systems Interconnection
QoS	Quality of Service
RBAC	Role Based Access Control
SAML	Security Assertion Markup Language
SCT	Secutiry Context Token
SDL	Security Development Lifecycle
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SLTI	Secretaria de Logística e Tecnologia da Informação
SOAP	Simple Object Access Protocol
SOA	Service-Oriented Architecture
SSL	Secure Sockets Layer
SSO	Single Sign On
TCP	Transmission Control Protocol
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TLS	Transport Layer Security
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modeling Language
URI	Uniform Resource Identifier
XACML	eXtensible Access Control Markup Language
XKMS	XML Key Management Specification

XML	eXtensible Markup Language
XSD	XML Schema Definition
W3C	World Wide Web Consortium
WS	Web Service
WS – I	Web Service Interoperation
WSDL	Web Services Description Language

1 INTRODUÇÃO

A situação atual do governo brasileiro nos revela um aumento da necessidade de informatizar o trabalho e as informações contidas nas entidades do governo. O objetivo é de aperfeiçoar o desempenho do processo operacional, analisar dados para tomadas de decisão e tornar mais ágil a comunicação entre órgãos do governo. No entanto, devido às diversas tecnologias utilizadas por diferentes entidades, surge o problema de comunicação entre diferentes plataformas, sistemas operacionais, linguagens de programação e tipos de dados.

Diante deste contexto, nasce a necessidade de se criarem sistemas capazes de reutilizar serviços já existentes. Assim, a adoção de Web Services vem ganhando grande importância nas aplicações governamentais. Contudo, estes sistemas devem preservar e promover a entrega confiável dos dados que, em grande parte das transações, são sigilosos e críticos para entidades governamentais. Desta forma, boas práticas de desenvolvimento seguro aliadas a guias de implementação de Web Service são de grande importância na construção destes sistemas.

O governo brasileiro tem migrado diversas atividades governamentais para sistemas automatizados com o objetivo de aumentar a eficiência e eficácia do trabalho público. A necessidade de informações consistentes padronizadas e principalmente seguras dentro do âmbito nacional da administração pública vem como legado dessa ampliação de serviços eletrônicos e vem sendo cada vez mais requisitados pelos gestores de projetos de sistemas de informação. Atualmente, outra característica vem ganhando destaque: a interoperabilidade entre sistemas e plataformas diferentes. Este fato está dando início aos sistemas baseados em Web Services dentro da Administração Pública Federal.

Os sistemas de informação têm avançado muito nos últimos anos. A *Internet* se tornou um recurso tão fundamental como ter água e luz em uma casa. Aliado a isto, sistemas de informação também evoluíram muito rápido e passaram a utilizar a *Internet* e, criando assim, uma necessidade de implementar novos sistemas reutilizando sistemas antigos. Contudo, nestes novos sistemas web, as informações trafegam em meios não confiáveis, ou seja, a *Internet*. Assim como existem indivíduos que querem obter vantagens fazendo desvios em redes de água ou em redes elétricas também existem aqueles que desejam tirar proveito dos recursos que trafegam pela *Internet*, ou seja, a informação.

Desta forma, cresceu a importância da segurança de dados que trafegam por sistemas não confiáveis de informação. Sistemas Web trocam constantemente mensagens com conteúdos valiosos para uma organização ou para um governo. Neste contexto, diversas recomendações relevantes à segurança da informação para a Administração Pública Federal brasileira foram propostas em documentos oficiais, cartilhas e normas pelos órgãos competentes. Porém, estas recomendações são baseadas, em grande parte, em normas internacionais de cunho geral e não específicas para cada caso de utilização. Tendo em vista esta situação, a criação de Web Services seguros depende de uma série de requisitos de segurança que envolve em todo ciclo de vida de um software.

A pesquisa foi dividida em três etapas. Primeiramente foram abordados os conceitos gerais de segurança da informação de forma a criar um levantamento teórico sobre o assunto, buscando focar na segurança da informação de sistemas baseados em Web Services. Além disso, foram levantadas as principais leis, decretos, guias, projetos, normas e entidades que estejam ligadas a segurança da informação de sistemas da Administração Pública brasileira e da interoperabilidade dos mesmos. Também foram citadas e analisadas as normas padrões internacionais que abordam temas que vão além das recomendações do governo brasileiro para a construção de sistemas seguros. Em seguida, foi apresentado o documento da OASIS - Organization for the Advancement of Structured Information Standards de construção de Web Services, o modelo de desenvolvimento seguro do ciclo de vida de sistemas, produzido pela *Microsoft* e o guia de considerações de segurança no desenvolvimento de sistemas. Por fim, foi proposto um guia para a construção de um Web Services seguro dentro da Administração Pública Federal brasileira baseado no documento de recomendação internacional proposto pela OASIS aliado a documentos de desenvolvimento seguros de software e normas de gestão de segurança da informação. A construção do documento foi embasada no guia de implementação proposto pela OASIS.

1.1 OBJETIVOS

1.1.1 OBJETIVO GERAL

Propor um guia com recomendações para a implementação de Web Services seguros para órgãos da Administração Pública Federal brasileira.

1.1.2 OBJETIVOS ESPECÍFICOS

- Apresentar conceitos de segurança da informação, Web Service e segurança em Web Service. Pesquisar, citar e analisar criticamente as principais recomendações de

segurança da informação especificadas por entidades do governo federal brasileiro que administram os recursos de TI.

- Realizar uma análise da metodologia de desenvolvimento de Web Services da OASIS, do modelo SDL da *Microsoft* e do documento Special Publication 800-64 do NIST - National Institute of Standards and Technology.
- Recomendar um guia para a construção de um Web Service seguro, baseado nas normas de segurança de desenvolvimento e gestão de TI – Tecnologia da Informação, embasado no modelo de desenvolvimento proposto pela OASIS.

1.2 METODOLOGIA

Primeiramente, foi levantado um arcabouço de documentos bibliográficos relacionados à pesquisa e que foram as principais fontes de informação para fundamentar os conceitos mais relevantes no que diz respeito a segurança da informação, Web Services, e segurança para Web Services, obtidos nas especificações e documentações da W3C - World Wide Web Consortium, OASIS, NIST e CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, nos livros de autores renomados como W. Stallings (STALLINGS, 2008) e nas normas internacionais como a ABNT NBR ISO/IEC – Associação Brasileira de Normas e Técnicas Norma Brasileira International Organization for Standardization/ International Electrotechnical Commission 27001, 27002 e 27005. A segunda atividade, foi realizar um estudo exploratório da situação atual das recomendações da APF – Administração Pública Federal no que se refere a tecnologia de Web Services, que teve como fonte de pesquisa os órgãos do governo ligados a segurança e documentação de tecnologia da informação, como o SISP - Sistema de Administração dos Recursos de Tecnologia da Informação, a SLTI - Secretaria de Logística e Tecnologia da Informação e o Gabinete de Segurança Institucional da Presidência da República. (MATHIAS-PEREIRA, 2012)

Em seguida, foram realizados estudos dos processos tecnológicos de desenvolvimento de sistemas e Web Services, tendo como base os modelos propostos pela OASIS, *Microsoft* e NIST. De forma a visualizar a aplicação das normas de segurança vigentes dentro da esfera governamental no contexto de Web Services, foi analisada a possibilidade de um estudo dentro de uma organização governamental brasileira sobre a utilização e a implementação destas normas, que não foi possível devido a disponibilidade dos envolvidos.

Desta forma, os trabalhos de pesquisa foram executados de forma gradual seguindo um cronograma pré-estabelecido. Também foram realizados pontos de controle semanais de forma a verificar o andamento das atividades e ocasionalmente reuniões.

A última etapa da pesquisa foi adaptar o modelo de desenvolvimento de Web Services da OASIS para propor um guia de desenvolvimento que possua um nível razoavelmente alto de segurança na implementação e na estrutura interna de Web Services, para que sirva como uma sugestão de roteiro para a APF. O modelo de desenvolvimento seguro de Web Service que foi recomendado, consistiu de três principais fontes de pesquisa.

- Web Service *Implementation Methodology* criado pela organização OASIS em 2005, foi o primeiro documento estudado e onde suas atividades foram traduzidas para língua portuguesa, que foram comparadas com outros dois documentos a serem listados. Neste documento inclui-se um guia de desenvolvimento de aplicações focado nos problemas, características e desafios de um Web Service, possuindo atividades e tarefas específicas, de alto nível, para a criação de um Web Service, como a necessidade do sistema ser baseado em Web Service e a identificação de possíveis Web Services reutilizáveis para complementar o que está sendo produzido.
- O NIST SP 800-64 (*Security considerations in the system development life cycle*) criado parceria com o departamento de comércio dos Estados Unidos em 2008, é um documento de recomendação de alto nível, do ciclo de vida de desenvolvimento seguro de aplicações. São abordadas atividades de gestão de desenvolvimento de sistemas com foco nos procedimentos que agreguem segurança ao processo e ao produto, como a avaliação dos riscos de segurança e a análise de impacto ao negócio.
- O SDL *Process Guidance* criado pela *Microsoft* em 2012, é um guia de tarefas distribuídas em fases de desenvolvimento que permitem a implementação segura de uma aplicação. Possui um caráter de mais baixo nível, com recomendações de codificação, como a utilização de funções seguras, de planejamento, como o tratamento de ameaça e de testes, como os testes dinâmicos e estáticos, dentre outros.

Foi realizada uma análise documental comparativa (MATHIAS-PEREIRA, 2012) dos documentos acima para se obter uma proposta única que reúna atividades específicas para o desenvolvimento correto e seguro de um Web Service, tanto na implementação como na operação. Foram gerados fluxogramas com as atividades distribuídas nas fases do desenvolvimento, tabelas explicativas e um mapeamento dos procedimentos que são

convergentes dos três documentos. De fato, existiram atividades que não foram mapeáveis, mas que possuíram uma importância considerável como recomendação. Neste caso, adicionamos ao guia como uma nova atividade ou tarefa, dependendo do nível de profundidade do procedimento. (SILVA, 2009)

Os fluxogramas foram elaborados pela ferramenta *Bizagi Process Modeler*, que é uma modelador de processos de negócio cuja documentação e *download* podem ser encontradas no *site* do fornecedor. Após a construção das tabelas e fluxogramas foi realizado um estudo descritivo das atividades e tarefas adicionadas no guia sugerido de acordo com os conhecimentos adquiridos durante a elaboração do trabalho.

2. CONCEITOS GERAIS DE SEGURANÇA DA INFORMAÇÃO

Neste capítulo foram apresentados os conceitos básicos de segurança da informação, mecanismos de segurança, tipos de ataques, Web Services e segurança para Web Services.

2.1 SEGURANÇA DA INFORMAÇÃO

> *"Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio."* (ABNT NBR, 2005)

A segurança da informação tem sido um dos grandes temas de discussão entre profissionais de TI, devido ao crescente aumento da quantidade e variedade de ataques a sistemas computacionais e a redes de computadores e pelo aumento da importância de dados e serviços íntegros e seguros.

A demanda crescente da informatização de serviços, tanto na área privada como na área pública tem sido uma das grandes mudanças na área de tecnologia, onde o cliente e o servidor não se preocupam apenas com os dados, mas sim com o serviço que é oferecido. Com este crescimento de atividades realizadas na *Internet*, a segurança se torna cada vez mais necessária e complexa. Os serviços de segurança necessitam de constante atualização por meio de novos ou adaptações de mecanismos de segurança para manter os serviços seguros. Cada vez mais ataques estão surgindo e se tornando mais elaborados e novas vulnerabilidades surgem com a diversidade de aplicativos construídos. Portanto, novas tecnologias como o Web Service precisam ser analisadas para manter a segurança da informação.

2.2 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Os princípios de segurança de comunicação são divididos nas seguintes categorias: autenticação, confidencialidade, integridade, controle de acesso, disponibilidade e o não-repúdio.

A **confidencialidade** *"propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados"* (ABNT NBR, 2006) pode ser entendida como a privacidade de uma informação a entes não autorizados, seja ela concreta como um dado, ou um fluxo anormal de pacotes para certo endereço que possa ser tratado e gerar alguma informação. Podemos verificar a importância desse serviço de segurança, como os acontecimentos atuais de violação de sigilo, interceptação de chamadas telefônicas entre países, que tornam o relacionamento político mais complicado e instável. (STALLINGS, 2008)

A **integridade** *"propriedade de salvaguarda da exatidão e completeza de ativos."* (ABNT NBR, 2006) , assim como a confidencialidade, é importantíssima para a segurança da informação, incluindo o impedimento de alteração, repetição e deleção de informações, mantendo-as consistentes para utilização.

A **disponibilidade** *"propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada"* (ABNT NBR, 2006) pode ser compreendida como o funcionamento completo de uma aplicação, por exemplo, quando solicitada por um usuário. É um dos serviços que vem sendo explorados por muitos atacantes, devido a sua difícil prevenção. Uma medida de recuperação e continuidade é recomendada para os serviços e dados mais essenciais ou sensíveis.

A **autenticação** consiste em duas principais fases: a identificação e a validação. A primeira seria a apresentação do usuário, como um nome, um e-mail ou uma conta corrente, sendo verificado se este usuário está devidamente cadastrado. Na segunda etapa o usuário precisa apresentar algo que comprove que ele é realmente o usuário que esta tentando entrar no sistema, por exemplo. Pode ser uma senha, uma impressão digital ou um *token*, por exemplo. O ideal é que para ser considerada forte sejam utilizados no mínimo dois métodos de validação de usuário.

O **não-repúdio** é um serviço que visa impedir que alguma ação esteja desvinculada a um ator, como a criação ou o recebimento de uma informação. Desta forma, é fundamental para a realização de auditorias e investigações de autoria de ataques. (STALLINGS, 2008)

2.3 MECANISMOS DE SEGURANÇA DA INFORMAÇÃO

Para a salvaguarda dos serviços citados na seção anterior, é necessária a adoção de alguns dos seguintes mecanismos de segurança: criptografia, assinatura digital, certificação digital, dentre outros. (STALLINGS, 2008)

A **criptografia** *"A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet."* (BRASIL, 2012) possui um papel de extrema importância na segurança da informação, sendo responsável por parte da maioria dos serviços. Possui como principal elemento a cifração, que pode ser de fluxo, realizada byte a byte ou bit a bit, ou de bloco, onde um conjunto de bytes é cifrado de uma vez. Ela pode ser realizada por meio de chave simétrica ou assimétrica, sendo que a primeira utiliza uma chave compartilhada entre os comunicantes para cifrar e decifrar a informação, os algoritmos simétricos devem possuir difusão e confusão. A difusão evita que a partir de um texto cifrado, um oponente decifre o texto original e é obtida por meio de permutações e funções. A confusão, por meio de substituições complexas, evita que o atacante descubra a chave utilizada no algoritmo, possuindo apenas o texto cifrado.

A criptografia assimétrica utiliza duas chaves diferentes, matematicamente relacionadas de tal forma que seja possível o remetente da mensagem cifrar com uma das chaves, denominadas pública, e que o destinatário consiga decifrar a mensagem com outra chave relacionada, a privada. Ainda é necessário que, conhecendo a chave pública seja muito difícil de encontrar a chave privada, e vice-versa. De fato, é necessário a utilização das duas chaves para decifrar uma mensagem. (SCHNEIER, 1996)

A cifração além de prover confidencialidade, pode também prover autenticação por meio da **assinatura digital** que utiliza a criptografia de chave pública, no entanto neste caso o usuário que deseja autenticar uma informação, deve cifrar a mensagem com a sua chave privada, para que o ente que queira verificar a autenticidade dessa mensagem, o faça por meio da chave pública do usuário que cifrou a mensagem. Basicamente, a assinatura gera uma maneira de comprovar a origem de documentos, enviando dados cifrados junto com a informação.

No entanto as chaves públicas, devido a sua própria natureza, devem ser seguras de tal forma que não seja possível uma representação falsa da chave. Para atingir esse objetivo gera-se um **certificado digital** e são necessárias autoridades certificadoras, que são organizações confiáveis que fornecem uma garantia de que a chave pública em questão é autêntica e não ocorreram modificações nas mesmas. As autoridades certificadoras possuem um modelo hierárquico de autoridade, onde uma autoridade certificadora autoriza uma outra autoridade certificadora a emitir certificados para as chaves públicas. (BRASIL, 2012)

O **controle de acesso** é uma maneira de se controlar, uma vez que o usuário esteja dentro do sistema, quais informações o mesmo pode ter acesso e o que é permitido realizar com tais informações. Existem alguns tipos de controle, como o RBAC – Role Based Access

Control, que é um controle baseado em papéis, onde a informação é relacionada a um papel e os usuários possuem diferentes papéis, dependendo do seu nível de autorização. (NIST, 2007)

Existem outros mecanismos importantes como a auditoria que contém informações de atividades armazenadas em logs protegidos e backups, que são meios projetados para recuperar uma informação perdida ou alterada. (STALLINGS, 2008)

2.4 ATAQUES, VULNERABILIDADES, RISCOS E AMEAÇAS PARA A SEGURANÇA DA INFORMAÇÃO

Para melhor compreensão, é importante definir a diferença entre os seguintes termos: ameaça, vulnerabilidade, risco e ataque. De acordo com o NIST ameaça é uma circunstância ou evento com o potencial de impactar de forma negativa, por meio de sistemas de informação, uma organização, pessoa ou nação. Segundo a ABNT (2011) *"O risco de segurança da informação está associado com o potencial de que ameaças possam explorar vulnerabilidades de um ativo de informação ou grupo de ativos de informação e consequentemente causar dano a uma organização."* (ABNT NBR, 2011)

A **vulnerabilidade** trata-se de uma fraqueza na implementação, no controle, na configuração ou no procedimento de segurança em sistemas, que podem ser exploradas por uma ameaça.

O **risco** é uma medida de probabilidade da ocorrência de uma fonte que **ameaça** explorar uma vulnerabilidade gerando um impacto.

O **ataque** é uma ação ou tentativa, com objetivo de causar algum dano ou obter uma informação, sem autorização, podendo ser uma manifestação de uma ameaça, como o DDoS, o *spoofing* ou um ataque de força bruta. (NIST, 2002)

- O *spoofing* é uma maneira do atacante falsificar a identidade se passando por um usuário confiável para obter informações ou desviá-las. Ele utiliza algumas vulnerabilidades dos protocolos, IP – *Internet Protocol*, ARP - *Address Resolution Protocol* e DNS - *Domain Name System* para realizar o ataque. Quando um atacante gera um ARP *Spoofing*, ele pode estar querendo realizar um ataque chamado *Man-in-the-middle.*
- O ataque de foça bruta, é um ataque que leva tempo pois ele simplesmente tenta todas as possibilidades de descoberta de senha, por exemplo. No entanto este ataque tem como o seu aliado o ataque de dicionário, que diminui o

número de tentativas consideravelmente, pois utiliza palavras, sequências e datas que tenham algum significado.

- O ataque de negação de serviço, é quando o atacante tem a intenção de criar uma situação que faça com que um servidor tenha seu buffer estourado com um bombardeamento de informações, gerando a indisponibilidade desse serviço. Ele é mais utilizado na sua versão distribuída, onde o atacante utiliza a sua máquina para controlar outras máquinas para atacar um alvo coordenadamente.
- Outros ataques como as fraudes são muito utilizadas, principalmente por e-mail, como o *sniffing*, onde o atacante rouba informações de rede por meio da interceptação de tráfego, e a varredura que tem como objetivo realizar buscas minuciosas na rede e máquinas para coletar informações, lembrando que este pode ser utilizado de maneira legítima no gerenciamento de rede. (BRASIL, 2012)

Sendo assim devemos nos proteger contra ataques, reduzir as vulnerabilidades, monitorando as ameaças e diminuindo os riscos nos sistemas projetados. A figura 2.1 ilustra o relacionamento dos conceitos de gerenciamento de risco, modelando uma estratégia de identificar o risco.

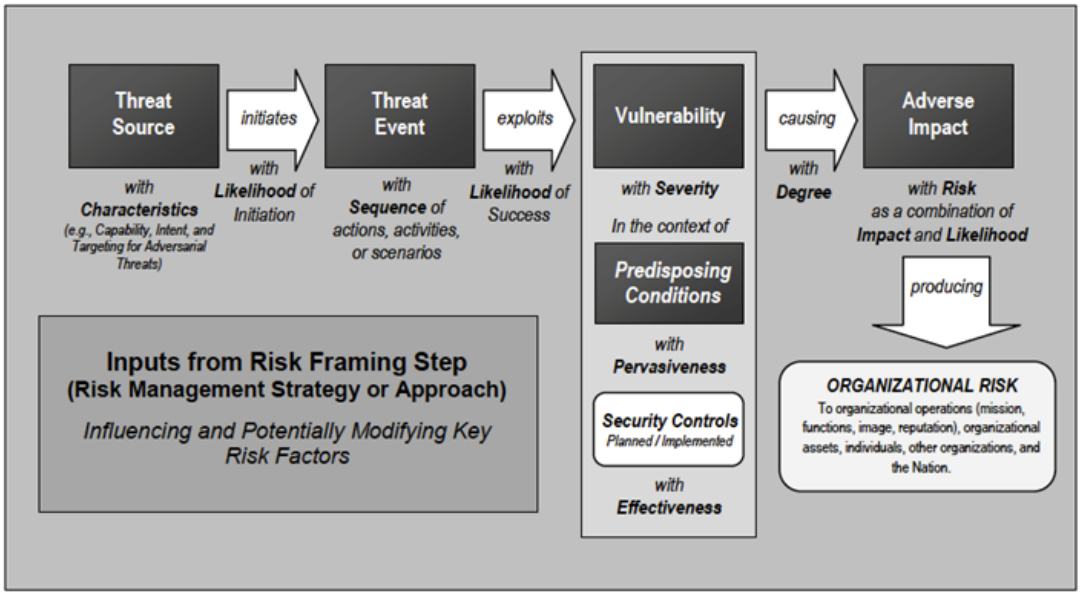

Figura 2.1. Modelo de estratégia de gerenciamento de Risco. (NIST, 2001)

De fato a segurança depende de diversos fatores, devendo ser analisada e estudada em cada caso, como a situação da informação no momento do ataque, se ela está sendo

transmitida, processada ou armazenada. Os diferentes estados da informação criam ambientes com vulnerabilidades específicas para cada caso. Dependente ainda da tecnologia, política e procedimento aplicados a informação, isto torna o trabalho dos gestores de segurança da informação extremamente importante, pois os atacantes não irão se restringir apenas a questões técnicas.

Uma das principais atividades da gestão de segurança da informação é o gerenciamento de risco, que de acordo com a norma ABNT NBR ISO/IEC 27005:2011 apresenta processos contínuos que devem explorar o ambiente da corporação para identificar os riscos vinculados, analisando e avaliando a possibilidade de ocorrência assim como impacto sobre o negócio, para gerar recomendações que diminuam as consequências até um nível aceitável. A figura 2.2 mostra o processo de gestão de risco da segurança da informação.

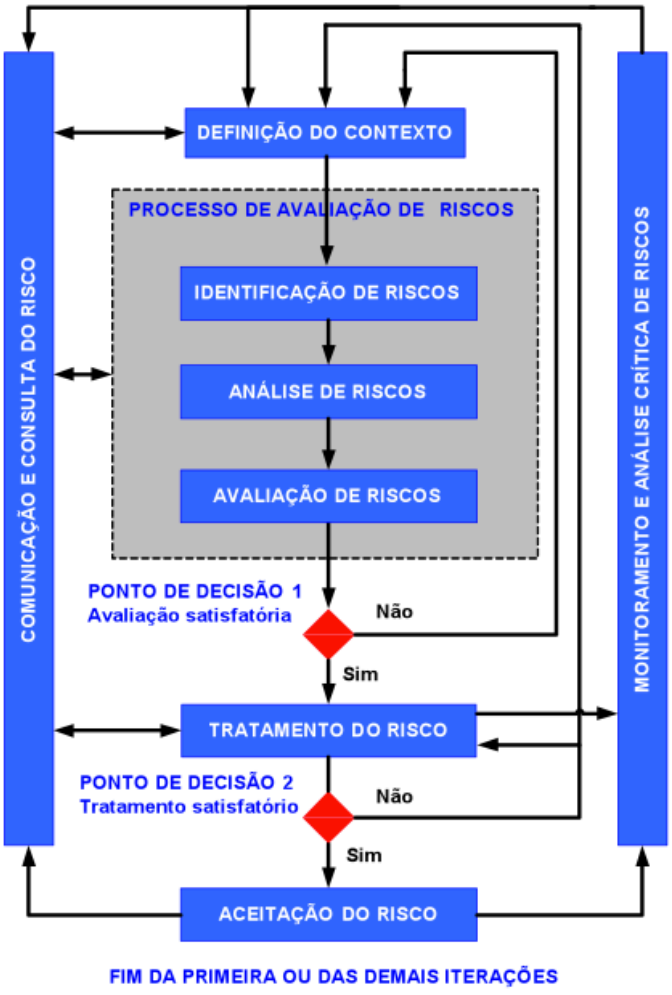

Figura 2.2. Processos de gestão de risco da segurança da informação. (ABNT, 2011)

O processo de gestão de risco da informação inicia com a definição do contexto que determina os critérios, escopos e limites da organização, que são as entradas do processo de avaliação de risco contendo as atividades de identificação de risco, análise de risco e

avaliação de risco. A identificação de risco revela os ativos, ameaças, controles e vulnerabilidades, enquanto a análise de risco foca na probabilidade e impacto do risco que é categorizado por métodos qualitativos e quantitativos. Na avaliação de risco é realizada a comparação do nível do risco com os critérios de aceitação, para priorizar o tratamento de risco. A aceitação do risco envolve o registro formal do tratamento utilizado, que pode ser a modificação, a retenção, o compartilhamento ou a contenção do risco. Por fim, deve ser realizado o monitoramento e distribuição dos resultados para as partes interessadas que executarão uma análise crítica do processo. (ABNT NBR, 2011)

A gestão de risco de segurança da informação possui um papel importantíssimo na complementação da segurança da informação, sendo essencial no desenvolvimento de sistemas, auxiliando no planejamento estratégico do negócio e identificando fraquezas de projeto e implementação antecipadamente.

2.5 SEGURANÇA DE REDES

Devido à situação atual dos serviços e produtos estarem ligados de alguma maneira com a *Internet*, sendo necessária uma rede para realizar a conexão, é essencial criar meios de proteção dos dados que trafegam pela mesma. O crescimento da *Internet* fez com que pessoas mal intencionadas cada vez mais se aproveitem da ingenuidade e desinformação das pessoas para criar golpes e invasões. Portanto, é importante certificarmos que a rede seja segura para os usuários, com básicos sistemas de proteção.

A segurança na rede também pode ser dividida, mais precisamente em camadas. A segurança pode ser implementada na camada de rede por meio do IPSec - *Internet Protocol Security*, por exemplo, ou na camada de transporte, por meio do SSL/TLS – *Secure Socket Layer/Transport Layer Security*, por exemplo. Não há problemas, exceto de performance, em se utilizar conjuntamente os dois protocolos de segurança. (TANENBAUM, 2003)

O IPSec é um conjunto de protocolos que fornece segurança no nível de rede da arquitetura OSI – *Open System Interconnection* de rede, onde é possível criar uma rede privada virtual mantendo o sigilo da comunicação fim a fim dos usuários. As funcionalidades variam de acordo com a necessidade de segurança da informação desejada, podendo prover autenticação, confidencialidade e gerenciamento de chaves, utilizando algoritmos criptográficos existentes. Os serviços a serem fornecidos dependem da técnica que será utilizada na proteção da mensagem, podendo ser o AH - *Authentication Header*, o ESP -

Encapsulating Security Payload, que são baseados em associações de segurança, que geram uma relação unidirecional de serviço de segurança, ou o IKE - *Internet Key Exchange*.

O AH não possui a funcionalidade de prover serviços de confidencialidade, e sim integridade sem conexão, autenticação da origem, *anti-replay* e controle de acesso. O AH pode ser realizado de 2 maneiras: a primeira é a forma de transporte, onde o cabeçalho IP do pacote original é mantido o mesmo, e apenas é inserido informações sobre os parâmetros a comunicação. A outra maneira é a modo túnel, onde um novo cabeçalho IP é criado e adicionado ao pacote por roteador, e novamente adicionado informações e parâmetros ao pacote. A autenticação é realizada no pacote inteiro, todo o pacote é cifrado.

O ESP pode ser utilizado de duas maneiras: a primeira provê serviços de confidencialidade, *anti-replay* e controle de acesso, e a outra são adicionados os serviços de autenticação da origem e integridade sem conexão. Assim como o AH, o modo transporte não adiciona um novo cabeçalho IP e insere informações de parâmetros, mas a autenticação do cabeçalho IP não é realizada, bem como a confidencialidade é fornecida apenas para os dados e o cabeçalho da camada de transporte. No modo túnel o serviço de confidencialidade e autenticação são expandidos para o cabeçalho IP da máquina de origem, e um novo cabeçalho IP é criado e concatenado ao pacote. Este caso é mais realizado entre roteadores de borda.

O IKE utiliza o protocolo Oakley *Key Determination Protocol* para a troca de chaves genérico sem especificar formatos, sendo baseado no algoritmo de *Diffei-Hellman* e no ISAKMP - *Internet Security Association and Key Management Protocol* para o gerenciamento de chaves que especifica protocolos de suporte, formatos e negociações de atributos de segurança.

O SSL/TLS é um conjunto de protocolos que protege a interseção da camada de transporte e aplicação da arquitetura OSI, e específico para o TCP – *Transmission Control Protocol*, apesar de existir uma variação para o UDP – *User Datagram Protocol*. O motivo da proteção de ser entre camadas, é o fato de que parte desse conjunto de protocolo está na camada de transporte como o SSL *Record Protocol*, e a outra junto dos protocolos que utilizam o TCP, como o HTTP - *Hypertext Transfer Protocol*, o SSL *Handshake* por exemplo.

Inicialmente o pacote original é fragmentado em partes menores, onde cada pedaço pode ser opcionalmente compactado antes da geração do *hash* de autenticação, adicionando um MAC - *Message Authentication Code* a mensagem. O processo é continuado pela cifração dos fragmentos do pacote que por final recebem um cabeçalho SSL. (STALLINGS, 2008)

Existem diversos meios de se proteger, tanto no próprio computador, como backups, contas e senhas, ou na rede, como *firewalls*, filtros e *antimalwares*. No entanto, um dos mais

eficientes mecanismos de proteção é a prevenção com a criptografia, que atua na troca de informações e no armazenamento. As assinaturas digitais, certificações digitais e as funções *hash*, derivam de métodos criptográficos e são amplamente utilizadas na infraestrutura de segurança de redes. Assim como a infraestrutura de chaves públicas, que no caso nacional é mantida pela ICP – Infraestrutura de Chaves Públicas - Brasil. Esse conjunto de mecanismo é que torna possível a implementação de sistemas que necessitem de sigilo nas comunicações e proteção de dados sensíveis.

2.6 WEB SERVICES

A evolução da *Internet* passou de apenas um repositor de dados e informações para também um grande provedor de serviços, que facilita e agiliza a vida das pessoas mundo afora. Grande parte das aplicações utilizadas em redes governamentais e corporativas nasceu de necessidades e ideias para atender determinadas situações. Desta forma, os sistemas eram desenvolvidos voltados para atender funções específicas de uma determinada situação, consumindo tempo e recurso. Na medida em que surgiam novas demandas outros sistemas eram desenvolvidos e agregados ao conjunto de sistemas existentes de uma corporação, aumentando o consumo de recursos e a manutenção dos mesmos.

Diante deste contexto surgiu necessidade de integração entre as ferramentas e aplicações de forma a gerar dados mais completos de acordo com o necessário e diminuir o custo e tempo de desenvolvimento, assim como o consumo de recursos necessários. A solução seria criar uma arquitetura que pudesse ser flexível, interoperável e com reuso. Dessa necessidade, surgiram modelos como SOA – Service Oriented Architecture, Cloud Computing, Grid Computing e Web Services. Segundo a W3C, a definição de Web Service é:

> *"Definição: Um Web Service é um sistema de software projetado para suportar a interação interoperável entre máquinas de uma rede. Possui uma interface descrita em um formato processável por máquinas (especialmente o WSDL). Outros sistemas interagem com Web Service de uma maneira prescrita na sua descrição usando mensagens SOAP, tipicamente transmitida através do HTTP com uma serialização XML conjuntamente de outros padrões relacionados."* (W3C, 2004)

O Web Service é uma "Aplicação lógica, programável que torna compatíveis entre si os mais diferentes aplicativos, independentemente do sistema operacional, permitindo a comunicação e intercâmbio de dados entre diferentes redes." (BRASIL, 2013) que tem como objetivo promover a comunicação entre sistemas com ambientes heterogêneos e com fraco acoplamento, para que métodos e funções possam ser chamadas remotamente. Esta arquitetura possui elementos definidos pela W3C e pelo OASIS, e no seu modelo tradicional

se encontra o WS-*, que utiliza os conceitos de SOAP - *Simple Object Access Protocol*, UDDI - *Universal Description, Discovery and Integration*, WSDL - *Web Services Description Language* e XML - *eXtensible Markup Language*. (IBM, 2001)

As características de Web Service, como a interoperabilidade, abstração e as especificações disponíveis ao público, admitem um caráter genérico quanto a linguagem de programação e a plataforma, assim como o aproveitamento de Web Services já implementados e a infraestrutura de rede existente, sem a necessidade de se conhecer os detalhes operacionais. A exposição pública do negócio permite a combinação, compartilhamento ou adequação das funcionalidades de um ou mais Web Services para ser utilizada na estratégia de implementação do serviço. (BRASIL, 2013)

O funcionamento de um Web Service, após a implementação do mesmo, começa na criação e registro do WSDL referente ao serviço criado no provedor de serviço. Em seguida deve ser inserido no registro de serviço como o UDDI para que os usuários possam buscar de forma organizada os serviços desejados. O usuário neste momento pode achar um serviço que procure pesquisando no UDDI, que o retornará com o WSDL do cliente, que por sua vez comporá um pedido de utilização do serviço que será enviado dentro de uma mensagem SOAP, por exemplo. Em seguida o provedor do serviço processa e responde o pedido, também por uma mensagem SOAP que ao chegar no consumidor, usufrui da informação ou serviço. A figura 2.3 mostra os passos de como é o descobrimento dos serviços e os relacionamentos dos componentes de um Web Service. (BREITMAN, 2005)

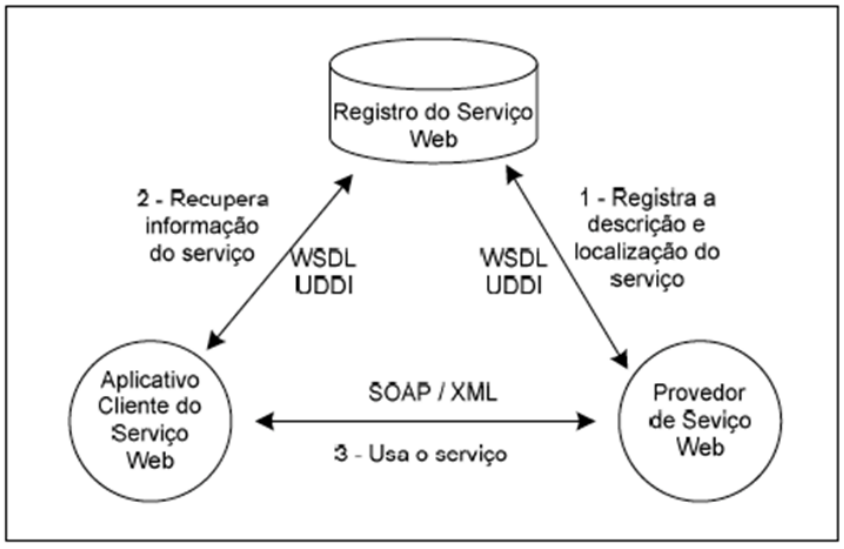

Figura 2.3. Modelo de descobrimento dos serviços Web. (WATHIER, 2005)

O XML é um formato de linguagem bem estruturado, independente de software ou hardware para a troca de informações via Web. O XML é muito utilizado em serviços web e é a base de linguagem de marcação, que é uma linguagem descritiva e é utilizada em técnicas

como SAML, que está descrita posteriormente. Um documento XML deve ser bem formado, com regras que devem ser seguidas na elaboração do documento e hierarquizado sendo possível a sua representação por árvores. O XML possui uma construção lenta, no entanto o protocolo é estabelecido rapidamente e padronizado.

A validade de um documento XML depende se o mesmo é bem formado e da sua gramática, ou *schema,* que possui as *tags* validas, a definição de ordem e tipos e a hierarquia. Pode ser um DTD – Document Type Definition, que é mais simples e limitado, ou um XSD – XML Schema Definition, mais complexo.

O SOAP é um protocolo de troca de informações de forma estruturada para plataformas descentralizadas e distribuídas, sendo a estrutura baseada em XML. Trata-se de um protocolo de transporte, responsável pelo envio de mensagens entre aplicações e possui três principais partes: o envelope, o cabeçalho e o corpo da mensagem. Essa estrutura gera organização e facilidade na transmissão da mensagem. O envelope tem como objetivo gerar uma padronização da mensagem, para que a mesma possa utilizar diversos protocolos de transporte, como o HTTP, fazendo como que a aplicação não dependa desses protocolos.

Dentro do envelope se encontra o cabeçalho e o corpo da mensagem, o primeiro responsável por fornecer informações sobre a gerência e segurança da troca de informações. O corpo SOAP mantem informação útil para a aplicação, com os dados específicos para a mesma. (WATHIER, 2005) Atualmente a W3C mantém o padrão SOAP, com a responsabilidade de realizar manutenções e melhorias nos modelos de extensão, processamento e estrutura do SOAP garantindo a confiabilidade da utilização do protocolo. A figura 2.4 ilustra a estrutura da mensagem SOAP e seus componentes.

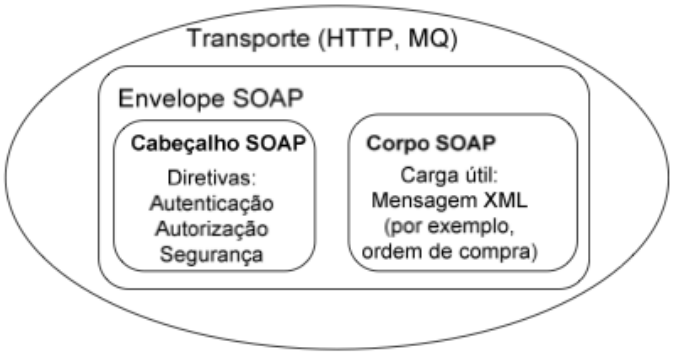

Figura 2.4. Estrutura do protocolo SOAP. (WATHIER, 2005)

O UDDI é o registro de serviços, onde há uma catalogação dos serviços, para que os mesmos possam ser descobertos mais facilmente. De maneira padronizada e organizada os serviços são expostos para que um cliente possa buscas e decidir qual serviço lhe melhor atende.

A informação em um UDDI é dividida, para uma melhor agilidade na localização da mesma, em três partes, que são denominadas páginas. As páginas brancas contêm os dados da empresa, como o nome o contato e a descrição da mesma. As descrições dos serviços, assim como seu código são disponibilizados nas páginas amarelas. Por fim, as páginas verdes oferecem as informações técnicas dos serviços, inclusive a especificação em WSDL e as regras de e-business. O UDDI permite que serviços e negócios sejam descritos para que outras empresas ou usuários descubram e interajam com as aplicações oferecidas.

O WSDL é a linguagem que descreve os serviços, as definições e parâmetros dos métodos e funções desejadas, sendo dividida em parte concreta e abstrata. A parte concreta contem os detalhes de como será realizada a comunicação entre os entes, os protocolos e formatos a serem usados estão na seção *bindind*, os endereços de saída estão na seção *port* e as portas na parte denominada *service*. A parte abstrata permite que as definições tornem os métodos independentes de sistemas operacionais e linguagem de programação, mas para isto é necessária a definição dos tipos de dados, interfaces, parâmetros de saída e entrada, dentre outros.

A W3C também mantém o WSDL, que está na versão 2.0, sendo bem aceita como padrão para a descrição de Web Services, que permite o aproveitamento de serviços de terceiros sem a necessidade de saber as operações internas, aplicando apenas os argumentos, protocolos e informações na composição e realização do trabalho desejado. A figura 2.5 mostra as divisões da parte abstrata e concreta de um documento WSDL. (HARTMAN, 2003)

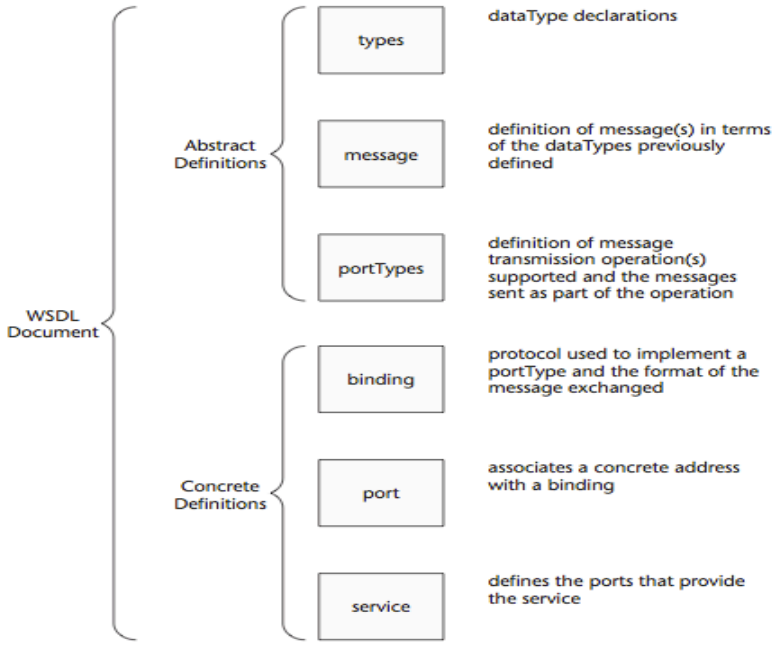

Figura 2.5. Estrutura de um documento WSDL. (HARTMAN; FLINN; BEZNOSOV; KAWAMOTO, 2003)

A primeira fase de um Web Service é a própria construção e documentação do serviço, que será armazenada no servidor utilizando o WSDL. O segundo passo, é a publicação do serviço, que será feita no UDDI, para que na terceira fase o usuário possa localizar o serviço desejado no UDDI, de forma rápida e organizada. Ao escolher o serviço, o UDDI retorna para o usuário a descrição do serviço, a interface e meio de acesso do mesmo. O usuário agora possui todas as informações necessárias para requisitar o serviço, requisitando-o e recebendo o serviço do provedor.

Devido ao alto custo de construção de um documento em XML, os desenvolvedores criaram uma outra forma de se realizar um Web Service, onde as mensagens de troca de informação entre aplicativos não utilizassem mensagens SOAP, diminuindo a complexidade do sistema. O REST - *Representacional State Transfer* surgiu com uma proposta de ser mais simples e de consumir menos recursos. A base da sua comunicação é o protocolo HTTP, onde são aproveitados os recursos de *Post, Get, Put, Delete* do protocolo HTTP. Além do meio de troca de informações, o REST também utiliza um equivalente ao WSDL padrão, no entanto este é modelado com URI - Uniform Resource Identifier e utiliza semântica para realizar a descrição dos serviços. Os parâmetros de comunicação e de serviço são enviados via URI, e podem retornar, por exemplo, por meio de um JSON - JavaScript Object Notation. Este método deixa menor o tamanho das mensagens e o processamento mais rápido, no entanto diminui o controle e segurança transacional. Apesar de menos seguro, ele vem sendo cada vez mais utilizado, principalmente para Web Services simples que não precisam de muitos serviços de segurança, sendo uma opção mais rápida e simples. Este modelo ainda possui duas situações, o *stateless* é a maneira mais simples e rápida de se implementar um Web Service baseado em REST, no entanto ela não utiliza informações de sessão e não sincroniza os dados. O modelo *statefull*, é mais robusto por guardar e utilizar informações da sessão do usuário e acompanhar a navegação do mesmo, fornecendo mais controle para a aplicação. (IBM, 2008)

De fato mesmo os Web Service baseados em SOAP estão sujeitos a diversos riscos, como por exemplo, no UDDI é necessário um controle na inserção e atualização de serviços, pois um atacante poderia criar ou alterar um registro, apontando para um serviço falso ou uma aplicação maliciosa, se o UDDI não for protegido. Ainda com o UDDI é possível o atacante utilizar as informações de padrões, especificações e comportamentos do serviço que está catalogado e achar alguma falha ou vulnerabilidade no serviço. O mesmo deve ser feito no WSDL, pois um atacante poderia alterar um serviço para conseguir informações privadas de usuários ou conseguir informações da arquitetura ou requisitos de segurança. A mensagem SOAP deve possuir os principais serviços de segurança para que a mensagem não possa ser

interceptada por um atacante. No entanto, somente o protocolo SOAP não gera proteções de integridade, confiabilidade e autenticidade e não possui um mecanismo de detecção de mensagens duplicadas. (NIST, 2007)

No entanto, existem modelos e padrões de segurança para Web Services e cada vez mais pesquisas estão sendo realizadas para criar um ambiente seguro para aplicações que utilizem Web Services. Como um padrão de segurança em Web Services temos o WS-Security.

2.7 SEGURANÇA DA INFORMAÇÃO PARA WEB SERVICES

Os sistemas baseados em arquiteturas distribuídas possuem características muito buscadas tanto pelos provedores como pelos usuários, fornecendo uma maneira inteligente de prover escalabilidade, interoperabilidade e agilidade. No entanto, isto traz complicações, como a segurança, a governança, a gestão e a *performance*. Estes controles devem estar presentes em todas as etapas dos processos de implementação e utilização de um sistema distribuído. No entanto, a segurança, sempre foi um dos problemas existentes que mais são buscados, devido ao número de informações que são trocadas.

A arquitetura distribuída de Web Services e as suas características dificultam a implantação da segurança nos Web Services, criando desafios como a emissão segura de credencias, a descoberta de *cover channels* e serviços comprometidos, a implementação correta de WS e a proteção contra os ataques de negação de serviço e a propagação de vírus e *malwares* embutidos no protocolo SOAP. (NIST, 2007)

Segundo Hartman et al (2003) *"O que torna a segurança de Web Services tão desafiante é a natureza distribuída e heterogênea desses serviços. A tecnologia de Web Services é baseada na interoperabilidade de várias aplicações de software diferentes..."* (HARTMAN, 2003). Para entender melhor as necessidades de segurança em ambientes que utilizem Web Services, são definidas algumas dimensões de segurança. As dimensões são essenciais na implementação segura de um Web Service e cada uma afeta um aspecto diferente de um Web Service. São elas: a segurança da mensagem, a proteção de recursos, a negociação de contratos, a gerência de confiança e as propriedades de segurança.

A segurança da mensagem é a dimensão que garante que mensagens SOAP não sejam modificadas ou bisbilhotadas por atacantes. Já a proteção de recursos advém da natureza pública de Web Services, onde garante que Web Services sejam protegido contra acessos não autorizados por meio de mecanismos de identificações, autenticações e controle de acessos. Essa proteção precisa de entidades confiáveis no envolvimento das transações.

Para gerar essa confiança de identidade dos entes de um Web Service, é necessário estabelecer um domínio da gerência de confiança.

A negociação de contratos é também um dos objetivos das arquiteturas orientadas a serviços nos processos de negócio, e para os Web Services esse domínio permite seja possível negociar contratos que respeitem as qualidades de serviço e proteção desejadas nas transações. O domínio de propriedades de segurança deseja alcançar um meio de se implementar Web Services, usando as ferramentas, processos e técnicas seguras, dificultando os ataques e diminuindo as vulnerabilidades.

Na figura 2.6 podemos observar um modelo de segurança em camadas, onde a segurança da mensagem é estabelecida pelo IPSec, SSL\TLS e XML *Encryption* e XML *Authentication*, que são implementados cada um em uma camada diferente.

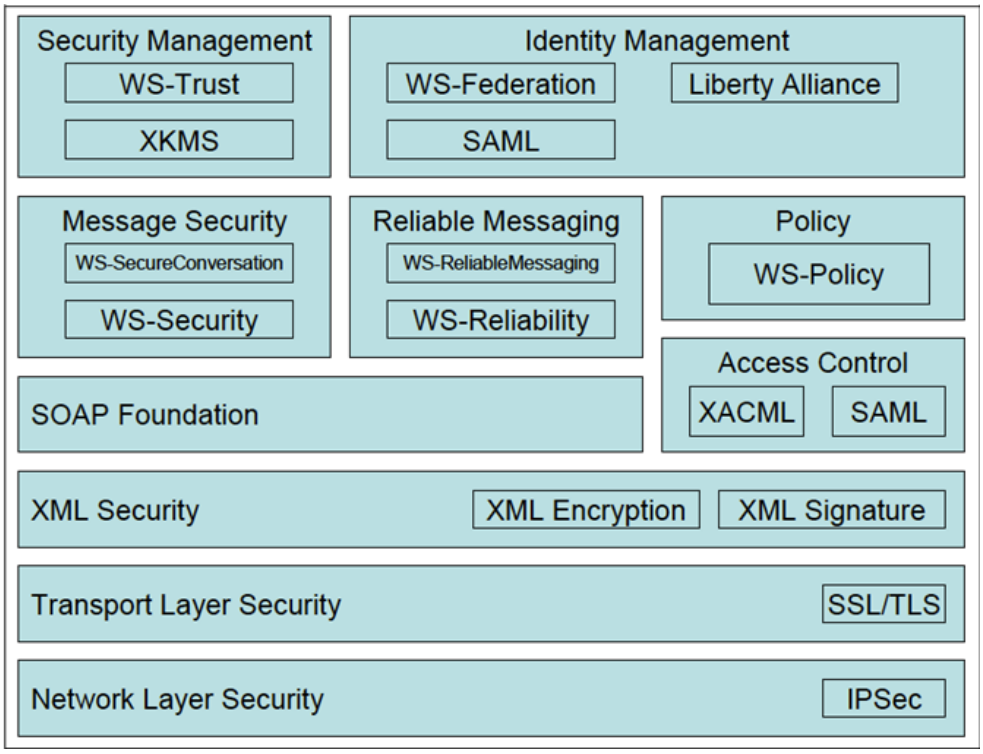

Figura 2.6. Pilha de padrões de segurança de Web Services. (NIST, 2007)

Nas camadas superiores existe uma divisão quanto a dependência do protocolo SOAP. O XACML – *eXtensible Access Control Markup Language* e o SAML – *Security Assertion Markup Language* são padrões não exclusivos de Web Services, enquanto os WS-*Security*, WS-*Trust*, WS-*Federation*, WS-*Reliability*, WS-*Policy*, WS-*Secureconversation*, o WS-*Reliablemessaging* e o XKMS – XML *Key Management Specification* são padrões específicos para serem aplicados a Web Services. (NIST, 2007)

- O XKMS é um modelo de distribuição de chaves públicas baseado em XML, que inclui informações sobre chaves, registro, verificação e revogação. O XKMS foi criado com o objetivo de dar suporte de gerenciamento de chaves ao XML *Encryption* e o XML *Authentication*, que utilizam chaves públicas para prover os seus serviços. (W3C, 2001)
- O WS-*Policy* como o próprio nome diz, define um modelo e arcabouço para a definição de políticas, como as restrições das normas de segurança, capacidades específicas de domínio, requisitos e características das entidades do Web Service. Permite a especificação de políticas QoS – Quality of Service e segurança usando XML.
- O WS-*Trust* descreve um modelo para se obter um relacionamento de confiança direto, ou por meio de terceiros e intermediários. Esse modelo de confiança é baseado em operações para adquirir, emitir, renovar e validar tokens de segurança e formas de serem criadas novas relações de confiança através de serviços intermediários, que são denominados *Security Token Service*.
- O WS-*Secure Conversation* permite que seja realizada a autenticação e o gerenciamento de troca de mensagens seguras, pelo intercâmbio de chaves de sessão, permitindo uma conexão segura para que vários serviços possam conversar e trocar informações. Este padrão define três meios de se estabelecer os contextos de segurança, que incluem as chaves simétricas de sessão: o SCT - *Secutiry Context Token* criado pelo *Security Token Service*, o SCT criado por um das partes da comunicação e enviado com a mensagem, ou o SCT criado através de negociações. (SANTOS, 2008)
- O WS-*Federation* é a base de relacionamento para ambientes heterogêneos, com diferentes plataformas ou tipos de dados mas que estejam associados, para prover um serviço único. Permite o gerenciamento de serviços de suporte a identidade, atributos, autenticação e autorização entre entes com domínios de segurança diferentes. Define federações de serviço sobre o WS-Trust, onde permite a troca de security tokens entre domínios de segurança diferentes, sem requerer que a identidade ou atributos local sejam apresentadas no serviço de destino. (SANTOS, 2008)
- Os WS-*Reliability* e WS-*Reliable Message* são dois padrões que permitem que o serviço de segurança de disponibilidade seja suportado em Web Services. Apesar do foco não ser a proteção contra ataques de DoS, permite

uma garantia de entrega das mensagens de uma troca de informação, por meio das seguintes semânticas: *At-least-once*, que garante a entrega de uma mensagem, *At-most-once*, que garante que uma mensagem duplicada não será entregue, e *Exactly-once*, que garante que a mensagem será entregue sem duplicação.

- O XACML é um padrão mantido pela OASIS que define uma linguagem baseada em XML de política e de decisão de requisições e respostas para controle de acesso. A linguagem de política é utilizada para descrever requisitos gerais de controles de acesso, definindo funções, tipos de dados, combinações lógicas, dentre outros. A linguagem de requisição e resposta cria uma pesquisa que permite descobrir se uma ação está autorizada ou não. As respostas podem ser do tipo permitido, negado, indeterminado (onde ocorreu algum erro), ou não aplicável, onde a ação não pode ser avaliada pelo serviço. (KIM, 2009)
- Outro componente importante para segurança mantido pela OASIS é o SAML, que fornece meios de troca de credenciais entre dois entes, ou quando um Web Service precisa trocar dados com outro Web Service para fornecer o serviço final. Provendo serviços de interoperabilidade entre diferentes sistemas de segurança, autenticação, autorização e federação, que é a troca de dados e requisições de diferentes empresas, suportando também o SSO – *Single Sing On*, facilitando a navegação do usuário, um *login* único com o acesso a diversas aplicações. Devido a natureza de um Web Service, é de extrema importância que a interoperabilidade das aplicações seja protegida e segura, desta forma o SAML fornece uma padronização de troca de informação segura entre diferente aplicações. Permitindo que um usuário possa transferir seus direitos e autorizações entre diferentes Web Services. (WATHIER, 2005)

No modelo o SAML e o XACML geram um controle de acesso seguro e padronizado. No entanto, a segurança não deve se restringir a apenas ao acesso não autorizado, pois um atacante pode estar apenas espiando, ou usando um ataque de *man-in-the middle* por exemplo. (OASIS, 2012)

O *Liberty Alliance* foi criado em 2001 para gerar padrões de gerenciamento de identidade de sistemas, no entanto desde 2009 ele foi extinto e seus trabalhos foram transferidos para a *Kantara Iniciative*.

O WS-Security é um padrão de segurança estabelecido para aplicações de Web Services que utilize como meio de troca de informações o protocolo SOAP, possuindo como principal meio de comunicação a segurança da informação a nível de aplicação ou de mensagem, pois em Web Services, o desempenho da troca de informações é fundamental para o funcionamento do mesmo. Os mecanismos de segurança quando aplicados em nível de rede e transporte, podem atrasar a comunicação devido ao elevado processamento nessas camadas. Este padrão é mantido pela organização OASIS, que reúne diversos mecanismos, tecnologias e modelos de segurança para proporcionar interoperabilidade entre plataformas e linguagens, mantendo os principais serviços de segurança. Trata-se de um conjunto de documentos, onde cada um explora um mecanismo de segurança da informação para Web Services que utilizem SOAP. Nesses documentos são elaboradas maneiras de se utilizar o protocolo SOAP para enviar de forma segura parâmetros para troca segura de informações e *tokens*. (WATHIER, 2005)

A ideia de se implantar segurança em nível de mensagem seria poder cifrar ou assinar apenas a parte da mensagem que fosse sigilosa, tornando muito mais rápido procedimento de cifração, decifração e assinatura, sendo fornecidas, respectivamente, pelo XML *Encryption* e o XML *Signature*. O WS-Security, também utiliza *tokens* que carregam informações de segurança, como o nome do usurário e a senha, e certificados X.509 e tickets *Kerberos*. O modelo *Kerberos* funciona com tickets que são trocados entre um ente confiável e o usuário e entre o ente confiável e o servidor, permitindo um acesso seguro do serviço. O X.509 trata-se de uma infraestrutura de chaves públicas que fornece um diretório com certificados de usurários.

O XML *Encryption* é mantido pela W3C e possui como principal vantagem, criptografar apenas as partes mais sensíveis do documento, mantendo pública a leitura de outras partes do documento. Isto é essencial para aplicações distribuídas, pelo fato de que antes de chegar ao destino final, a mensagem deve passar por entes intermediários para ser processada. Além de ser independente de protocolos de transporte e rede, possui uma melhor performance, que impacta no QoS da aplicação. Ele não propõe novos algoritmos, ou novos meios de trocas de chaves, mas utiliza modelos existentes, apenas especificando quais são os recomendados.

O XML *Signature*, também mantido pela W3C, utiliza a criptografia de chaves públicas para manter a integridade das partes selecionadas pelo usuário, provendo também a autenticação e o não-repúdio da mensagem. Por serem baseados em XML, são utilizados nas mensagens que utilizam SOAP. (OASIS, 2006)

As principais ameaças de um Web Service, são a alteração de mensagem, perda de confidencialidade, o ataque *man-in-the-middle*, falsificação de identidade, o *spoofing*, repetição de parte ou da mensagem inteira e a negação de serviço. No entanto, a importância de cada ameaça depende dos objetivos da corporação. Os mecanismos citados acima são soluções para boa parte dessas ameaças. (NIST, 2007)

Todos esses mecanismos de segurança, qualidade de serviço e confiança devem ser monitorados, controlados e reportados para que exista um mínimo de gestão da segurança da informação. Quando aplicado a ambientes que utilizem Web Services, os quesitos de disponibilidade, acessibilidade, performance, interoperabilidade e segurança devem estar sempre sobe monitoramento. Faz parte da gestão, verificar os parâmetros de utilização do Web Service para melhor monitorá-lo, como a frequência, acessos, durações, dentre outros. Existe uma dependência quanto as politicas de gestão que devem se comunicar com as capacidades de gestão citadas acima. Este entendimento deve ser realizado para que a relação entre o requisitante e o provedor seja alcançada. (W3C, 2004)

Foi possível concluir que a segurança da informação vai estar bem atrelada as tecnologias emergentes, sendo uma preocupação constante dos servidores e consumidores de serviços da *Internet.* A evolução da segurança deve acompanhar as inovações tecnológicas e o aumento das ameaças, senão irá comprometer ideias que podem revolucionar a interpretação de prestação de serviços, por exemplo o *Cloud Computing* ainda sofre com requisitos de segurança, que não estão satisfazendo os críticos e os usuários.

Os componentes de redes e de computadores possuem limitações físicas que fazem com que pessoas quebrem paradigmas e elaborem novos meios de se resolver um problema. Os Web Services possuem papel fundamental nas prestações de serviço *on-line* atual, devido as suas características de reusabilidade, interoperabilidade e baixo acoplamento, que torna essa tecnologia interessante do ponto de vista de custo e tempo de desenvolvimento.

Conforme outras novas tecnologias a segurança se torna um aspecto fundamental nessa arquitetura, sendo um dos mais relevantes a confidencialidade da troca de mensagem, a confiança entre aplicações, a preservação dos recursos, a coordenação de contratos e os domínios de segurança. A segurança para Web Services possui aspectos de ambientes distribuídos e de negócio, que permite a cobertura de diversas dimensões de segurança da informação, no entanto o fato de seus padrões de segurança serem especificados por mais de uma organização dificulta o desenvolvimento da tecnologia.

Apesar da segurança de Web Services possuir diversos padrões e especificações para a proteção de recursos e troca de mensagens que formam uma infraestrutura mais robusta e confiável, são necessárias outras abordagens de segurança da informação como a gestão de

risco, o desenvolvimento de medidas de recuperação e continuidade de negocio, a criação da defesa em profundidade e uma segura metodologia de implementação.

A seguir foi pesquisada na APF as recomendações de segurança em Web Services e as análise nas normas ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005 dos controles relevantes para o desenvolvimento de um Web Service.

3. RECOMENDAÇÕES DE TI NA ADMINISTRAÇÃO PÚBLICA FEDERAL E NORMAS INTERNACIONAIS

Neste capítulo foram abordadas algumas definições no que tange a Administração Pública Federal, sistemas de TI no governo, cartilhas de recomendação e leis que dizem respeito à segurança da informação. Em seguida foram abordados os controles das normas ABNT ISO/IEC 27001:2006 e ABNT ISO/IEC 27002:2005 no contexto de segurança para o desenvolvimento de sistemas Web Services.

3.1 A ADMINISTRAÇÃO PÚBLICA FEDERAL

A Administração Pública, segundo Moraes (2008), pode ser definida objetivamente como a atividade concreta que o Estado desenvolve para assegurar os interesses coletivos e subjetivamente como o conjunto de órgãos e de pessoas jurídicas aos quais a Lei atribuiu o exercício da função administrativa do Estado. Desta forma, sob este aspecto operacional a administração pública é o desempenho contínuo e sistemático, legal e técnico dos servidores próprios do Estado, em benefício da coletividade. Assim, a administração pública tem como principal objetivo o interesse público, seguindo os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade e eficiência.

Segundo Di Pietro (2010), a administração pública direta é composta por órgãos integrantes da União, dos estados, dos munícipios e do Distrito Federal, aos quais é conferido o exercício de funções administrativas. Já a Administração pública indireta é composta por pessoas jurídicas com personalidade pública e privada realizando atividades de forma descentralizada. São entes da administração pública indireta fundações públicas, autarquias, empresas públicas e sociedades de economia mista.

3.2 SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA

A segurança da informação nos órgãos e entidades da Administração Pública Federal Brasileira é instituída pelo decreto presidencial nº 3.505 de 13 de junho de 2000. Neste documento fica instituída a política de segurança da informação nos órgãos e nas entidades da Administração Pública Federal e abrange os seguintes pressupostos básicos (BRASIL, 2000):

- Assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
- Proteção de assuntos que mereçam tratamento especial;
- Capacitação dos segmentos das tecnologias sensíveis;
- Uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
- Criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
- Capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado;
- Conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

A Segurança da informação, segundo a conceituação adotada pelo Governo Federal Brasileiro (BRASIL, 2000), trata da proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Desta forma, a legislação ainda aborda os objetivos da política da segurança da informação conforme descrito abaixo: (BRASIL, 2000)

- Dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;
- Eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;
- Promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;
- Estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;
- Promover as ações necessárias à implementação e manutenção da segurança da informação;

- Promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;
- Promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação;
- Assegurar a interoperabilidade entre os sistemas de segurança da informação.

Ainda, segundo o decreto presidencial nº 3.505 de 13 de junho de 2000, as seguintes diretrizes de segurança da informação, assessoradas pelo comitê Gestor da Segurança da Informação, são adotadas: (BRASIL, 2000)

- Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos de que trata o artigo anterior, visando garantir a adequada articulação entre os órgãos e as entidades da Administração Pública Federal;
- Estabelecer programas destinados à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da segurança da informação;
- Propor regulamentação sobre matérias afetas à segurança da informação nos órgãos e nas entidades da Administração Pública Federal;
- Estabelecer normas relativas à implementação da Política Nacional de Telecomunicações, inclusive sobre os serviços prestados em telecomunicações, para assegurar, de modo alternativo, a permanente disponibilização dos dados e das informações de interesse para a defesa nacional;
- Acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação;
- Orientar a condução da Política de Segurança da Informação já existente ou a ser implementada;
- Realizar auditoria nos órgãos e nas entidades da Administração Pública Federal, envolvidas com a política de segurança da informação, no intuito de aferir o nível de segurança dos respectivos sistemas de informação;
- Estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos criptográficos, de modo a assegurar a

confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os Sistemas de Segurança da Informação;

- Estabelecer as normas gerais para o uso e a comercialização dos recursos criptográficos pelos órgãos e pelas entidades da Administração Pública Federal, dando-se preferência, em princípio, no emprego de tais recursos, a produtos de origem nacional;
- Estabelecer normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados e das informações, em vista da possibilidade de detecção de emanações eletromagnéticas, inclusive as provenientes de recursos computacionais;
- Estabelecer as normas inerentes à implantação dos instrumentos e mecanismos necessários à emissão de certificados de conformidade no tocante aos produtos que incorporem recursos criptográficos;
- Desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações;
- Estabelecer as normas relativas à implementação dos Sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilização dos dados e das informações de interesse para a defesa nacional;
- Conceber, especificar e coordenar a implementação da infraestrutura de chaves públicas a serem utilizadas pelos órgãos e pelas entidades da Administração Pública Federal.

3.3 ÓRGÃOS LIGADOS À SEGURANÇA NA ADMINISTRAÇÃO PÚBLICA FEDERAL

3.3.1 GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA

Criado pela Medida Provisória nº 1.911-20, de 24 de setembro de 1999, que alterou dispositivos da Lei nº 9.649 de maio de 1998, passou a Casa Militar a chamar-se Gabinete de Segurança Institucional que é dirigido pelo Ministro Chefe do Gabinete de Segurança institucional da Presidência da República. (BRASIL, 1998)

Desta forma, o Gabinete de Segurança Institucional é um Órgão essencial da Presidência da República e tem como área de competência os seguintes assuntos (BRASIL, 2010):

- Assistência direta e imediata ao Presidente da República no desempenho de suas atribuições;

- Prevenção da ocorrência e articulação do gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional;
- Assessoramento pessoal ao Presidente da República em assuntos militares e de segurança;
- Coordenação das atividades de inteligência federal e de segurança da informação;

Segurança pessoal do Chefe de Estado, do Vice-Presidente da República e dos respectivos familiares, dos titulares dos órgãos essenciais da Presidência da República e de outras autoridades ou personalidades quando determinado pelo Presidente da República, assegurado o exercício do poder de polícia;

- Segurança dos palácios presidenciais e das residências do Presidente da República e do Vice-Presidente da República, assegurado o exercício do poder de polícia.

Ainda cumpre ao Gabinete de Segurança Institucional exercer as atividades de Secretaria Executiva da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, de conformidade com regulamentação específica.

Dentro do Gabinete de Segurança Institucional da Presidência da República existe um departamento responsável pela segurança da informação e comunicações, o DSIC. Este departamento por objetivos as seguintes premissas (BRASIL, 2010):

- Adotar as medidas necessárias e coordenar a implantação e o funcionamento do Sistema de Segurança e Credenciamento - SISEC, de pessoas e empresas, no trato de assuntos, documentos e tecnologia sigilosos;
- Planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal;
- Definir requisitos metodológicos para implementação da segurança cibernética e da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal;
- Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;
- Estudar legislações correlatas e implementar as propostas sobre matérias relacionadas à segurança cibernética e à segurança da informação e comunicações;
- Avaliar tratados, acordos ou atos internacionais relacionados à segurança cibernética e à segurança da informação e comunicações, referentes ao inciso I;
- Coordenar a implementação de laboratório de pesquisa aplicada de desenvolvimento e de inovação metodológica, bem como de produtos, serviços e processos, no âmbito da segurança cibernética e da segurança da informação e comunicações;

3.3.2 SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO - SLTI

A Secretaria de Logística e Tecnologia da Informação - SLTI – tem como seu principal objetivo a ampliação da transparência e do controle social sobre as ações do Governo Federal no sentido de planejar, coordenar, supervisionar e orientar, normativamente com enfoque na melhoria da prestação de serviços por meio eletrônicos e na regulamentação das compras e contratações públicas relacionadas ao uso das tecnologias da informação e comunicação, no âmbito da administração Pública direta, autárquica e fundacional.

Neste sentido, competem à SLTI as seguintes premissas: (BRASIL, 2013)

- Propor políticas, planejar, coordenar, supervisionar e orientar normativamente as atividades:
  - ❖ de administração dos recursos de informação e informática, que compreendem a infraestrutura tecnológica de suporte ao ciclo da informação;
  - ❖ de serviços gerais, que compreendem as atividades de administração de material, transporte, comunicações administrativas e de documentação;
  - ❖ de gestão de convênios e contratos de repasse;
  - ❖ de governo eletrônico, relacionadas à disponibilização de serviços eletrônicos e de boas práticas;
  - ❖ de gestão de recursos de tecnologia da informação do Ministério, no âmbito do SISP;
  - ❖ de gestão de recursos de tecnologia da informação do Sistema de Informações de Serviços Gerais- SISG; do Sistema de Gestão de Convênios e Contratos de Repasse-SICONV; e do Programa Governo Eletrônico-e-GOV;
  - ❖ Presidir a Comissão de Coordenação do SISP;
  - ❖ Atuar como secretaria-executiva da Comissão Gestora do SICONV.

3.3.3 SISTEMA DE ADMINISTRAÇÃO DOS RECURSOS DE TECNOLOGIA INFORMAÇÃO - SISP

A necessidade de padronização e melhor gestão dos projetos de sistemas eletrônicos do governo, fez com que a SLTI – Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, criasse o Sistema de Administração de Recursos de Tecnologia da Informação – SISP para que fosse possível criar politicas, diretrizes e soluções de TI, voltadas para a Administração Pública Federal.

De acordo com o Decreto n. 7.579 de 11 de Novembro de 2011, atualmente em vigor, compete ao SISP definir modelos de planejamento, organização, coordenação, operação,

controle e supervisão de recursos de TI para as entidades e órgão da administração pública federal direta, autárquica e fundacional. Possui como Órgão Central a SLTI do MPOG, os Órgãos Setoriais, a Comissão de Coordenação, os Órgãos Seccionais e os Órgãos Correlatos. Dentre a suas finalidades encontramos a facilitação de obtenção de informação resguardando aspectos de disponibilidade, integridade, confidencialidade e autenticidade, a promoção de integração, interoperabilidade, padronização e normalização entre programas do governo para que possibilitem uma disseminação de informação de forma desconcentrada e descentralizada, desenvolver treinamentos e capacitações de profissionais de TI e aperfeiçoar os mecanismos de gestão de recursos de informação.

Um dos modelos documentados pela SLTI foi o Padrões de Interoperabilidade de Governo Eletrônico - e-PING, que estabelece premissas e especificações técnicas de interoperabilidade entre sistemas para o Governo. Esta arquitetura especifica em um de seus de segmentos de segurança, nos padrões recomendados e adotados para o desenvolvimento de sistemas, o WS-Security, o SAML e a assinatura e cifração via XML, que foram tratados neste trabalho.

3.4 LEGISLAÇÃO BRASILEIRA

Com o rápido avanço da tecnologia da informação houve a necessidade do alinhamento e da postura das políticas de segurança da informação com legislações específicas. A informação digital tornou-se um bem valioso e de efeito jurídico. Desta forma, a preservação da integridade, disponibilidade e autenticidade são de grande importância para a garantia dos serviços oferecidos pela tecnologia. Entretanto, o Brasil não poderia ser diferente de outros Estados quanto ao tratamento de informações digitais, tendo em vista que a tecnologia da informação está alinhada ao processo de desenvolvimento de um país. Assim, um conjunto de leis, decretos, cartilhas e guias sobre segurança da informação compõe um conjunto de regras e práticas adotadas até o momento no desenvolvimento de soluções públicas de tecnologia da informação.

3.4.1 LEIS, DECRETOS, NORMAS E MEDIDAS PROVISÓRIAS LIGADAS À SEGURANÇA DA INFORMAÇÃO

A Administração Pública Federal tem direcionado grande atenção para a segurança da informação e comunicações tendo em vista a importância de se proteger os dados confidenciais envolvidos nas transações eletrônicas. O reflexo desta preocupação está no crescente número de normas, diretrizes e leis acerca desse assunto.

Atualmente, de acordo com o Gabinete Institucional da Presidência da República, as principais legislações relacionadas à segurança da informação aplicadas a Administração Pública Federal são enumeradas, conforme a tabela 3.1:

Tabela 3.1: Leis, decretos e instruções normativas brasileiras. (GUALBERTO, 2010)

Lei, Decreto, Norma ou Medida Provisória	**Dispõe**
Lei 12.527 de 18 de novembro de 2011.	Regula o acesso a informações como o previsto no inciso XXXIII do art. 5o, no inciso II da Constituição Federal Brasileira.
Lei 9.983 de 14 de julho de 2000.	Acrescenta penas ao código penal brasileiro a indivíduos que violarem os sistemas de informação seja acrescentando informações falsas ou se apropriando de dados sigilosos para obter vantagens próprias ou de outrem.
Lei 7.232 de 29 de outubro de 1984.	Dispõe sobre a Política Nacional de Informática e dá outras providências.
Decreto 3.505 de 13 de julho de 2000.	Institui a política de segurança da Informação nos Órgãos e entidades da Administração Pública Federal.
Decreto nº 4.553 de 27 de dezembro de 2002.	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal e dá outras providências.
Instrução normativa nº1 do GSI de 13 de junho de 2008.	Disciplina a Gestão de segurança da Informação e comunicações na Administração pública Federal, direta e indireta.
Norma Complementar nº 002 – Metodologia de gestão de SIC.	Define a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal direta e indireta.
Norma Complementar nº 003 – Elaboração e manutenção da política de Segurança.	Define diretriz para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da administração pública federal.
Norma Complementar nº 004 – Gestão de Riscos.	Estabelece as diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal - APF, direta e indireta.
Instrução Normativa nº 04 de 19 de maio de 2008.	Dispõe sobre o processo de contratação de serviços

de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional.

Além das leis, normas e decretos citados acima há também um conjunto de recomendações distribuídas em cartilhas e guias criados de forma a tratar assuntos mais específicos ligados à segurança da informação. Dentre os mais conhecidos guias estão: Boas práticas de segurança da informação do Tribunal de Contas da União e o E-ping que define padrões de interoperabilidade de Governo Eletrônico. (BRASIL, 2013)

3.5 GUIAS DE BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Os guias de boas práticas de segurança da informação lançados pela Administração Pública Federal tem como objetivo propor recomendações na implantação e administração de sistemas em órgãos da Administração. Estes guias são publicados anualmente ou a cada dois anos dependendo da entidade governamental. Neles estão presentes recomendações com base em outras geralmente obtidas das Normas ISO e recomendações internacionais. Desta forma, dois guias de boas práticas de segurança da informação e interoperabilidade ganham destaque na Administração Pública: Boas práticas de segurança da informação do TCU – Tribunal de Contas da União e padrões de interoperabilidade de governo eletrônico conhecido como e-PING.

3.5.1 BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO – TCU

O guia de boas práticas de segurança da informação concebido pelo Tribunal de Contas da União já está em sua 4ª edição (2012) e fornece um conjunto de recomendações de políticas de segurança de informações. O principal objetivo deste guia é apresentar boas práticas de segurança da informação, a qualquer pessoa que interaja de alguma forma com ambientes informatizados, de profissionais de TI envolvidos com segurança de informações até auditores, usuários e dirigentes preocupados em proteger o patrimônio, os investimentos e os negócios da instituição, em especial, os agentes da Administração Pública Federal.

Assim, neste guia, são tratadas questões de alto nível ligadas a políticas de segurança de informações, controles de acesso lógico, plano de continuidade de negócio e os enquadramentos das políticas do TCU com a NBR ISO/IEC 27002:2005. Em particular, nesta 4º edição do guia (BRASIL, 2012) comentários dos processos da NBR ISO/IEC 27002:2005 onde são explanadas as seções da norma e citados acórdãos do tribunal que tratam, entre outros aspectos, de segurança da informação foram introduzidos no quarto capítulo.

Adiantando o que será exposto posteriormente, a NBR ISO/IEC 27002:2005 trata de técnicas de segurança em tecnologia da informação e funciona como um código de práticas para gestão de segurança da informação. Contudo, esta norma foi elaborada pelo Comitê Brasileiro de Computadores e Processamento de Dados e é equivalente à norma internacional ISO/IEC 27002:2005. Assim, tendo em vista o reconhecimento da ABNT e as instituições internacionais ISO e IEC o TCU utiliza essa norma como padrão em suas auditorias de segurança da informação.

3.5.2 PADRÕES DE INTEROPERABILIDADE DE GOVERNO ELETRÔNICO: E-PING

Os padrões de interoperabilidade de governo eletrônico do Brasil são reunidos sob o nome de e-PING. Estes padrões formam um conjunto de premissas, políticas e especificações técnicas que regulamentam a utilização da tecnologia da informação e comunicação (TIC) no governo federal brasileiro, estabelecendo as condições de interação com os demais poderes e esferas de governo com a sociedade em geral. Desta forma, o e-Ping busca estabelecer políticas e especificações técnicas de qualidade que permitam a prestação de serviços eletrônicos à sociedade brasileira.

Contudo, a adoção dos padrões e políticas contidos neste conjunto não pode ser imposta aos cidadãos e às diversas instâncias do governo brasileiro. Entretanto, o governo brasileiro, estabelece essas especificações como o padrão por ele selecionado e aceito, ou seja, as políticas técnicas com as quais deseja interoperar com as entidades fora do governo federal. Porém, neste contexto, entende-se como governo federal o Poder Executivo do Brasil. Assim, a adoção do e-PING por outras entidades fora do poder executivo se dá de forma voluntária. Já dentro do Poder Executivo brasileiro a adoção dos padrões e políticas da e-PING é obrigatório, de acordo com a portaria nº 5 de 14 de julho de 2005.

O governo federal – Poder Executivo brasileiro inclui:

- Órgãos da administração Direta;
- Autarquias e fundações;

No contexto do governo federal, de acordo com o guia de referência da e-PING(2013) são obrigatórias as especificações contidas para (BRASIL, 2013):

- "Novos sistemas de informação que vierem a ser desenvolvidos e implantados no governo federal e que se enquadram no escopo de interação, dentro do governo federal e com a sociedade em geral;" (BRASIL, 2013)

- "Sistemas de informação legados que sejam objeto de implementações que envolvam provimento de serviços de governo eletrônico ou interação entre sistemas;" (BRASIL, 2013)
- "Outros sistemas que façam parte dos objetivos de disponibilizar os serviços de governo eletrônico". (BRASIL, 2013)

Ainda, segundo o guia, a adesão ocorrerá de maneira gradativa, após a definição do Plano Diretor de Tecnologia da Informação – PDTI de cada órgão participante.

3.5.3 POLÍTICAS GERAIS

O e-PING tem como premissa recomendar padrões abertos para desenvolvimento e manutenção de sistemas dentro do governo federal. Os padrões proprietários são aceitos de forma transitória. Contudo, caso haja necessidade de consideração de requisitos de segurança e integridade, sistemas proprietários podem ser mantidos no governo, porém, mantendo-se as perspectivas de mudança quando houver condições de adotar o padrão livre.

Além dos padrões abertos, as políticas da e-PING englobam a utilização do software público e o software livre, em conformidade com as diretrizes do comitê executivo de governo eletrônico e normas definidas no âmbito do SISP.

No contexto de Web Service, o documento (BRASIL, 2013) trata no capítulo dez sobre as especificações técnicas para áreas de integração para governo eletrônico. O documento apresenta uma tabela com os componentes, especificações, observações e um campo de conformidade que diz respeito a adoção, recomendação ou estudo do componente. Seguem as tabelas 3.2 retirada do documento em questão:

Tabela 3.2: Especificações para Áreas de Integração para Governo Eletrônico – Web Services (e-PING, 2013).

Componente	**Especificação**	**SIT**	**Observações**
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Infraestrutura de registro	Especificação UDDI v3.0.2(Universal Description, Discovery and Integration) definida pela OASIS http://uddi.org/pubs/uddi_v3.htm	**R**	

	ebXML (Electronic Business using eXtensible Markup Language). A especificação pode ser encontrada em http://www.ebxml.org/specs/index.htm	**E**	
Linguagem de definição do serviço	WSDL 1.1 (Web Service Description Language) como definido pelo W3C. A especificação pode ser encontrada em http://www.w3.org/TR/wsdl	**A**	
	WSDL 2.0 (Web Service Description Language) como definido pelo W3C. A especificação pode ser encontrada em http://www.w3.org/TR/wsdl20/	**E**	
Protocolo para acesso a Web Service	SOAP v1.2, como definido pelo W3C http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/ Especificações do protocolo SOAP podem ser encontradas em http://www.w3.org/TR/soap12-part0/	**A**	
	HTTP/1.1 (RFC 2616)	**A**	Utilizado para desenvolvimento de projetos baseados em REST, conforme item 10.1.5
Perfil básico de interoperabilidade	Basic Profile 1.1 Second Edition, como definido pela WS-I http://www.ws-i.org/Profiles/BasicProfile-1.1.html	**E**	A versão 1.2 do Basic Profile encontra-se como rascunho (Working Draft) em http://www.wsi.org/Profiles/BasicProfile-1.2.html
Portlets remotos	WSRP 1.0 (Web Services for Remote Portlets) como definido pela OASIS http://www.oasis-	**E**	

	open.org/committees/wsrp	
Descoberta de Web Services Governamentais	Descoberta de Web Services Governamentais	**E**

3.6 ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO - ISO

Fundada em 1947, a Organização Internacional para Padronização - ISO é uma entidade que reúne e consolida diversos itens que se referem à padronização e normalização. O principal objetivo da organização é aprovar normas internacionais no campo referente a normas técnicas, classificações, normas de procedimentos entre outras questões pertinentes a padrões de utilização técnica. Atualmente, os padrões são adotados por mais de 170 países, incluindo o Brasil, onde é conhecido como ABNT – Associação Brasileira de Normas Técnicas.

Dentre as recomendações técnicas propostas pela ISO podem-se destacar as normas da família 27000. Estas tratam de aspectos de gestão de segurança da informação destacando-se os requisitos para gestão de segurança da informação e o código de prática para a gestão de segurança da informação.

3.6.1 NORMA ABNT ISO/IEC 27001:2006

A norma 27001 foi preparada com o objetivo de prover um modelo para estabelecer, implementar, operar, monitorar, analisar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) dentro de uma determinada organização que necessite ou queira implementá-la. Desta forma, adotar um modelo de SGSI deve ser uma decisão estratégica para uma organização. Assim, a especificação e a implementação do SGSI são determinadas pelas necessidades e objetivos, requisitos de segurança, processos adotados, tamanho e estrutura do ambiente.

3.6.1.1 ABORDAGEM DE PROCESSO

A Norma ABNT ISO/IEC 27001:2006 promove a adoção de uma abordagem de processo de forma a estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI de uma organização específica.

Desta forma, uma entidade precisa reconhecer e gerenciar diversas atividades para funcionar efetivamente. Qualquer ação que se utiliza de recursos e os gerencia para habilitar a transformação de entradas em saídas pode ser considerada um processo. Entretanto, a saída de um processo forma diretamente a entrada do processo seguinte.

Pode ser considerada como abordagem de processo a aplicação de vários processos dentro de uma organização em conjunto com a identificação e interações desses processos aliado a sua gestão podem ser consideradas como "abordagem de processo" (ABNT,2001). Esta abordagem, segundo a norma, promove a importância dos seguintes aspectos:

a) Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;

b) Implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;

c) Monitoramento e análise crítica do desempenho e eficácia do SGSI; e

d) Melhoria contínua baseada em medições objetivas.

De forma a estruturar todos os processos do SGSI, a Norma utiliza o modelo PDCA - Plan-Do-Check-Act. Desta forma, este modelo evidencia como um SGSI considera as entradas de requisitos de segurança da informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento as expectativas. A figura 3.1 ilustra como o modelo é utilizado:

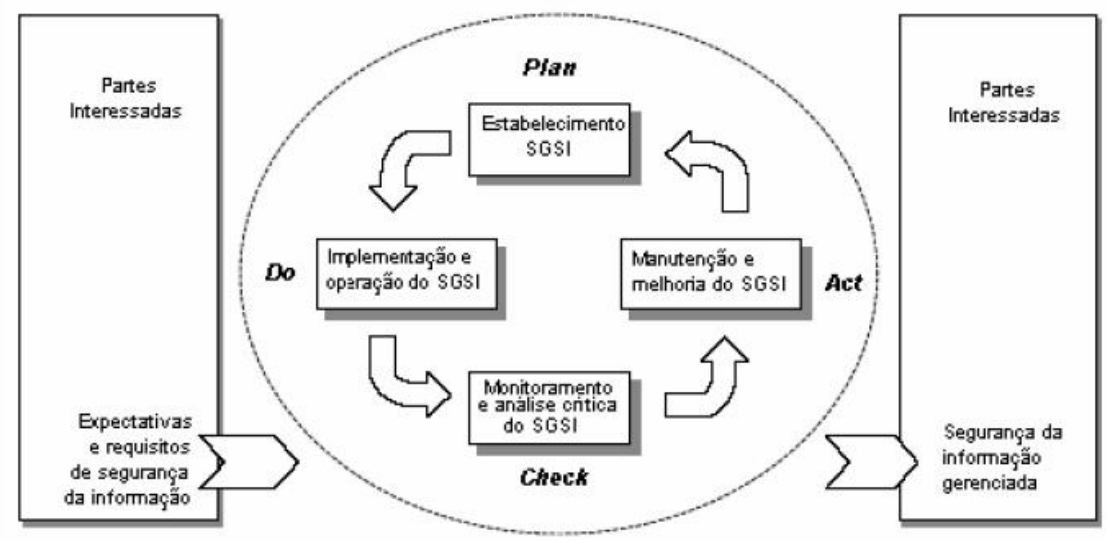

Figura 3.1. Modelo PDCA aplicado aos processos do SGSI. (ABNT NBR 27001, 2006).

O objetivo de cada etapa do modelo PDCA, conforme a tabela 3.3, obtida da Norma 27001:2006: são os seguintes:

Tabela 3.3: Etapas do modelo PDCA (ABNT, 2006).

Plan(planejar) (estabelecer o SGSI)	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do(fazer) (implementar e operar o SGSI)	Implementar e operar a política, controles, processos e procedimentos do SGSI.
Check(checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
Act(agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Vale ressaltar que esta Norma pode ser utilizada por todos os tipos de organizações. O seu principal objetivo é especificar os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos globais de negócio de uma organização.

3.6.1.2 CONTROLES APLICÁVEIS A WEB SERVICES

No contexto de utilização da Norma, a segurança em Web Services encontra-se distribuída em diversos objetivos de controle e controles abordados pelo documento. Estes processos foram obtidos através do Anexo A do documento da ABNT e são organizados e, neste caso, divididos conforme os aspectos de confidencialidade, disponibilidade e integridade. Em cada abordagem estão descritas em tabelas os objetivos de controle obtidos do documento.

No aspecto de confidencialidade, propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados [ISO/IEC 13335-1:2004], estão presentes os seguintes objetivos de controle descritos nas tabelas 3.4 e 3.5:

Tabela 3.4: Objetivos de controle A.6 da norma 27001(ABNT, 2006).

6. Organizando a segurança da informação
A.6.1 Infra-estrutura da segurança da informação
Objetivo: Gerenciar a segurança da informação dentro da organização.
A.6.1.5 Acordos de confidencialidade
Controle: Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados e analisados criticamente, de forma regular.

Tabela 3.5: Objetivos de controle A.12 da norma 27001 (ABNT, 2006).

A.12 Aquisição, desenvolvimento e manutenção de sistemas de informação
A.12.3 Controles criptográficos
Objetivo: Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.
A.12.3.1 Política para o uso de controles criptográficos
Controle: Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.
A.12.3.2 Gerenciamento de chaves
Controle: Um processo de gerenciamento de chaves deve ser implantado para apoiar o uso de técnicas criptográficas pela organização.

No contexto de disponibilidade, propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada [ISO/IEC 13335-1:2004], estão presentes os seguintes objetivos de controle descritos nas tabelas 3.6 e 3.7:

Tabela 3.6: Objetivos de controle A.10 da norma 27001(ABNT, 2006).

A.10 Gerenciamento das operações e comunicações
A.10.5 Cópias de segurança

Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.
A.10.5.1 Cópias de segurança das informações
Controle: Cópias de segurança das informações e dos softwares devem ser efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança definida.

Tabela 3.7: Objetivos de controle A.14 da norma 27001(ABNT, 2006).

A.14 Gestão da continuidade do negócio
A.14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação
Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.
A.14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação
Controle: Os planos devem ser desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.

A integridade, propriedade de salvaguarda da exatidão e completeza de ativos, estão presentes nos seguintes objetivos de controle descritos nas tabelas 3.8 e 3.9:

Tabela 3.8: Objetivos de controle A.10 da norma 27001(ABNT, 2006).

A.10 Gerenciamento das operações e comunicações
A.10.4 Proteção contra códigos maliciosos e códigos móveis
Objetivo: Proteger a integridade do software da informação.
A.10.4.1 Controle contra códigos maliciosos
Controle: Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.
A.10.4.2 Controles contra códigos móveis
Controle: Onde o uso de códigos móveis é autorizado, a configuração deve garantir que o código móvel autorizado opere de acordo com uma política de segurança da informação claramente definida e que códigos móveis não autorizados tenham sua execução impedida.
A.10.9 Serviços de comércio eletrônico
Objetivo: Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.
A.10.9.3 Informações publicamente disponíveis
Controle: A integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida, para prevenir modificações não autorizadas.

Tabela 3.9: Objetivos de controle A.12 da norma 27001(ABNT, 2006).

A.12 Aquisição, desenvolvimento e manutenção de sistemas de informação
A.12.1 Requisitos de segurança de sistemas de informação

Objetivo: Garantir que segurança é parte integrante de sistemas de informação.

A.12.2 Processamento correto de aplicações

Objetivo: Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.

A.12.2.1 Validação dos dados de entrada

Controle: Os dados de entrada de aplicações devem ser validados para garantir que são corretos e apropriados.

A.12.2.2 Controle do processamento interno

Controle: Devem ser incorporadas, nas aplicações, checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas.

A.12.2.3 Integridade de mensagens

Controle: Requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações devem ser identificados e os controles apropriados devem ser identificados e implementados.

A.12.2.4 Validação de dados de saída

Controle: Os dados de saída das aplicações devem ser validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.

A.12.3 Controles criptográficos

Objetivo: Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.

A.12.3.1 Política para o uso de controles criptográficos

Controle: Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.

A.12.3.2 Gerenciamento de chaves

Controle: Um processo de gerenciamento de chaves deve ser implantado para apoiar o uso de técnicas criptográficas pela organização

3.6.2 NORMA ABNT ISO/IEC 27002:2005

Esta norma tem por objetivo estabelecer diretrizes e princípios gerais para iniciar, manter e melhorar a gestão de segurança da informação em uma determinada organização (ABNT NBR, 2005). Assim, diretrizes gerais sobre as atividades aceitas para a gestão de segurança da informação são descritas nesta Norma.

Para atender os requisitos identificados por meio de análise ou avaliação de risco, objetivos de controle e os controles propostos nesta Norma são estabelecidos de forma a suprir essas necessidades. Sendo assim, esta Norma pode servir como um guia prático para estabelecer e gerir processos de segurança da informação de uma determinada organização, também sendo utilizada como parâmetro de aceitação e confiança em atividades interorganizacionais.

3.6.2.1 ESTRUTURA DA NORMA 27002

A norma ISO/IEC 27002 (ABNT, 2005) possui 39 categorias principais de segurança. Além destas categorias existe uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos. Assim, a Norma possui 11 seções das quais categorias de controle de segurança da informação estão distribuídas. Sendo assim, as principais seções descritas no documento são:

1) política de segurança da informação;
2) organizando a segurança da informação;
3) gestão de ativos;
4) segurança em recursos humanos;
5) segurança física e do ambiente;
6) gestão das operações e comunicações;
7) controle de acesso;
8) aquisição, desenvolvimento e manutenção de sistemas de informação;
9) gestão de incidentes de segurança da informação;
10) gestão de continuidade do Negócio;
11) conformidade;

Ainda, segundo a Norma, cada categoria principal de segurança contém um objetivo de controle que define o que deve ser alcançado e um ou mais controles que podem ser aplicados para alcançar o objetivo do controle.

3.6.2.2 UTILIZAÇÃO DA 27002:2005 EM WEB SERVICES

Presente na Norma, a segurança em Web Services encontra-se distribuída em diversos objetivos de controle e controles abordados pelo documento. Estes processos foram obtidos através da análise das 11 seções presentes no documento da ABNT e estão descritos nas tabelas abaixo conforme os aspectos de confidencialidade, disponibilidade e integridade. Em cada seção analisada estão descritos em tabelas os objetivos de controle obtidos do documento.

No contexto de confidencialidade, propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados (ABNT, 2005), estão presentes os seguintes objetivos de controle descritos nas tabelas 3.10, 3.11 e 3.12:

Tabela 3.10: Objetivos de controle 10.8.4 da norma 27002 (ABNT, 2005).

10.8 Troca de informações
10.8.4 Mensagens eletrônicas
Controle:
Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.
Diretrizes para implementação:
Convém que as considerações de segurança da informação sobre as mensagens eletrônicas incluam o seguinte:
a) proteção das mensagens contra acesso não autorizado, modificação ou negação de serviço;
b) assegurar que o endereçamento e o transporte da mensagem estejam corretos;
c) confiabilidade e disponibilidade geral do serviço;
d) aspectos legais, como, por exemplo, requisitos de assinaturas eletrônicas;
e) aprovação prévia para o uso de serviços públicos externos, tais como sistemas de mensagens instantâneas e compartilhamento de arquivos;
f) níveis mais altos de autenticação para controlar o acesso a partir de redes públicas.

Tabela 3.11: Objetivos de controle 10.9.1 da norma 27002 (ABNT, 2005).

10.9 Serviços de comércio eletrônico
10.9.1 comercio eletrônico
Controle:
Convém que as informações envolvidas em comércio eletrônico transitando sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.
Diretrizes para implementação:
Convém que as considerações de segurança da informação para comércio eletrônico incluam os seguintes itens:
a) nível de confiança que cada parte requer na suposta identidade de outros, como, por exemplo, por meio de mecanismos de autenticação;
b) processos de autorização com quem pode determinar preços, emitir ou assinar documentos-chave de negociação;
c) garantia de que parceiros comerciais estão completamente informados de suas autorizações;
d) determinar e atender requisitos de confidencialidade, integridade, evidências de emissão e recebimento de documentos-chave, e a não repudio de contratos, como, por exemplo, os associados aos processos de licitações e contratações;
e) nível de confiança requerido na integridade das listas de preços anunciadas;
f) a confidencialidade de quaisquer dados ou informações sensíveis;
g) a confidencialidade e integridade de quaisquer transações de pedidos, informações de pagamento, detalhes de endereço de entrega e confirmações de recebimentos;
h) grau de investigação apropriado para a verificação de informações de pagamento fornecidas por um cliente;
i) seleção das formas mais apropriadas de pagamento para proteção contra fraudes;
j) nível de proteção requerida para manter a confidencialidade e integridade das informações de pedidos;

k) prevenção contra perda ou duplicação de informação de transação; l) responsabilidades associados com quaisquer transações fraudulentas;

Tabela 3.12: Objetivos de controle 12.3.1 da norma 27002. (ABNT, 2005)

12.3 Controles criptográficos Objetivo: Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos. Convém que uma política seja desenvolvida para o uso de controles criptográficos. Convém que o gerenciamento de chaves seja implementado para apoiar o uso de técnicas criptográficas. 12.3.1 Política para o uso de controles criptográficos Controle: Convém que seja desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação. Diretrizes para implementação: Convém que, quando do desenvolvimento de uma política para criptografia, sejam considerados: a) a abordagem gerencial quanto ao uso de controles criptográficos em toda a organização, incluindo os princípios gerais sob os quais as informações de negócio sejam protegidas; b) a identificação do nível requerido de proteção com base em uma análise/avaliação de riscos, levando em consideração o tipo, a força e a qualidade do algoritmo de criptografia requerido; c) o uso de criptografia para a proteção de informações sensíveis transportadas em celulares e PDA, mídias removíveis ou móveis, dispositivos ou linhas de comunicação; d) a abordagem do gerenciamento de chaves, incluindo métodos para lidar com a proteção das chaves criptográficas e a recuperação de informações cifradas, no caso de chaves perdidas, comprometidas ou danificadas; e) papéis e responsabilidades, por exemplo, de quem for responsável: 1) pela implementação da política; 2) pelo gerenciamento de chaves, incluindo sua geração (ver 12.3.2); f) os padrões a serem adotados para a efetiva implementação ao longo de toda a organização (qual solução é usada para quais processos de negócios); g) o impacto do uso de informações cifradas em controles que dependem da inspeção de conteúdos (por exemplo, detecção de vírus).

Convém ainda que sejam consideradas, na implementação da política de criptografia da organização, as leis ou regulamentações e restrições nacionais aplicáveis ao uso de técnicas criptográficas, nas diferentes partes do mundo, e das questões relativas ao fluxo transfronteiras de informações cifradas.

Controles criptográficos podem ser usados para alcançar diversos objetivos de segurança, como, por exemplo:

a) Confidencialidade: usando a criptografia da informação para proteger informações sensíveis ou críticas, armazenadas ou transmitidas;

b) Integridade/autenticidade: usando assinaturas digitais ou códigos de autenticação de mensagens (MAC) para proteger a autenticidade e integridade de informações sensíveis ou críticas, armazenadas ou transmitidas;

c) Não-repúdio: usando técnicas de criptografia para obter prova da ocorrência ou não ocorrência de um evento ou ação.

Além disso, a Norma traz informações adicionais conforme descrito abaixo:

"Convém que a tomada de decisão para verificar se uma solução de criptografia é apropriada seja vista como parte de um processo de análise/avaliação de riscos e seleção de controles mais amplos. Essa avaliação pode, então, ser usada para determinar se um controle criptográfico é apropriado, que tipo de controle seja usado e para que propósito e processos de negócios." (ABNT NBR, 2005)

A integridade, propriedade de salvaguarda da exatidão e completeza de ativos, estão presentes os seguintes objetivos de controle descritos na tabela 3.13:

Tabela 3.13: Objetivos de controle 12.2.3 da norma 27002. (ABNT, 2005)

12 Aquisição, desenvolvimento e manutenção de sistemas de informação
12.2 Processamento correto nas aplicações
12.2.3 Integridade de mensagens
Controle:
Convém que requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações sejam identificados e os controles apropriados sejam identificados e implementados.
Diretrizes para implementação:
Convém que seja efetuada uma análise/avaliação dos riscos de segurança para determinar se a integridade das mensagens é requerida e para identificar o método mais apropriado de implementação.
Informações adicionais:
As técnicas criptográficas podem ser usadas como um meio apropriado para a implementação da autenticação de mensagens.

Tendo em vista os aspectos da Administração Pública Federal brasileira analisados neste capítulo, verificamos que existem diversos órgãos responsáveis por criar, manter e regular aspectos de segurança da informação dos dados e aplicações utilizadas por entidades governamentais. Contudo, não existem recomendações específicas de alto nível ligadas ao desenvolvimento de Web Services seguros. Na cartilha do e-PING 2013, por exemplo, encontramos recomendações genéricas relativas a implementação destas aplicações. Nas normas análisadas, foram encontrados apenas controles e considerações relativas a segurança, aquisições e requisitos que devem ser adotados em determinadas situações. Assim, considerando vital a o desenvolvimento seguro de Web Services, procuramos em outras

entidades governamentais recomendações e padrões utilizados na implementação destes seviços. Desta forma, no próximo capítulo, foram análisados três documentos de órgãos internacionais com foco em web service e ciclo de vida de desenvolvimento seguro de aplicações.

4 ANÁLISE DE DOCUMENTOS DE REFERÊNCIA

Este capítulo apresenta três documentos utilizados para a construção de Web Services seguros. O primeiro, o documento do OASIS, descreve as fases para a construção de um Web Service. O segundo, O SDL, é um documento construído pela Microsoft e define um processo de garantia de segurança no desenvolvimento de software. O último documento, proposto pelo NIST, define um ciclo de vida seguro para o desenvolvimento de sistemas.

4.1 METODOLOGIA DE IMPLEMENTAÇÃO DE WEB SERVICES OASIS

A organização OASIS elabora padrões abertos ao público que ajuda no estabelecimento de regras para as indústrias nas áreas de SOA, *Cloud Computing, Smart Grids*, Web Services, segurança da informação, dentre outras. O trabalho dessa organização ajuda a reduzir os custos pesquisa, estimula o mercado e possibilita uma melhor possibilidade de escolha de tecnologias e conta com milhares de participantes de centenas de organizações e membros.

"OASIS (Organização para o Avanço de Padrões de Informação Estruturada) é um consórcio sem fins lucrativos que impulsiona o desenvolvimento, convergência e adoção de padrões abertos para a sociedade da informação global." (OASIS,2005)

A organização OASIS possui um documento *OASIS Web Service implementation methodology* (OASIS,2005) que orienta os desenvolvedores e analistas de sistemas, a implementar aplicações que utilizem Web Services. Este documento apresenta uma metodologia de desenvolvimento que utiliza outros modelos ágeis existentes, de desenvolvimento de software, como o RUP e o *Extreming programing*, mas não recomenda a utilização de um modelo específico, apenas adapta esses modelos considerando as principais características e pontos importantes de uma aplicação Web Services. Como por exemplo, a reutilização, a granularidade, a interoperabilidade, dentre outros.

Trata-se de um modelo de alto nível, entretanto, eventualmente aborda em alguns detalhes técnicos. Apesar de ser um guia muito prático de desenvolvimento de Web Services, a sua orientação quanto a segurança no procedimento de elaboração e dentro de sua estrutura

é pouco explorada. A única recomendação do guia, se dá na fase de teste, onde existe uma tarefa de testes de segurança.

A metodologia (OASIS,2005) consiste em fases de elaboração do sistema, que formam o ciclo de vida de implementação. As fases podem ser incrementais e iterativas o suficiente para não comprometer a agilidade do processo, onde cada fase possui a sua subseção. As fases consistem em levantamentos de requisitos, análise, desenho, codificação, teste e liberação representadas pela figura 4.1:

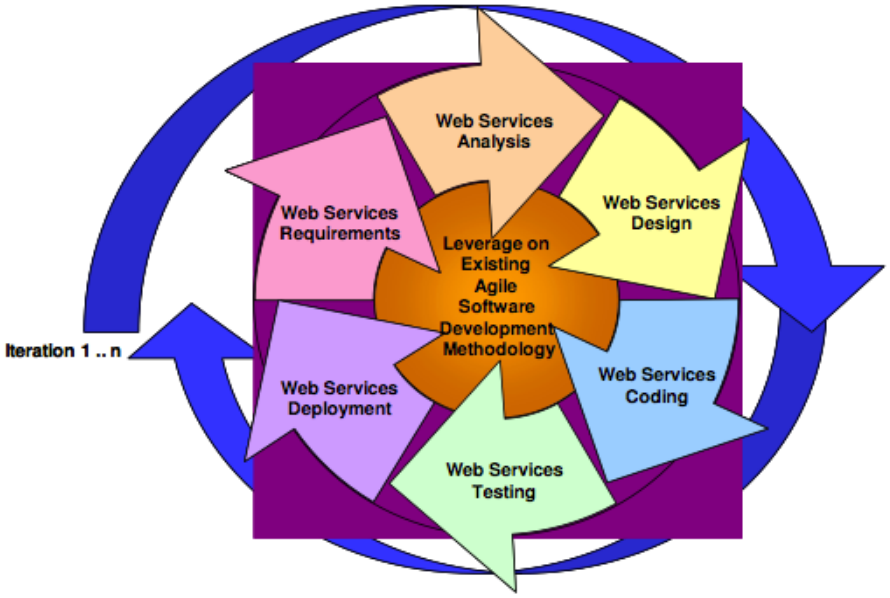

Figura 4.1. Fases do modelo de implementação da OASIS. (OASIS, 2005)

Dentro de cada fase, existem diversas atividades, que por sua vez contém artefatos, papéis e tarefas. Os papéis são os responsáveis, ou os especialistas, que devem estar envolvidos na atividade. Os artefatos são as entregas de cada atividade, podendo ser um documento, especificações, parte da implementação, dentre outros. As tarefas são procedimentos para cada atividade, que definem mais detalhadamente os procedimentos. A figura 4.2 ilustra o relacionamento das fases, atividades, papéis, tarefas e artefatos.

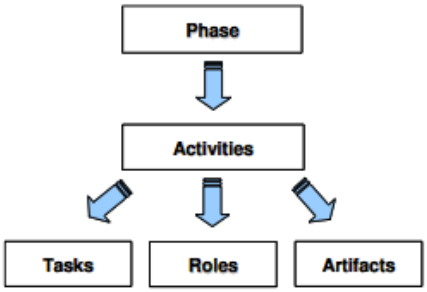

Figura 4.2. Relação dos componentes do modelo OASIS. (OASIS, 2005)

A fase de Requisitos consiste no levantamento das necessidades do negócio para transformá-lo em serviços a serem providos por Web Services, além dos requisitos funcionais e não-funcionais. Trata-se de uma fase em alto nível que deve ser realizada por diversos integrantes, como os usuários, os patrocinadores, os *stakeholders*, o analista de requisitos dentre outros. Segue a tabela 4.1 que descreve as atividades, tarefas, papéis e artefatos.

Tabela 4.1: Atividades, tarefas, papéis e artefatos da fase de requisitos. (OASIS, 2005)

Atividades	Tarefas	Papéis	Artefatos
Determinar a necessidade para o WS	Identificar *stakeholders* Identificar as necessidades dos *stakeholders* Identificar as necessidades da tecnologia de WS Determinar o posicionamento do WS de acordo com os problemas identificados Definir as características do WS baseadas nas necessidades Identificar limitações	Arquiteto Analista de requisitos *Stakeholders* Gestor do projeto	Especificações dos requisitos de negócio
Extrair Requisitos	Identificar as fontes de coleta de requisitos Recolher informações Identificar requisitos funcionais Identificar requisitos não-funcionais	Arquiteto Analista de requisitos Gestor de testes	Especificações dos requisitos
Gerenciar os requisitos do WS	Identificar WS e estabelecer dependências e prioridades Criar matrizes de rastreabilidade Administrar mudanças de requisitos	Arquiteto Analista de requisitos Gestor de testes	Especificações dos requisitos
Cenários de modelos de uso	Transformar requisitos funcionais em modelos conceituais de uso Especificar os cenários de integração com os clientes do WS	Arquiteto Analista de requisitos Gestor de testes	Especificações dos requisitos
Preparar casos de teste para Teste de Aceitação do Usuário (UAT) e Teste do Sistema	Criar os cenários de negócio para os casos de teste Construir a matriz de validação de requisitos Administrar mudanças nos casos de teste	Analista de requisitos Gestor de testes Planejador de testes	Plano de teste – UAT e Teste do Sistema

- Determinar a necessidade para o WS

Esta atividade, iguala-se a uma fase de início de projeto, onde serão abordadas as necessidades de negócio, que deverão ser transformadas em serviços baseados em Web Services. Primeiramente, identificam-se os clientes, gerentes de projetos, patrocinadores, diretores das áreas afins, para descobrir se o que o cliente procura pode ser fornecido por um Web Service. Caso possa as primeiras características e limitações quanto ao projeto do Web Services devem ser definidas.

- Extrair Requisitos

A extração de requisitos funcionais, como a consulta de banco de dados, e não-funcionais como a usabilidade e a escalabilidade, deve ser realizada por meio de coletas de informações de uma ou mais fontes selecionadas, como um departamento ou um usuário.

- Gerenciar os requisitos de WS

Durante e após a extração de requisitos, deve ser realizado um monitoramento para priorizar os requisitos mais importantes, com base nas dependências mais críticas do negócio. Durante o ciclo de vida de um projeto de desenvolvimento de software, é comum ocorrerem mudanças de opinião e necessidades, por isso uma matriz de rastreabilidade deve ser criada para retirar ou adicionar requisitos do projeto.

- Cenários de modelos de uso

Nesta atividade, deve-se modelar os requisitos funcionais, por meio de técnicas como os diagramas de caso de uso, ou atividade, para que seja possível traduzir o que o cliente está requisitando com o que o analista está pensando. Importante ressaltar os cenários mais importantes, como no caso de Web Services, a troca de informações por exemplo.

- Preparar casos de teste para Teste de Aceitação do Usuário (UAT) e Teste do Sistema

Preparar os testes de aceitação do usuário e de sistema, de acordo com os requisitos, para que seja possível verificá-los durante a implementação. Paralelamente, criar uma matriz de validação de requisitos para monitorar as mudanças.

Na fase de análise, os requisitos são transformados em modelos conceituais para que possam ser entendidos pela equipe técnica de desenvolvedores. Consiste também no refinamento dos requisitos e um planejamento de uma estrutura básica e interfaces do sistema. Segue a tabela 4.2 que descreve as atividades, tarefas, papéis e artefatos.

Tabela 4.2: Atividades, tarefas, papéis e artefatos da fase de análise. (OASIS, 2005)

Atividades	Tarefas	Papéis	Artefatos
Selecionar uma plataforma de tecnologia para a arquitetura de implementação	Especificar os padrões de implementação Decidir a plataforma tecnológica para a implementação Decidir a plataforma tecnológica para a implantação Decidir a IDE (*Integrated Development Environment*) de ferramentas usadas no desenvolvimento	Arquiteto	Especificação da arquitetura do software
Definir uma sugestão de arquitetura	Definir arquitetura de alto nível Identificar os componentes arquiteturais que expõem as funcionalidades de WS Especificar as trocas de informações mais relevantes do WS com os clientes	Arquiteto	Especificação da arquitetura do software
Decidir granularidade do WS	Decidir critérios de granularidade das operações do WS Identificar e agrupar funcionalidades Escolher os mecanismos que compõem ou agreguem funcionalidades	Arquiteto	Especificação da arquitetura do software
Identificar Web Services reutilizáveis	Identificar componentes arquiteturais que possam ser aproveitados por WS existente Identificar os provedores dos WS reutilizáveis Definir os principais cenários de reutilização	Arquiteto	Especificação da arquitetura do software
Identificar interface de serviço para novos Web Services	Identificar novas assinaturas e padrões de operações de WS Definir a gramática do XML para a troca de mensagem	Arquiteto Designer	Gramática XML Especificação das assinaturas para o WS
Preparar casos de teste para o Teste de Desempenho	Preparar casos de testes para o desempenho	Administrador dos testes de sistema Planejador de testes	Plano de teste - teste de performance

Preparar casos de teste para o Teste de Integração / interoperabilidade	Preparar casos de testes para a integração e interoperabilidade	Planejador de testes Testador	Plano de teste - teste de interoperabilidade e integração
Preparar casos de teste para o Teste Funcional	Preparar casos de testes funcionais	Planejador de testes Testador	Plano de teste - teste funcional
Preparar teste de ambiente	Preparar testes de ambiente	Administrador dos testes de sistema Planejador de testes	Plano de teste - teste de ambiente

- Selecionar uma plataforma de tecnologia para a arquitetura de implementação

Nesta atividade devemos identificar os padrões de Web Services com base nos requisitos e restrições de implementação. Considerando questões como a compatibilidade e versões dos padrões, a adoção de padrões comerciais, e a normas aprovadas pela organização ou governo. Além disso, escolher a plataforma tecnológica de implementação e implantação, a IDE, que pode ser gratuita ou paga, dependendo das ferramentas fornecidas.

- Definir uma sugestão de arquitetura

Nesta etapa, é possível modelar uma estrutura básica de como serão as trocas de mensagens e as principais outras funcionalidades. Os componentes básicos da arquitetura de alto nível, devem ser identificados e as definições de tipos de dados e formatos das trocas de informações devem ser especificados.

- Decidir granularidade do WS

Utilizar os requisitos e cenários para decidir os critérios da granularidade das operações e realizar agrupamentos de funcionalidades dentro do Web Service. Assim como, escolher mecanismos que agreguem ou componham funcionalidades do Web Service.

- Identificar Web Services reutilizáveis

Uma das grandes vantagens dos sistemas baseados em Web Services, é o fato de se poder aproveitar um serviço que já exista. Serviços genéricos podem ser reutilizados, bastando verificar se a plataforma do Web Service terceiro, ou interno mas já existente,

suporta a que foi escolhida para o desenvolvimento. Além disso, deve-se checar os provedores de reutilização de serviços e definir quais cenários e funções poderão reutilizar Web Services.

- Identificar interface de serviço para novos Web Services

Definir a gramática XML, que servirá de guia para manter a estrutura de um XML bem formado, para a troca de mensagens. Deve-se, também escolher as interfaces de operações do serviço.

- Preparar casos de testes

Como últimas atividades da fase, temos a preparação dos testes de performance, interoperabilidade, funcionais e de ambiente, que devem ser escritos e documentados para posterior utilização.

A fase de desenho trata-se da definição e construção do sistema Web Service e das interfaces, que devem possuir os detalhes da comunicação entre o cliente e o serviço, tipos de dados, protocolos e tecnologias. Deve constar também o modelo técnico da estrutura interna do serviço, assim como as considerações para se cumprir os requisitos. Segue a tabela 4.3 que descreve as atividades, tarefas, papéis e artefatos.

Tabela 4.3: Atividades, tarefas, papéis e artefatos da fase de desenho. (OASIS, 2005)

Atividades	Tarefas	Papéis	Artefatos
Transformar as assinaturas dos WS reusáveis	Realizar o mapeamento dos tipos de dados Identificar os padrões de design para o mapeamento das interfaces dos WS reutilizáveis	Designer	Especificações de design
Refinar a interface de serviços do novo WS	Refinar a assinatura de interface do WS Refinar a gramática XML para a troca de mensagem	Designer	Especificações de design
Desenhar WS	Usar técnicas de modelagem para descrever a estrutura interna do WS Considerar os requisitos não-funcionais e as restrições de design	Designer	Especificações de design
Refinar casos de teste para o Teste Funcional	Refinar os casos de teste funcionais	Planejador de teste Testador	Plano de teste – Teste funcional

- Transformar as assinaturas dos WS reusáveis

Realizar o mapeamento dos tipos de dados que não forem suportados pela plataforma, e por meio da identificação dos padrões do projeto mapear as interfaces do Web Service reutilizado. Caso não haja suporte direto, pode-se criar um adaptador que expõe uma interface do Web Service existente, ou encapsula-se a complexidade da saída, para um serviço de maior granularidade.

- Refinar a interface de serviços do novo WS

Esta atividade possui tarefas de refinamento das interfaces e da gramática XML, para melhor adequar ao projeto. Tomar cuidado, para que não impacte na interoperabilidade do serviço.

- Desenhar WS

O projeto da estrutura interna deve considerar o pré-processamento de pedido, a intermediação do pedido e o processamento do pedido, o destinatário e o envio e recebimento da resposta. Além dos requisitos não-funcionais e restrições, como a performance, escalabilidade, interoperabilidade, disponibilidade, dentre outros.

Técnicas de modelagem existentes, como UML - *Unified Modeling Language*, devem ser utilizadas para projetar a arquitetura.

- Refinar casos de teste para o Teste Funcional

Após a definição de uma arquitetura, refinar os testes funcionais, pois é comum acontecer mudanças ou adaptações de requisitos nessa fase.

A implementação propriamente dita ocorre na fase de codificação, onde os desenvolvedores realmente constroem a aplicação. Para Web Services o desenvolvedor deve separar a construção, onde primeiramente desenvolve o WSDL que deve ser o componente do servidor, as suas interfaces e os *stubs* do lado cliente. *Stubs* são conectores que o usurário deve utilizar para se comunicar com o usuário. Segue a tabela 4.4 que descreve as atividades, tarefas, papéis e artefatos.

Tabela 4.4: Atividades, tarefas, papéis e artefatos fase de implementação (OASIS, 2005)

Atividades	**Tarefas**	**Papéis**	**Artefatos**
Elaborar o código do WS	Código baseado na linguagem de implementação escolhida Expor APIs públicas como interfaces Criar WSDL para o cliente	Desenvolvedor	Códigos de implementação

Criar o código para o WS do usuário	Decidir o modelo de operação Criar códigos do usuário	Desenvolvedor	Códigos dos usuários
Teste de unidade	Criar o ambiente de testes Realizar os testes de unidade funcionais	Desenvolvedor	Scripts de testes de unidade

- Elaborar o código do WS

Nesta atividade inicia-se a codificação, onde o programador transforma o projeto em produto, de acordo com a linguagem escolhida previamente, levando em conta as restrições e dependências da mesma. Devido ao fato de um Web Service ter características de serviço publico, APIs - *Application Programming Interface* devem ser criadas para suprimir os detalhes de implementação e o WSDL deve ser gerado.

- Criar o código para o WS do usuário

Existem três principais maneiras do usuário utilizar um Web Service, primeiramente por meio de *stubs* estáticos, que são pequenos códigos que invocam as funcionalidades do serviço. A segunda maneira, se da por meio de proxy, que é gerado dinamicamente quando o cliente executa a aplicação, e por ultimo a chamada dinâmica de interface, que é a maneira mais flexível dentre as três. Procedendo a escolha, criar o WSDL que o cliente usará para chamar um método.

- Teste de unidade

Ao criar um código que realize uma funcionalidade, deve-se aplicar testes de ambiente e de funcionais, afim de verificar a exatidão e restrições dos serviços implementados.

Na fase de testes além de certificar a completeza dos requisitos e funcionamento, são realizados testes de interoperabilidade, segurança e performance, pois são elementos críticos da qualidade de serviço de um Web Service. Os testes em diferentes plataformas e com diversos usuários completam a fase de testes. Segue a tabela 4.5 que descreve as atividades, tarefas, papéis e artefatos.

Tabela 4.5: Atividades, tarefas, papéis e artefatos da fase de testes (OASIS, 2005)

Atividades	**Tarefas**	**Papéis**	**Artefatos**
Testes de funcionalidades	Teste das funcionalidades básicas do WS Teste de segurança Teste das funcionalidades do UDDI	Planejador de testes Testador	Códigos dos usuários Scripts dos testes Resultado dos testes

	Teste da capacidade intermediaria do SOAP		
Testes de integração	Teste de conformidade com o WS-I Realizar os testes de interoperabilidade baseados em cenários variados Realizar os testes de integração baseados em cenários variados	Planejador de testes Testador Administrador dos testes de sistema	Códigos dos usuários Scripts dos testes Resultado dos testes
Testes no sistema	Checar as funcionalidades do sistema e o tempo de resposta com cargas variadas Checar as funcionalidades do sistema e o tempo de resposta de diferentes combinações de requisições válidas ou inválidas	Planejador de testes Testador Administrador dos testes de sistema	Códigos dos usuários Scripts dos testes Resultado dos testes
Testes de aceitação do usuário	Realizar o Testes de aceitação do usuário	Administrador dos testes de sistema Usuário Gestor de testes	Códigos dos usuários Scripts dos testes Resultado dos testes

- Testes de funcionalidades

O Web Service deve responder corretamente às solicitações dos seus clientes, por meio mensagens SOAP que devem estar com o formato em conformidade com as especificações do OASIS. Os arquivos WSDL, que contêm os metadados sobre interfaces, devem estar de acordo com as especificações da W3C. Testes de entradas inesperadas devem ser realizados para verificar o comportamento do sistema.

Testes de níveis de privacidade e segurança da mensagem devem ser realizados para que os requisitos de segurança sejam verificados. Assim como o registro do Web Service no UDDI, deve ser apurada a sua funcionalidade, verificando se realmente os dados do registro estão chamando o serviço correto. Por fim, os intermediários das trocas de informação de uma mensagem SOAP devem ser validados, quanto ao seu funcionamento.

Os resultados dos testes devem ser registrados e os bugs encontrados devem ser reportados aos responsáveis pelos códigos.

- Testes de integração

A distribuição dos serviços prestados, requer uma padronização para que ocorram as trocas de informações e serviços. Os testes de interoperabilidade e integração devem ser realizados com base nos testes criados na fase de análise e estarem de acordo com as recomendações do WS-I, que se tornou parte da organização OASIS.

Os testes devem considerar diversos cenários de operação para conseguir cobrir o maior número de processos interoperáveis.

- Testes no sistema

Devido a alta variação nos picos de carga, é necessário realizar teste de tempo de resposta do sistema, afim de se determinar os possíveis gargalos e prever a escalabilidade do mesmo. Deve-se utilizar ainda, entradas e solicitações válidas e inválidas para averiguar o comportamento do sistema e a qualidade esperada dos serviços, com o que foi especificado nos requisitos não-funcionais.

A figura 4.3, demonstra como as fases, atividade e artefatos se relacionando com os testes que devem ser implementados, demostrando as dependências e influências das atividades.

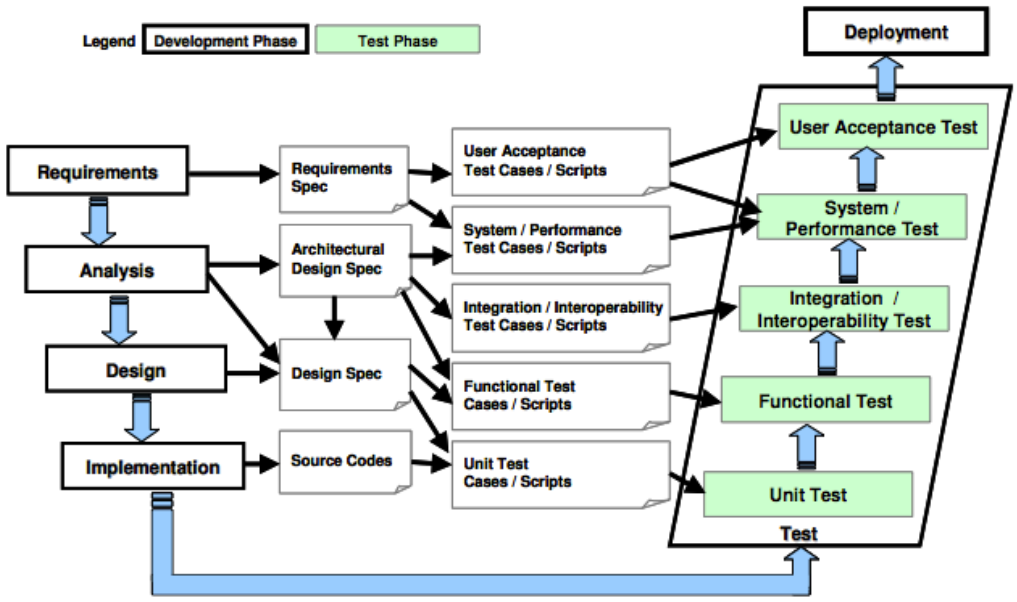

Figura 4.3. Relacionamento das fases, atividade, artefatos e testes. (OASIS, 2005)

- Testes de aceitação do usuário

Os casos de teste elaborados na fase de requisitos são usados nesta atividade para validar a exatidão e integridade do sistema Web Service. Principalmente, se o usuário está

satisfeito com o que foi desenvolvido e se está de acordo com o que foi requisitado pelo mesmo. Quaisquer incompatibilidades encontradas devem ser reportadas e corrigidas.

Por último, após todos os testes e certificação dos serviços, é realizada uma configuração final no ambiente de liberação. A liberação precede testes finais, e a divulgação do Web Service no UDDI e o registro adequado do mesmo. Segue a tabela 4.6 que descreve as atividades, tarefas, papéis e artefatos.

Tabela 4.6: Atividades, tarefas, papéis e artefatos da fase de implantação. (OASIS, 2005)

Atividades	Tarefas	Papéis	Artefatos
Preparar ambiente de implantação	Configurar e iniciar hardware Configurar e iniciar software Determinar a URL do serviço	Engenheiro de sistemas	Lançar notas
Implantar o WS	Preparar o Script de Implantação Implantar WS Criar WSDL	Desenvolvedor	Arquivo WSDL Script de Implantação
Testes de Implantação	Criar ou reusar o código de usuário Criar WS com o código de usuário	Testador	Códigos dos usuários
Criar material de suporte para os usuários finais	Criar o material de suporte	Desenvolvedor	Guia de interoperabilidade Guia do usuário Serviços On-line Tutoriais Material de treinamento
Publicar WS	Identificar o registro UDDI para a publicação Preparar a informação para a publicação Publicar no registro UDDI Realizar pesquisa com palavras-chave depois de realizar a publicação	Desenvolvedor	Nenhum

- Preparar ambiente de implantação

A preparação do ambiente inclui a instalação e configuração dos softwares, tais como o servidor de aplicações, o banco de dados, entre outros, que devem estar aptos a processarem mensagens SOAP. A configuração do hardware também deve ser realizada para a implantação.

- Implantar o WS

A implantação do Web Service deve preceder da identificação da URL que será utilizada para localizar o serviço, e a criação dos scripts de implantação que devem incluir as etapas de implantação dos diretórios, cópias de arquivos e a iniciação do servidor.

O script deve ser rodado e depois, um arquivo WSDL deve ser criado para descrever as funções fornecidas pelo Web Service. O WSDL pode ser criado manualmente ou pela maioria dos servidores, que o gerará automaticamente, após a implantação.

- Testes de Implantação

Neste teste é apenas verificado se o Web Service está devidamente implementado e configurado, ou a verificação de quaisquer outras características especiais do servidor de aplicativos.

- Criar matéria de suporte para os usuários finais

Guias de orientação e tutoriais para os usuários finais devem ser criados e armazenados para que os mesmos possam ter acesso aos materiais de treinamento e migração, históricos e todos os documentos criados no projeto devem ser arquivados para posterior utilização.

- Publicar WS

Os serviços devem ser descobertos por meio do UDDI, que fornece uma catalogação e organização de diversas aplicações. Deve-se decidir quanto a necessidade de se utilizar um UDDI privado ou público e quanto as suas versões, as palavras-chaves que serão utilizadas para a localizar o serviço, a URL do arquivo e outras informações que serão utilizadas pelo UDDI.

Após a publicação, deve ser realizada a pesquisa da publicação com diversos navegadores e ferramentas, pelas palavras-chave a fim de verificar se a localização esta sendo alcançada.

Apesar deste modelo (OASIS, 2005) apresentar atividades específicas para Web Services dando ênfase nessas pequenas diferenças em seu modelo de desenvolvimento, ele ainda carece de informações quanto aos procedimentos a serem tomados durante a implementação nos quesitos de segurança da informação. Este documento apenas tem como atividades de segurança, os testes, sendo eles pouco descritivos e detalhados. É necessário um modelo que torne mais seguro o desenvolvimento de uma aplicação baseada em Web Services e que contemple todas as fases do desenvolvimento.

4.2 CICLO DE VIDA DE DESENVOLVIMENTO SEGURO DA MICROSOFT - *MSDL*

A iniciativa *Microsoft-wide* começou em 2004 ao criar o SDL - *Security Development LifeCycle* - que se tornou um modelo que possibilitou integrar a segurança e privacidade aos produtos criados pela *Microsoft.* De maneira fácil e completa, o SDL inclui aspectos de segurança durante todo o processo de produção, ajudando a corporação a melhorar seus projetos.

O SDL é um processo de garantia de segurança nos desenvolvimentos de aplicações diversas, que pode ser aplicado a sistemas com características coorporativas ou governamentais. Os cumprimentos de segurança são baseados no SD3+C, que significam, *Secure by Design, Secure by Default, Secure in Deployment, and Communications*. Ao aplicar esses elementos dentro do ciclo de vida de desenvolvimento de software, o modelo possui as seguintes características. A figura 4.4 ilustra as fases e atividades do modelo SDL.

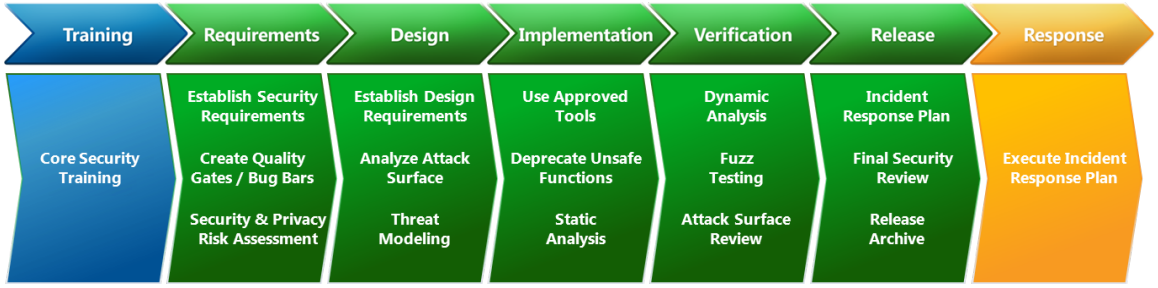

Figura 4.4. Atividades do modelo SDL. (*Microsoft*, 2012)

Assim como os modelos tradicionais de desenvolvimento de software o SDL possui fases bem marcadas para cada etapa da construção do sistema. Antes de iniciar a implementação o SDL recomenda o treinamento dos profissionais que estarão envolvidos com o projeto, incluindo o programador, o arquiteto, o analista, o gestor e o testador. Essa pré-fase é necessária para capacitar os profissionais, ou mantê-los atualizados. A recomendação é que todo ano cada profissional realize no mínimo o seguinte curso básico:

- Projeto de segurança inclui os seguintes tópicos: redução da superfície de ataque, defesa em profundidade e em camadas e o princípio do menor privilégio.
- Modelagem de ameaças inclui os seguintes tópicos: implicações do projeto de modelagem de ameaças e as restrições de codificação da modelagem.
- Codificação segura inclui os seguintes tópicos: estouro de *buffer,* erros de aritmética de inteiros, *cross-site scripting, SQL injection* e criptografia fraca.
- Testes de segurança incluem os seguintes tópicos: métodos de testes de segurança e funcionais e avaliação de riscos.

- Privacidade inclui os seguintes tópicos: tipos de dados sensíveis à privacidade, projetar, desenvolver e testar a privacidade de acordo com as melhores práticas.

Para os mais avançados, explorar temas atuais e mais específicos. De acordo com o documento a equipe deve ter no mínimo 80% dos profissionais com conhecimentos básicos adquiridos antes do final do projeto.

Tabela 4.7: Fase de treinamento do SDL. (*MICROSOFT*, 2012)

Treinamento	**Práticas do Treinamento**
Treinamento	Treinamento básico de segurança

Cada fase possui três práticas que somam 15 no total, com uma prática adicional de treinamento. A fase de requisitos possui a pratica de estabelecer requisitos de segurança de acordo com a necessidade da privacidade e confiabilidade, e um responsável especialista em segurança para a orientação do resto da equipe, além de definir um critério mínimo de segurança para a aplicação final. Outra prática desta fase é criação de *Quality gates e Bug Bars* que geram níveis mínimos de qualidade de segurança, performance e privacidade. Esses critérios ajudam a definir os riscos associados a segurança da informação e a resposta a falhas no desenvolvimento. A última prática desta fase trata da avaliação de riscos de segurança e dos riscos de privacidade, que definem os principais requisitos funcionais de segurança e privacidade relacionados ao projeto priorizando cada um deles.

Tabela 4.8: Fase requisitos do SDL. (*MICROSOFT*, 2012)

Requisitos	**Práticas de requisitos**
Estabelecer requisitos de segurança	Designar conselheiro de segurança
	Definir critérios mínimos de segurança
	Especificar ferramenta de rastreabilidade
Criar plano de qualidade	Criar critério/plano de qualidade
Realizar a avaliação do risco e privacidade	Realizar a análise e avaliação de risco e privacidade

A fase de Desenho estrutura o projeto com base nos requisitos e, assim, a primeira tarefa estabelece as necessidades de segurança no desenho do software, como as especificações de privacidade, criptografia, controle de acesso, autenticação, base de dados dentre outros. Nesta prática deve-se realizar ainda uma revisão das necessidades de segurança

e privacidade com o especialista encarregado e a verificação se os requisitos criptográficos estão de acordo.

A segunda prática desta fase é a realização da análise da superfície de ataques, com o objetivo de reduzir as vulnerabilidades de intrusão, como o controle de acesso de código fonte e das exceções do firewall, assim como conseguir manter o ambiente seguro para usuários comuns. A última prática dessa fase diz respeito ao tratamento de ameaças que deve considerar todo o processo de desenvolvimento, os códigos, características, funcionalidades e atualizações. Criar um documento com o tratamento de ameaças e submetê-lo a aprovação de testadores, desenvolvedores e gestores. Este documento deve ser armazenado e ter o seu acesso controlado.

Tabela 4.9: Fase de desenho do SDL. (*MICROSOFT*, 2012)

Design	**Práticas do Design**
Estabelecer os requisitos de segurança para o desenho	Revisão do projeto da segurança
	Revisão do projeto da privacidade
	Satisfazer requisitos mínimos de criptografia para desenho
Analisar a superfície de ataque	Análise da superfície de ataque
Realizar a modelagem de ameaças	Completar a modelagem/tratamento de ameaças

Após a definição de como que o sistema será desenvolvido, chega-se ao momento de construí-lo. Nessa fase também são necessárias práticas de segurança, como a utilização de ferramentas e compiladores que sejam aprovados pelo consultor de segurança da equipe e que estejam atualizadas, de forma que possuam proteções novas e atuais. Os desenvolvedores devem sempre utilizar funções que sejam seguras, e devem criar um rol de funções banidas, para que a equipe de desenvolvedores esteja sempre atualizada. For fim a última prática desta fase é a realização periódica da análise estática do código, por meio de ferramentas apropriadas.

Tabela 4.10: Fase de Implementação do SDL. (*MICROSOFT*, 2012)

Implementação	**Práticas de Implementação**
Especificar tecnologia	Especificar/Aprovar compiladores e ferramentas seguras
Utilizar funções seguras	Identificar funções inseguras
Análise estática	Realizar análise estática de código periodicamente

Ao terminar o desenvolvimento e ter uma versão do produto, os testadores vão validar o sistema por meio de análises dinâmicas de código, para verificar se está realmente funcionando conforme o esperado, se está com os requisitos críticos de segurança de acordo com o planejado e monitorando o comportamento das máquinas, rede e usuários durante a execução do software. Outra prática é o teste onde se força o erro do sistema, tentando inserir dados errados, ou não-formatados, realizando operações inusitadas e improváveis, tentando gerar uma situação inesperada do sistema. Por final, a última prática destina-se a revisão das vulnerabilidades, dos pontos de entradas de intrusos, devido ao comum desvio na implementação do que foi realmente planejado, ou seja, mudanças ocorrem, mas devem ser cuidadosamente analisadas, para que as mesmas não criem brechas no sistema.

Tabela 4.11: Fase de verificação do SDL. (*MICROSOFT*, 2012)

Verificação	**Práticas de Verificação**
Análise dinâmica	Realizar a análise dinâmica de código
Fuzz test	Realizar teste de erro forçado
Revisão da superfície de ataque	Conduzir a revisão da superfície de ataque

Antes de realizar a liberação do software, a fase de lançamento realiza as últimas revisões e se preocupa com a continuidade e manutenção do produto. A primeira prática é criar um plano de resposta a incidentes, que deve conter equipes de pronta resposta, primeiros contatos e ações, responsáveis disponíveis 24 horas, *backups*, dentre outros. A realização de uma última revisão dos aspectos da segurança da informação, que analisa as exceções, o modelo de tratamento de ameaças, não realiza nenhuma introdução de requisitos de segurança que não constem nos documentos iniciais. Por final, a última tarefa é o armazenamento de todos os documentos, modelos, especificações, códigos, planos e licenças utilizadas na produção do sistema, para que serviços que posterguem o lançamento dos produtos como manutenção, atualização, apoio técnico, dentre outros.

Tabela 4.12: Fase de lançamento do SDL. (*MICROSOFT*, 2012)

Lançamento	**Práticas de lançamento**
Plano de resposta a incidentes	Criar o plano de resposta a incidentes
Revisão final	Realizar a revisão final da segurança
Arquivar documentos	Arquivar todos os documentos produzidos

Este documento também descreve um modelo de desenvolvimento para os modelos ágeis como o XP e o Scrum, que tem como objetivo criar um modelo que utilize os princípios dos modelos ágeis, mantendo um mínimo de segurança no desenvolvimento do SDL. Os ciclos pequenos dos modelos ágeis torna impraticável o levantamento completo dos requisitos de um sistema nesses ciclos. Portanto, esse modelo retira as fases clássicas do SDL, mas mantém algumas atividades de segurança dentro dos sprints. Para projetos que sejam de grande porte e que principalmente não tenham todos seus requisitos definidos no início do projeto, o modelo SDL-Agile torna-se uma opção interessante.

De acordo com Scott Charney, vice presidente do grupo de confiança computacional da corporação Microsoft, o SDL esta em conformidade com a ISO/IEC 27034-1:2011 — *Information technology — Security techniques — Application security — Overview and concepts*, que oferece um guia de informações de segurança da informação para os implementadores, designers, programadores que desejem criar um sistema de informação, com o objetivo de garantir que sejam modelados e projetados sistemas com o nível necessário de segurança, demonstrando a comprometimento desse modelo com as normas internacionais.

4.3 CONSIDERAÇÕES DE SEGURANÇA NO CICLO DE VIDA DE DESENVOLVIMENTO DO SISTEMA – NIST

O *National Institute of Standards and Technology* – NIST é uma agência governamental não-regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. O NIST foi criado com a missão de promover a inovação e a competitividade industrial dos Estados Unidos através do avanço da metrologia, dos padrões e da tecnologia de forma que ampliem a segurança econômica e melhorem a qualidade de vida.

Atividades do NIST são distribuídas em programas de laboratório e programas de extensão Universitária. Os programas de laboratório incluem: (NIST, 2008)
Laboratório de Engenharia (EL)

- *Information Technology Laboratory (ITL).*
- Material de medição de laboratório (MML).
- Laboratório de medição física (PML).
- Centro de Nanociência e Nanotecnologia (CNST).
- *NIST Center for Neutron Research (NCNR).*

Já os programas de extensão incluem:

- *Hollings Manufacturing Extension Partnership (MEP).*
- Programa de Inovação Tecnológica (TIP).

Este documento (NIST, 2008) do National Institute of Standard and Technology trata de aspectos de segurança no ciclo de vida de desenvolvimento de sistemas, e foi criada para assistir entes governamentais a adequarem as suas implementações de sistemas as atividades essências de segurança da informação e análise e controle de riscos.

O documento é dividido em quatro capítulos e sete apêndices. O primeiro capítulo trata da proposta e do escopo do documento. O segundo capítulo trata da visão dos fundamentos do desenvolvimento do ciclo de vida de sistemas seguros. Já o terceiro capítulo trata da incorporação de segurança no ciclo de vida de desenvolvimento de sistemas. Por fim, o quarto capítulo fala sobre considerações adicionais de segurança. Dentre os apêndices deste documento vale ressaltar, para este trabalho, o anexo G que contem as visualizações gráficas da segurança dentro da SDLC.

4.3.1 VISÃO DOS FUNDAMENTOS DO DESENVOLVIMENTO DO CICLO DE VIDA DE SISTEMAS SEGUROS

Este segundo capítulo do documento (NIST, 2008) trata a respeito dos processos de segurança de sistemas de informação que proporcionam uma contribuição para gestão de sistemas de TI e seu desenvolvimento, permitindo assim a identificação de riscos. A abordagem de gerenciamento de risco envolve o equilíbrio continuo à proteção de informações e de ativos com o custo de controles de segurança e estratégias de balanceamento para todo o sistema de informações do ciclo de vida de desenvolvimento. Esta abordagem pode ser melhor representada pela ilustração da figura 4.5. (NIST, 2008)

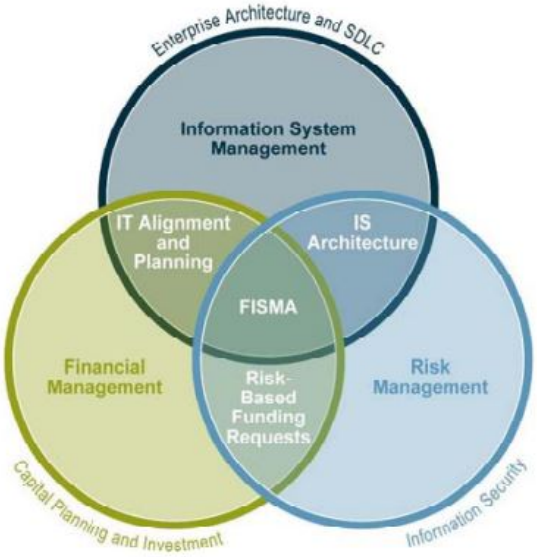

Figura 4.5. Considerações de segurança. (NIST, 2008)

Ainda, segundo o documento, a forma mais eficaz de se implementar gestão de riscos é identificar os ativos críticos e operações bem como as suas vulnerabilidades. Os riscos são compartilhados e não estão presentes em apenas uma determinada área.

Para ser mais eficaz, a segurança da informação deve ser integrada no SDLC do sistema em criação. Integração precoce de segurança no SDLC permite que as agências maximizem o retorno sobre os investimentos em seus programas de segurança, através dos seguintes aspectos (NIST, 2008):

- A identificação precoce de vulnerabilidades de segurança e erros de configuração, resultando em menor custo de implementação de controles de segurança e mitigação da vulnerabilidade;
- Conscientização sobre os desafios de engenharia causados por controles de segurança obrigatórios;
- Identificação dos serviços de segurança compartilhados e reutilização de estratégias e ferramentas;
- Custo de desenvolvimento e programação, melhorando a postura de segurança através de métodos comprovados e técnicas.

Assim, a diretriz SDLC descrita nas fases do processo proposto pelo NIST fornece utilitário, documentando as seguintes características (NIST, 2008):

- Visão sobre as principais atividades e metas;
- Pontos de decisão ou controles;
- Saídas especificadas que fornecem informações vitais para o projeto do sistema;
- Projeto de realizações;
- Manutenção do sistema, segurança e considerações operacionais;

Considerando o ciclo de vida de desenvolvimento seguro de sistemas (SDLC), o documento (NIST, 2008) propõe cinco fases para a implementação. São elas: Iniciação, Desenvolvimento/Aquisição, Implementação/Análise, Operação e manutenção e a fase de Descarte. Contudo, para efeito deste trabalho, foram descritas apenas as três primeiras fases do clico de vida proposto pelo documento. Levamos isto em conta devido aos aspectos do documento do OASIS que não enfatiza a Operação e o Descarte do sistema. Assim, em cada

fase, foram abordados aspectos sobre as atividades e saídas de cada tarefa. Estas informações serão distribuídas em tabelas ao longo do texto de forma a facilitar a visualização destes processos. Além disso, será explanada uma breve descrição sobre cada tarefa.

4.3.2 A FASE DE INICIAÇÃO

A fase de iniciação é uma atividade de análise que avalia a capacidade de uma organização satisfazer as demandas existentes e emergentes. Esta é a etapa de determinação das necessidades que irão resultar em uma descrição de alto nível dos controles de segurança em determinado sistema proposto e também as exigências de garantia.

Desta forma, as atividades de segurança chave para esta fase incluem (NIST, 2008):

- Delimitação inicial de requisitos de negócio em termos de confidencialidade, integridade e disponibilidade;
- Padrões de categorização de Segurança para ajudar as organizações a fazer a seleção adequada de controles de segurança para suas informações;
- Determinação de quaisquer requisitos de privacidade.

Nesta etapa, a segurança é vista mais em termos de riscos do negócio. Assim, a avaliação preliminar de riscos resulta em uma descrição inicial das necessidades básicas de segurança do sistema. Esta avaliação deve definir o ambiente de ameaça em que o sistema irá operar e em seguida determinar uma identificação inicial de controles de segurança necessários que devem ser cumpridos para proteger o sistema no ambiente operacional pretendido.

Os tipos gerais de controle descritos nesta fase podem ser assim descritos (NIST, 2008):

- A determinação da estratégia de aquisição a ser usada durante todo o restante do processo de desenvolvimento;
- Uma revisão de conceito de sistema que verifica a viabilidade em consonância com os objetivos da organização e também as restrições orçamentárias;
- Uma revisão de especificação de desempenho que garante que o projeto inicial do sistema abordou todos os aspectos identificados e os requisitos de segurança especificados;

- Um alinhamento de arquitetura empresarial (EA, NIST 2008) de acordo com a visão TI, padrões e requisitos de negócio, bem como o alinhamento de segurança com os serviços de segurança atuais e iminentes;
- A análise financeira que verifica se o sistema será alinhado com artefatos e orientação CPIC (NIST 2008), equilibrando as implicações de custos associados à gestão de riscos;
- Uma análise de gestão de riscos em conformidade com o gerenciamento de risco NIST recomendando orientações para reduzir a ambiguidade na gestão de risco do sistema. Incluídos nesta etapa da gestão de risco estão as revisões dos resultados de categorização de segurança de sistemas de informação, que incluem tipos identificados de informação, níveis de impacto resultante, e o sistema final de categorização de segurança.

O documento (NIST, 2008) destaca atividades que merecem maior atenção nesta etapa do ciclo de vida de desenvolvimento seguro de sistemas. A figura 4.6, obtida do documento, ilustra estas atividades, saídas e controles.

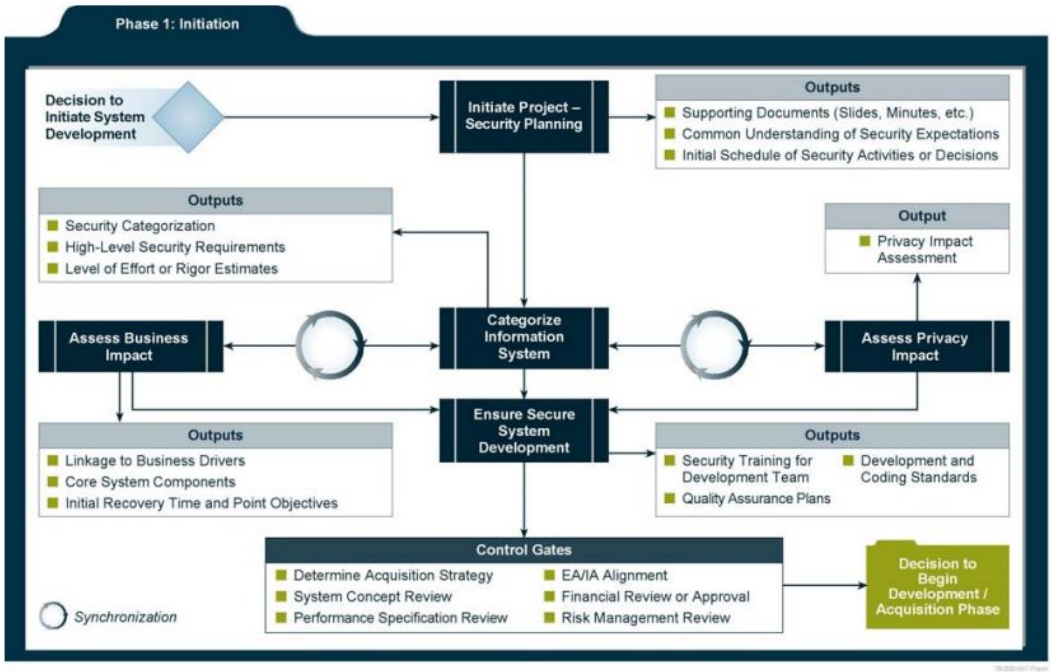

Figura 4.6. Fase de iniciação. (NIST, 2008)

A tabela 4.13 a seguir ilustra as atividades tratadas no processo de iniciação e suas respectivas saídas:

Tabela 4.13: Atividades e saídas da fase de iniciação. (NIST, 2008)

Atividade	Saídas
Iniciar o planejamento de segurança	▪ Os documentos de apoio (slides, atas de

	reuniões, etc); ▪ Entendimento comum das expectativas de segurança; ▪ Cronograma inicial das atividades de segurança ou decisões;
Categorizar as informações do sistema	▪ Documentar a investigação, as decisões-chave, e as razões de apoio para a segurança do sistema de informação; ▪ Requisitos de Alto Nível de Segurança;
Avaliação do impacto de negócio	▪ Identificar as linhas de negócio suportadas por este sistema e como essas linhas de negócio serão impactadas; ▪ Identificar os componentes do sistema de base necessários para manter a funcionalidade mínima; ▪ *Recovery Time Objective;* ▪ Identificar a tolerância de negócios por perda de dados;
Avaliação do impacto de privacidade	▪ Avaliação do Impacto de Privacidade fornecendo detalhes sobre onde e em que grau de privacidade de informações é coletado, armazenado ou criado dentro do sistema;
Garantir a utilização de um processo de desenvolvimento de sistemas seguro	▪ Planos para treinamento da fase de segurança de desenvolvimento; ▪ Técnicas de garantia da qualidade planejada, resultados e metas; ▪ Desenvolvimento e padrões de codificação, incluindo ambiente de desenvolvimento;

Abaixo, foram descritas as principais atividades desta fase que, segundo o documento (NIST, 2008) são mais críticas no ponto de vista de segurança:

4.3.2.1 INICIAR O PLANEJAMENTO DE SEGURANÇA

A fase de planejamento de segurança deve começar com as seguintes etapas (NIST, 2008):

- Identificação das funções fundamentais de segurança para o desenvolvimento;
- Identificar as fontes de requisitos de segurança, tais como leis, regulamento e normas;
- Garantir que todas as partes interessadas tenham um entendimento comum, inclusive sobre segurança.
- Delinear pensamentos iniciais sobre marcos de segurança importantes, incluindo prazos ou desenvolvimento de gatilhos que sinalizam que um passo de segurança esta se aproximando.

Este envolvimento inicial permite aos desenvolvedores e agentes planejar os requisitos de segurança a associar restrições ao projeto. Adicionalmente também mostra aos líderes de projeto que muitas decisões tomadas tem implicações de segurança e que elas devem ser ponderadas de forma adequada, conforme o projeto continue.

Identificação das funções de segurança (NIST, 2008):

Este é um importante passo que deve levar em consideração o quanto é necessário dedicar-se a essa tarefa, as habilidades necessárias ao exercício das funções e a capacidade que o indivíduo tem para efetivamente realizar as responsabilidades. Identificar as funções de segurança no início do processo fornece as ideias-chave baseadas no risco de decisões tomadas no início do processo e fornece aos outros membros da equipe acesso às funções para apoio na integração de segurança para o desenvolvimento do sistema.

Conscientização da integração da segurança aos *Stakeholder* (NIST, 2008):

O ISSO (NIST, 2008) é um agente que fornece ao proprietário do negócio e ao desenvolvedor uma compreensão inicial dos passos de segurança, requisitos e expectativas para que a segurança possa ser planejada desde o início. Nesta etapa, os seguintes tópicos se destacam:

- Responsabilidades de segurança;
- Métricas Relatórios de Segurança;
- Controles de segurança comuns (se aplicável);
- Certificação e aceitação do Processo;
- Teste de Segurança e Técnicas de Avaliação;
- Documento de segurança e exigência de Entrega;
- Design seguro, Arquitetura e práticas de codificação;
- Segurança, Aquisição e Considerações;
- Principais atividades com cronograma de desenvolvimento e impacto de recursos, tais como testes de ativo, aceitação e formação.

4.3.2.2 CATEGORIZAR AS INFORMAÇÕES DO SISTEMA

Esta etapa fornece um passo vital no sentido de integrar a segurança no negócio das agências governamentais e funções de gestão de tecnologia da informação. Além disso, estabelece as bases para a segurança e padronização entre os sistemas de informação. Os

passos seguintes se concentram na avaliação de segurança em termos de confidencialidade, integridade e disponibilidade. O resultado é uma forte ligação entre sistemas de informação com a segurança da informação com um bom custo-benefício.

"Nível de estimativas de esforço - nível inicial de esforço que pode ser derivada a partir da aplicação do resultante da categorização de segurança para os controles de segurança mínimos na NIST SP 800-53, e a avaliação de procedimentos em NIST SP 800-53A, o Guia para a Avaliação dos controles de segurança na Federal Sistemas de Informação." (NIST, 2008)

4.3.2.3 AVALIAÇÃO DO IMPACTO DE NEGÓCIO

Uma avaliação do impacto do sistema sobre as linhas de negócios correlaciona os componentes específicos do sistema com os serviços críticos de negócios. Esta informação é então usada para caracterizar as consequências da missão de negócios com uma ruptura com o sistema de componentes.

4.3.2.4 AVALIAÇÃO DO IMPACTO DE PRIVACIDADE

Nesta etapa, considerações importantes sobre o sistema são realizadas. Transmitir, armazenar ou criar informações que podem ser consideradas de privacidade são tipicamente identificadas durante o processo de categorização de segurança, ao identificar os tipos de informação. Contudo, uma vez identificado como um sistema em desenvolvimento que provavelmente irá lidar com a privacidade das informações, o proprietário do sistema deve trabalhar no sentido de identificar e implementar as medidas de proteção apropriadas e controles de segurança, incluindo processos para atender às exigências de privacidade de informações de manuseio e de relatórios de incidentes .

4.3.2.5 GARANTIR A UTILIZAÇÃO DE UM PROCESSO DE DESENVOLVIMENTO DE SISTEMAS SEGURO

Nesta tarefa são realizadas considerações de forma a garantir o uso de processos seguros de desenvolvimento de sistemas de informação. Ainda, esta tarefa considera que o principal responsável pela segurança do aplicativo, durante as fases iniciais, é a equipe de desenvolvimento que tem a compreensão mais aprofundada do funcionamento da aplicação e a capacidade de identificar defeitos de segurança de comportamento funcional. Eles são o primeiro nível de proteção e a oportunidade de construir segurança. O documento ainda considera que é importante que o seu papel não pode ser assumido ou diminuído. Assim, considerações sobre o plano podem incluir (NIST, 2008):

- Conceito seguro de operações para o desenvolvimento;
- Processos e padrões;
- Treinamento de segurança para a equipe de desenvolvimento.
- Gerenciamento de qualidade;
- Ambiente seguro;
- Práticas de códigos seguros.

4.3.3 DESENVOLVIMENTO E AQUISIÇÃO

Nesta segunda fase, são abordadas as seguintes considerações de segurança (NIST, 2008):

- Realizar a avaliação de risco e usar os resultados para complementar os controles de segurança básicos;
- Analisar os requisitos de segurança;
- Realizar testes funcionais de segurança;
- Preparar documentos iniciais para a certificação e aceitação do sistema;
- Arquitetura de segurança do projeto.

Complementarmente, o documento (NIST, 2008) destaca atividades que merecem maior atenção no ciclo de vida de desenvolvimento seguro de sistemas. A figura 4.7, obtida do documento, ilustra estas atividades, saídas e controles.

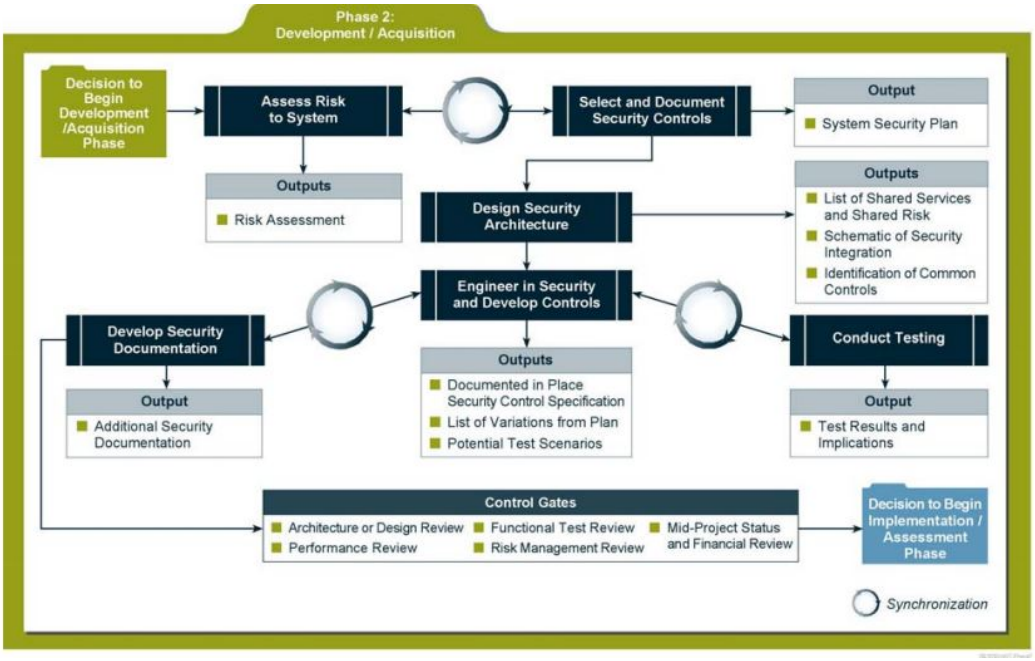

Figura 4.7. Fase de desenvolvimento/aquisição. (NIST, 2008)

A tabela 4.14 a seguir ilustra as atividades tratadas no processo de desenvolvimento/aquisição e suas respectivas saídas:

Tabela 4.14: Atividades e saídas da fase desenvolvimento/aquisição. (NIST, 2008)

Atividades	**Saídas**
Análise de risco do sistema	▪ Uma avaliação de risco refinada com base em um projeto de sistema mais maduro que reflete com mais precisão o risco potencial para o sistema, os pontos fracos conhecidos do design, identificando restrições do projeto e ameaças para o negócio; ▪ Componentes de TI conhecidos. Além disso, os requisitos anteriores são agora a transição para controles específicos do sistema.
Selecionar e documentar os controles de segurança	▪ Plano de Segurança do Sistema - especificação dos controles de segurança que identificam o que, onde e como controles de segurança serão aplicados.
Projetar a arquitetura de segurança	▪ Esquema de integração de segurança fornecendo detalhes sobre onde, dentro do sistema, a segurança é implementada e compartilhada. Arquiteturas de segurança devem ser representadas graficamente e detalhadamente, na medida em que o leitor possa ver onde os controles de segurança básicos são aplicados e também como são implementados; ▪ Listagem de serviços partilhados resultando risco compartilhado.
Desenvolver controles	▪ Controles implementados com especificação documentada para inclusão no plano de segurança;

	▪ Lista de variações de controle de segurança resultantes de decisões de desenvolvimento; ▪ Cenários de avaliação de potenciais riscos para testar vulnerabilidades ou limitações conhecidas.
Criar a documentação de segurança	▪ Documentação de segurança adicional; ▪ Apoiar o plano de segurança do sistema.
Conduzir testes (Implementação, funcionais e segurança)	▪ Documentação dos resultados dos testes, incluindo quaisquer variações inesperadas descobertas durante os testes.

Abaixo, foram descritas as principais atividades que, segundo o documento, são as mais críticas do ponto de vista de segurança:

4.3.3.1 ANÁLISE DE RISCO DO SISTEMA

O objetivo de uma avaliação de risco é validar o conhecimento do design do sistema e os requisitos mínimos de segurança derivados do processo de classificação de segurança para determinar a sua eficácia de forma a reduzir os riscos previstos. Os resultados devem mostrar que os controles de segurança especificados anteriormente fornecem proteções apropriadas ou processos de destaque, onde o planejamento ainda é necessário. Segundo o documento (NIST, 2008), para um projeto ser bem sucedido é necessária a participação de pessoas que tenham conhecimento nas disciplinas dentro do domínio do sistema (por exemplo, usuários, especialistas em tecnologia, especialistas em operações). A avaliação de risco de segurança deve ser realizada antes da aprovação das especificações de projeto. Também devem ser feitas considerações sobre integrações com outros sistemas.

4.3.3.2 SELECIONAR E DOCUMENTAR OS CONTROLES DE SEGURANÇA

A seleção de controles de segurança, segundo o documento (NIST, 2008), consiste nas três seguintes atividades: Seleção de controles de segurança básicos (incluindo controles de segurança comuns), Aplicação de controles de segurança orientados para ajustar o controle de segurança básico, e a ampliação de controles de segurança básicos adaptados aos controles adicionais, com base em uma avaliação de risco e condições locais.

Ainda, segundo o documento (NIST, 2008), O processo de seleção de controles de segurança deve incluir uma análise das leis e regulamentos, os atos de habilitação, governança específica do órgão e demais legislação e regulamentos federais que definem especificações aplicáveis aos controles de segurança selecionados.

4.3.3.3 PROJETAR A ARQUITETURA DE SEGURANÇA

Segundo o documento (NIST, 2008), no nível do sistema, a segurança deve ser projetada e concebida para o todo o projeto. Isto é obtido através de serviços de agrupamento ou de zoneamento em conjunto ou distribuído para quaisquer camadas adicionais de proteção. A Concepção de segurança no nível do sistema deve levar em consideração os serviços obtidos e interconexões externas do sistema, planejadas e as diferentes orientações de utilizadores da rede. Ainda, nesta etapa, é realizada auditoria nos sistemas de forma a encontrar possíveis pontos onde podem conter falhas de segurança. Assim, segundo o documento (NIST, 2008) esta atividade pode ser realizada durante a revisão do desenvolvimento de forma a reconhecer gargalos e pontos únicos de falha. Ainda, esta atividade pode proporcionar maior valor para o sistema com a redução do custo total de planejamento de componentes principais de uma forma segura.

4.3.3.4 DESENVOLVER CONTROLES

Durante esta fase, segundo o documento (NIST, 2008), os controles de segurança são implementados e tornam-se parte do sistema. A aplicação dos controles de segurança em desenvolvimento deve ser realizada com cuidado e planejada de forma lógica. A intenção é integrar os controles para que os desafios com relação ao desempenho do sistema sejam conhecidos precocemente. Além disso, alguns controles de segurança podem limitar ou impedir o normal funcionamento do sistema.

Assim, durante esta tarefa, as decisões são tomadas com base em desafios de integração e *trade-offs*. Nos casos em não há um controle planejado possível ou conveniente, os controles de compensação devem ser considerados e documentados.

4.3.3.5 CRIAR A DOCUMENTAÇÃO DE SEGURANÇA

O documento do (NIST, 2008) elucida nesta tarefa uma lista de documentação de apoio para o desenvolvimento seguro de um sistema (NIST, 2008). São elas:

- Plano de gerenciamento de configuração;
- Plano de contingência (incluindo um Estudo de Impacto de Negócios);
- Plano de monitoramento contínuo;
- Consciência de segurança, formação e educação;

- Plano de resposta a incidentes;
- Avaliação do impacto de Privacidade.

O desenvolvimento destes documentos deve considerar a maturidade dos serviços de segurança. Em alguns casos, esses documentos podem conter só requisitos conhecidos, controles comuns e modelos. Segundo o documento (NIST, 2008), o preenchimento destes documentos deve começar o mais cedo possível durante o projeto.

4.3.3.6 CONDUZIR TESTES (IMPLEMENTAÇÃO, FUNCIONAIS E SEGURANÇA)

O documento (NIST, 2008) menciona que o processo centra-se na especificidade, repetição e iteração. Para a especificidade, o teste deve ser realizado para verificar os requisitos de segurança relevantes, uma vez que se destina ao uso em seu ambiente. Para repetição, o processo deve ser capaz de executar de uma série de testes contra um sistema de informação mais de uma vez (ou contra sistemas semelhantes em paralelo) e produzir resultados semelhantes a cada vez. Para iteração, em cada sistema será necessário executar os testes funcionais, no todo ou em parte, um número de vezes sucessivas, a fim de alcançar um nível aceitável de conformidade com os requisitos do sistema. Para alcançar este objetivo, o teste funcional será automatizado, e os casos de teste serão publicados, em detalhe, para assegurar que o processo de ensaio seja possível de se repetir e também seja iterativo.

4.3.4 IMPLEMENTAÇÃO E AVALIAÇÃO

A implementação e avaliação é a terceira fase do SDLC descrito no documento (NIST, 2008). Durante esta fase, o sistema irá ser instalado e avaliado no ambiente operacional de determinada organização.

As principais atividades de segurança nesta fase são:

- Integrar o sistema de informação em seu ambiente;
- Planejar e conduzir as atividades de certificação de sistemas na sincronização com os testes de segurança e controles;
- Completar as atividades de aceitação do sistema.

Entre as etapas de controle desta fase, estão (NIST, 2008):

- Sistema de teste de revisão de preparação;
- Criar plano para *C&A*;

- Status Final de Projetos e Análise Financeira;
- Implantação de revisão de preparação;
- Agente de autorização (AO) de decisão;
- Implantação de TI ou Aprovação de conexão.

A tabela 4.15 a seguir ilustra as principais atividades tratadas no processo de implementação/avaliação e suas respectivas saídas:

Tabela 4.15: Atividades e saídas da fase implementação/avaliação. (NIST, 2008)

Atividades	Saídas
Criar plano para a C&A	▪ Plano de Trabalho inicial: Um documento de planejamento que identifica os participantes-chave, restrições do projeto, núcleo componentes, escopo dos testes e nível de rigor esperado. O pacote de certificação deve estar perto da conclusão.
Integrar segurança dentro ambiente e sistema estabelecido	▪ Lista de verificação de controles de segurança operacionais; ▪ Concluir a documentação do sistema.
Avaliar a segurança do sistema	▪ Pacote de Segurança de aceitação, que inclui o Relatório de Avaliação de Segurança, o POA & M, e do Plano de Segurança do Sistema atualizado.
Autorizar o sistema de informação	▪ Decisão de autorização de segurança, documentado e transmitido emitido pelo *Authorizing Official* para o Proprietário do sistema e ISSO (NIST 2008); ▪ Pacote de Autorização de Segurança final.

As principais atividades de segurança se destacam, segundo o documento, por serem mais críticas no ponto de vista de segurança do sistema:

4.3.4.1 CRIAR PLANO PARA A C&A (CERTIFICAÇÃO E APROVAÇÃO)

Esta atividade se destaca porque o agente de autorização (AO) é responsável por aceitar o risco de operar o sistema, e ele pode aconselhar a equipe de desenvolvimento quanto aos riscos associados a uma eventual operação do sistema que pode ser inaceitável. Assim, as especificações podem impor encargos excessivos e elevados custos se os riscos residuais aceitáveis não são conhecidos. Desta forma, é necessário o envolvimento do AO para este determinação desses riscos aceitáveis.

4.3.4.2 INTEGRAR SEGURANÇA DENTRO AMBIENTE E SISTEMA ESTABELECIDO

A integração do sistema ocorre no local operacional onde o sistema de informação deverá ser implantado para operação. Integração e testes de aceitação ocorrem após a entrega do sistema. Configurações de controle de segurança são ativadas de acordo com as instruções dos fabricantes e especificações de segurança documentadas.

4.3.4.3 AVALIAR A SEGURANÇA DO SISTEMA

Sistemas que estão sendo desenvolvidos deverão ser formalmente avaliados antes de ser concedida a sua aceitação. O objetivo do processo de avaliação de segurança é confirmar que o sistema está em conformidade com os requisitos de segurança funcionais e que irá operar dentro de um nível aceitável de segurança residual risco.

4.3.4.4 AUTORIZAR O SISTEMA DE INFORMAÇÃO

O sistema construído nesta arquitetura, segundo o documento (NIST, 2008), requer a autorização de segurança para processar, armazenar, ou transmitir informações. Esta autorização, também conhecida como aceitação de segurança, é concedida por uma agência oficial e baseia-se no certificado de eficácia dos controles de segurança para algum nível de garantia de risco residual identificado. A decisão de autorização de segurança é baseada no risco de escolha, que depende fortemente, mas não exclusivamente, dos testes de segurança e dos resultados da avaliação produzidos durante o processo de verificação de controle de segurança. Um agente que autoriza baseia-se principalmente no plano de segurança do sistema completo, teste nos resultados da avaliação de segurança de forma a reduzir ou eliminar as vulnerabilidades do sistema de informação.

Segue a figura 4.8 obtida no documento (NIST, 2008) relativa à fase Implementação e Avaliação.

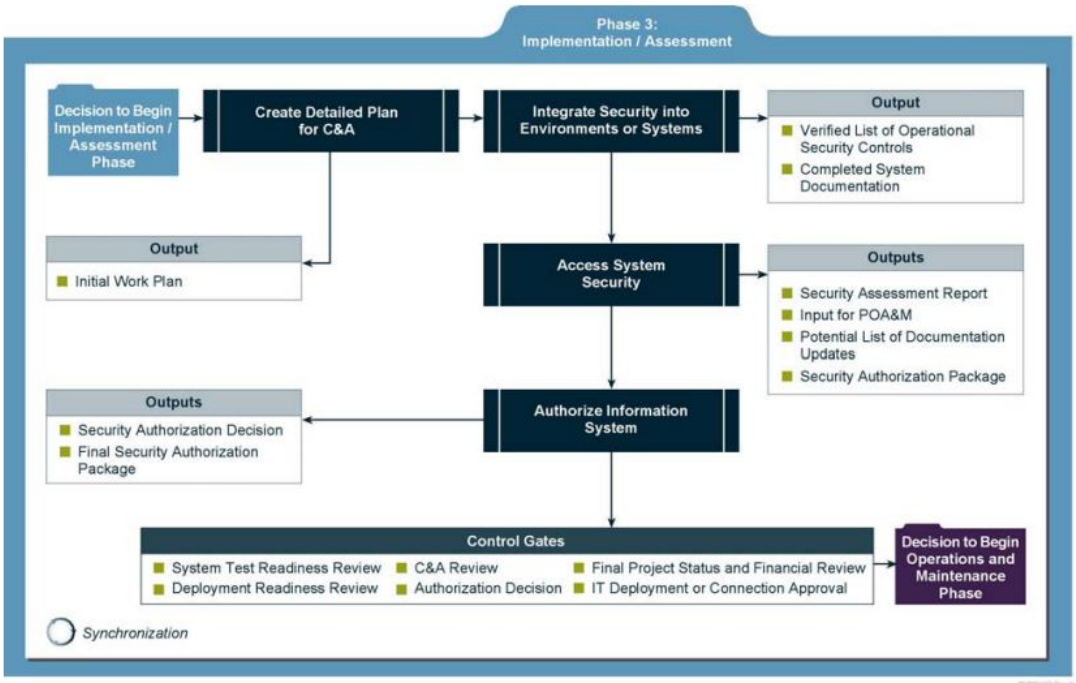

Figura 4.8. Fase de implementação/avaliação. (NIST, 2008)

4.4 CONSIDERAÇÕES FINAIS SOBRE OS DOCUMENTOS

Tendo em vista os documentos apresentados, verificamos que o primeiro documento, *OASIS Web Service implementation methodology* (OASIS, 2005) trata de aspectos e considerações sobre o desenvolvimento de Web Services apresentando um ciclo de interação ágil com seis fases. Estas fases podem ser incrementais e iterativas, porém não comprometendo a agilidade do processo. Constatamos ainda que o documento apresenta carência nas atividades e tarefas de segurança, sendo pouco detalhadas.

O segundo documento, *Microsoft security development lifecycle* (MICROSOFT, 2012), propõe um ciclo de vida para o desenvolvimento seguro de softwares, especificando fases e práticas que devem ser adotadas durante determinadas etapas de um projeto de implementação de software. Trata-se de um documento mais técnico, mas ainda abordando procedimento de analistas, arquitetos e gerentes de projeto.

Por fim, o terceiro documento, *Security considerations in the system development life cicle* (NIST,2008) trata de aspectos de segurança no ciclo de vida de desenvolvimento de sistemas. Ainda, neste documento, foram abordadas apenas as três primeiras fases: Iniciação, Desenvolvimento/Aquisição e Implementação/Análise, onde formam examinadas apenas as atividade e as saídas das atividades de cada fase, suprimindo a averiguação da sincronização, das interdependências, das dicas e dos *control gates*. No entanto, foi deixada de fora do trabalho a análise das fases de Operação/ Manutenção e Descarte, que são recomendações posteriores à implementação.

Assim, considerando que cada um destes documentos não trata isoladamente de recomendações de segurança para o desenvolvimento de Web Services, buscamos integrar as atividades propostas nos documentos da Microsoft e do NIST ao documento do OASIS, com o intuito de assim construir um guia de recomendações para a implementação de Web Services seguros. Desta forma, neste próximo capítulo, foi construído um guia com aspectos de alto nível de considerações para a implementação e desenvolvimento de Web Services seguros.

5 ANÁLISE E CONSTRUÇÃO DO GUIA DE RECOMENDAÇÕES PARA A IMPLEMENTAÇÃO DE WEB SERVICES SEGUROS

Neste capítulo foi realizada uma adaptação do documento do OASIS, fornecendo ao seu modelo de desenvolvimento de Web Services aspectos de segurança durante a elaboração do sistema, e recomendações quanto a sua estrutura, para torná-lo mais seguro. Foram descritas e explicadas apenas as adaptações realizadas no modelo, as atividades que não tiverem sido alteradas não foram descritas, pois já foram realizadas nos capítulos anteriores.

Após a análise dos documentos no capítulo anterior, foi possível verificar a importância de cada modelo dentro de seus escopos. Nesta parte do trabalho apresentaremos um estudo demonstrando por meio de tabelas, desenho de processos e análises de dados relações entre os documentos apresentados no capítulo anterior para construir um guia com recomendações de segurança na implementação de Web Services. As atividades, saídas e práticas dos documentos da *Microsoft* e do NIST serão mapeadas para outras atividades ou tarefas do documento de modelo de desenvolvimento de Web Services da OASIS, que manteve as suas seis fases originais, com as suas atividades e tarefas originais ou apenas agrupadas às normas sugeridas.

Precedendo a primeira fase de requisitos, é recomendado pelo SDL que a equipe do projeto passe por treinamentos básicos de segurança da informação, tanto para os papéis mais técnicos, como para gestores. Recomenda-se ter um mínimo de membros com conhecimentos necessários para avaliar corretamente as questões de segurança no âmbito do projeto. Além disso, constantes atualizações são encorajadas para manter o profissional atento a novas ameaças. Os treinamentos básicos contém o projeto de segurança, a modelagem de ameaças, a codificação e testes seguros e a privacidade que devem ser averiguados na seção 4.2 deste trabalho. A seguir, estão apresentadas as seis fases do guia de recomendações: requisitos, análise, design, codificação, testes e implantação.

5.1 FASE DE REQUISITOS

Nesta fase foi adicionada uma atividade de iniciação do planejamento da segurança que consiste em uma forma de adequar as implicações de segurança ao projeto, permitindo o controle das mudanças ao longo do ciclo de vida. Nesta atividade serão realizadas as seguintes tarefas:

- Identificar o especialista de segurança de Web Services, que irá orientar quanto aos aspectos de segurança mais importantes durante o andamento do projeto, dando suporte às decisões mais críticas e auxiliando na atribuição de encargos da equipe.
- Identificar as principais funções de segurança para o desenvolvimento atribuindo responsabilidades aos integrantes do projeto, organizando as habilidades e tempo para cada tarefa. A norma ABNT NBR ISO/IEC 27002:2005 possui na sua seção 6.1.3 um controle correspondente a essa tarefa, que pode ser analisada para um melhor entendimento.
- Definir as expectativas de segurança do projeto que estabelece os serviços de segurança mais importantes para o negócio, como por exemplo a necessidade de alta disponibilidade para aplicação ser crucial para o negócio.
- Categorizar a informação integra os aspectos de segurança ao negócio, que servirá de contexto para a análise risco e insumo para a definição dos controles de segurança. A categorização de informação ajuda a organização a atingir a missão estabelecida, proteger seus ativos e indivíduos bem como satisfazer os requisitos legais. Mais informações podem ser obtidas na norma ABNT NBR ISO/IEC 27002:2005 na seção 7.2.

  "O resultado é uma forte ligação entre a missão, informação e sistemas de informação com uma relação de custo benefício com a segurança da informação." (NIST, 2008)
- A conscientização dos *stakeholders* gera um entendimento antecipado destes com os desenvolvedores quanto as práticas e expectativas de segurança. Essa comunicação esclarece melhor o motivo da realização de algumas práticas de segurança.

O artefato desta atividade contém o cronograma inaugural dos procedimentos que será adotado e um conjunto de documentos de apoio, como as principais fontes de requisitos, como as leis e padrões que serão seguidos.

A atividade de gerência de requisitos foi complementada com a tarefa de criação do planejamento de qualidade, como mostra a figura 5.1, que permite estabelecer um nível mínimo de qualidade de serviço, como a segurança, interoperabilidade, usabilidade, dentre outros. A prática de especificar a ferramenta de rastreabilidade do SDL está contida na tarefa criar matrizes/ferramentas de rastreabilidade, que existia no modelo original do OASIS. Seguem a tabela 5.1 e a figura 5.1 ilustrando a análise da fase de requisitos.

Tabela 5.1: Fase de requisitos do guia proposto

Atividades	**Tarefas**	**Papéis**	**Artefatos**
Determinar a necessidade para o WS	Identificar *stakeholders* Identificar as necessidades dos *stakeholders* Identificar as necessidades da tecnologia de WS Determinar o posicionamento do WS de acordo com os problemas identificados Definir as características do WS baseadas nas necessidades Identificar limitações	Arquiteto Analista de requisitos *Stakeholders* Gestor do projeto	Especificações dos requisitos de negócio Cronograma inicial das atividades
Iniciar Planejamento de Segurança (**NIST**)	Identificar conselheiro de segurança de WS (**SDL**) Identificar as funções fundamentais de segurança (**NIST**) Determinar critérios e expectativas de segurança (**SDL/NIST**) Categorizar informação (**NIST**) Integrar os *stakeholders* (**NIST**)		Documentos de apoio(**NIST**) Cronograma inicial das atividades de segurança(**NIST**)
Extrair requisitos	Identificar as fontes de coleta de requisitos Recolher informações Identificar requisitos funcionais Identificar requisitos não-funcionais	Arquiteto Analista de requisitos Gestor de testes	Especificações dos requisitos
Gerenciar os requisitos de WS	Identificar WS e estabelecer dependências e prioridades Criar planejamento de qualidade (**NIST/SDL**) Criar matrizes/ferramentas de rastreabilidade Administrar mudanças de requisitos	Arquiteto Analista de requisitos Gestor de testes	Especificações dos requisitos

Cenários de modelos de uso	Transformar requisitos funcionais em modelos conceituais de uso Especificar os cenários de integração com os cliente do WS	Arquiteto Analista de requisitos Gestor de testes	Especificações dos requisitos
Preparar casos de teste para Teste de Aceitação do Usuário (UAT) e Teste do Sistema	Criar os cenários de negócio para os casos de teste Construir a matriz de validação de requisitos Administrar mudanças nos casos de teste	Analista de requisitos Gestor de testes Planejador de testes	Plano de teste – UAT e Teste do Sistema

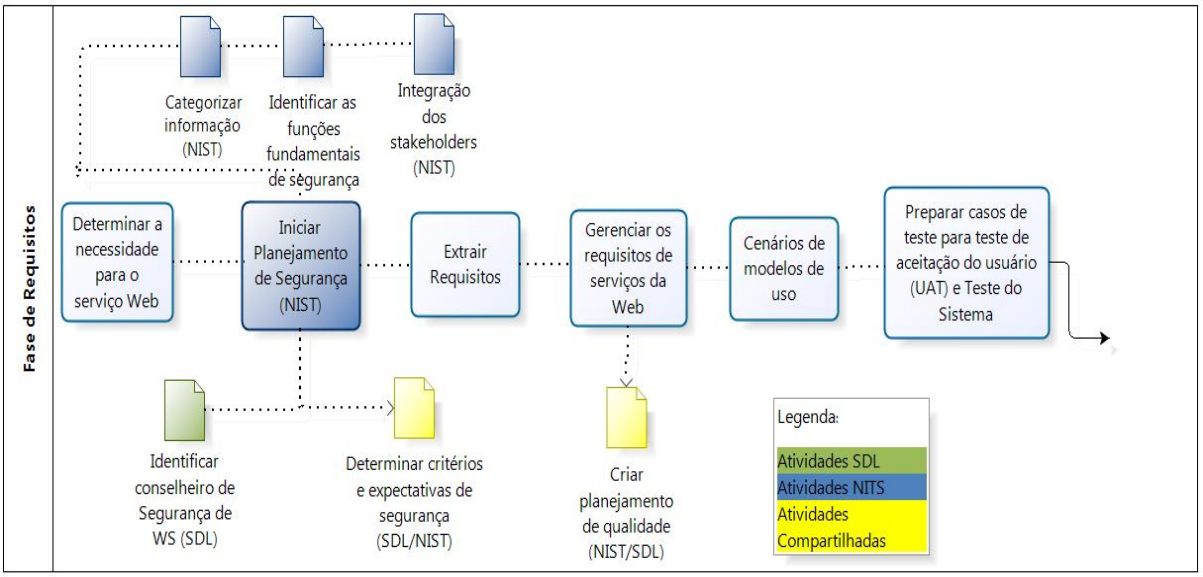

Figura 5.1. Fluxograma da fase de requisitos do guia proposto.

5.2 FASE DE ANÁLISE

A fase de análise recebeu como principal acabamento a atividade de análise e avaliação de risco, que estava presente nas recomendações de segurança do SDL e do NIST, que possui as tarefas baseadas na norma ABNT NBR ISO/IEC 27005. No entanto, o NIST recomenda o documento NIST SP 800-30, *Risk Management Guide for Information Technology Systems* para conduzir a análise de risco. Esta atividade deve se atentar principalmente aos riscos inerentes a Web Services, como os vinculados ao protocolo SOAP ou ao UDDI, que estão descritos na seção 2.6 deste trabalho. O objetivo das suas tarefas são:

- Identificar os riscos que envolvem a busca do conhecimento da fonte, do evento, do motivo e do impacto do risco, por meio de análises, dados coletados ou considerações dos clientes e usuários.

- A análise de impacto de negócio e de risco verifica a probabilidade do evento causador do risco ocorrer, assim como as suas consequências e faz a estimativa dos riscos.
- A avaliação do risco utiliza a análise de risco e os critérios levantados nos requisitos, para definir se o impacto é ou não tolerável.
- Os possíveis tratamentos de risco se baseiam na avaliação de risco para estabelecer medidas corretivas, preventivas ou até não estabelecer nenhuma ação, aceitando o risco. Pode diminuir ou extinguir a probabilidade e ocorrência ou o impacto do mesmo ao negócio. A aceitação do risco acontece quando o tratamento é mais custoso que o reparo, ou quando a probabilidade de ocorrência é muito pequena. (ABNT NBR, 2011)
- A modelagem de ameaças é realizada para situações de riscos mais significativos para a aplicação, abrangendo o projeto, os códigos, tanto privados como os de terceiros, as funcionalidades e a atualização de versão. Esta atividade deve analisar os fluxos de dados, vulnerabilidades e ativos, sendo executada por ferramentas ou especificações que auxiliem a tarefa e por diversos membros da equipe do projeto como desenvolvedores, arquitetos, testadores e analistas. Esta técnica permite descobrir implicações de segurança no projeto e no ambiente operacional. (*MICROSOFT*, 2012)

Esta atividade produz como artefato, um documento da avaliação de risco, que deve conter as vulnerabilidades, o ambiente, os impactos, os resultados e os possíveis tratamentos. (NIST, 2002)

A atividade de definição de uma sugestão de arquitetura recebe a tarefa de planejamento da arquitetura e controles de segurança, que é essencial para o projeto de uma estrutura de segurança de Web Service confiável. Os controles devem ser especificados quanto a seu local, modo e momento de aplicação, que devem seguir três procedimentos descritos na seção 4.6.2 do documento. Os controles de segurança podem ser explorados nas normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, se necessário. Ainda deve ser realizada a verificação dos riscos compartilhados, quando serviços e dados forem partilhados, tarefa da atividade de identificação de Web Services reutilizáveis devido ao potencial de aproveitamento de serviços existes. O planejamento da arquitetura de segurança deve considerar as dimensões de segurança para Web Services, a segurança da mensagem, a proteção de recursos, a negociação de contratos, a gerência de confiança e a propriedades de segurança, que estão mais descritos na seção 2.7 desse texto.

O SDL recomenda que seja realizada uma aprovação das ferramentas e compiladores que serão utilizadas na implementação, para que sejam escolhidas apenas tecnologias seguras. Essa especificação foi mapeada para a seguinte tarefa: selecionar uma plataforma de tecnologia para a arquitetura de implementação, que apesar de implícita no documento original, pode-se inferir que a seleção contenha critérios de compatibilidade e segurança.

As atividades de preparar casos de teste para teste de desempenho, preparar casos de teste para integração / interoperabilidade teste, preparar casos de teste para teste funcional e preparar teste de ambiente foram agrupadas em uma única atividade para simplificação do guia. A tabela 5.2 e a figura 5.2, demonstram as complementações da fase de análise.

Tabela 5.2: Fase de análise do guia proposto.

Atividades	**Tarefas**	**Papéis**	**Artefatos**
Realizar análise e avaliação de risco (**SDL/NIST**)	Identificação dos riscos (**SDL/NIST**) Análise de impacto de negócio e de riscos (**SDL/NIST**) Avaliar riscos (**SDL/NIST**) Identificar possíveis tratamentos de riscos (**SDL**) Modelagem de ameaças (**SDL**)	Analista	Documento de avaliação de risco
Selecionar uma plataforma de tecnologia para a arquitetura de implementação	Especificar os padrões de implementação Decidir a plataforma tecnológica para a implementação Decidir a plataforma tecnológica para os usuários Decidir a IDE de ferramentas usadas no desenvolvimento	Arquiteto	Especificação da arquitetura do software
Definir uma sugestão de arquitetura	Definir arquitetura de alto nível Identificar os componentes arquiteturais que expõem as funcionalidades de WS Especificar as trocas de informações mais relevantes do WS com os clientes Planejar arquitetura e controles de segurança para WS (**SDL/NIST**)	Arquiteto	Especificação da arquitetura do software Plano de segurança do sistema (**NIST**)
Decidir granularidade do WS	Decidir critérios de granularidade das operações do WS Identificar e agrupar funcionalidades	Arquiteto	Especificação da arquitetura do software

	Escolher os mecanismos que compõem ou agreguem funcionalidades		
Identificar Web Services reutilizáveis	Identificar componentes arquiteturais que possam ser aproveitados por WS existente Identificar os provedores dos WS reutilizáveis Definir os principais cenários de reutilização Verificar riscos compartilhados (**NIST**)	Arquiteto	Especificação da arquitetura do software
Identificar interface de serviço para novos Web Services	Definir novas assinaturas e padrões de operações de WS Definir a gramática do XML na troca de mensagem	Arquiteto Designer	Gramática XML Especificação das assinaturas para o WS
Preparar casos de teste	Preparar casos de testes para o desempenho Preparar casos de testes para a integração e interoperabilidade Preparar casos de testes funcionais Preparar testes de ambiente Preparar testes de segurança	Administrador dos testes de sistema Planejador de testes Testador	Plano de testes

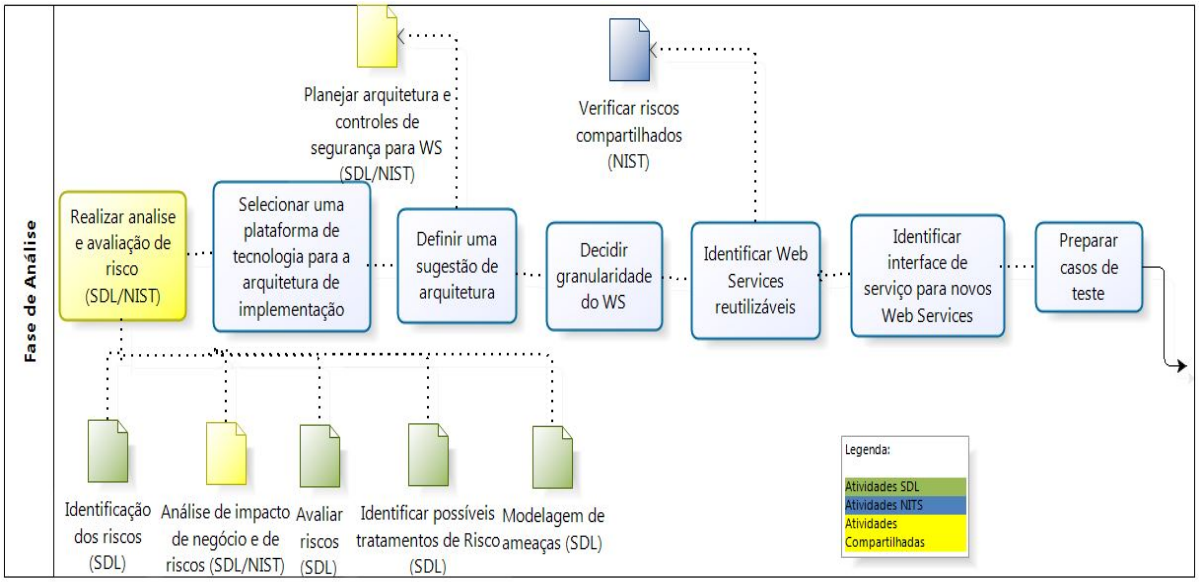

Figura 5.2. Fluxograma da fase de análise do guia proposto.

5.3 FASE DE DESIGN

A fase de design foi complementada com duas novas atividades: definir a estrutura de segurança de Web Services e criar a documentação de segurança. É fortemente recomendado examinar o documento do NIST SP 800-95, *Guide to Secure Web Service,* para entender as principais considerações da segurança para chegar a uma arquitetura protegida e estável.

Na definição da estrutura de segurança de Web Services, recomenda-se utilizar o modelo em camadas de segurança da figura 2.6 (seção 2.7), para garantir as dimensões de segurança analisadas na fase anterior. Apesar de não ser mandatório, os padrões citados na seção 2.7 são específicos para Web Services, ou aplicáveis a este ambiente, logo aconselha-se a sua adoção, uma vez que Web Services possuem vulnerabilidades e ameaças específicas que necessitam ser tratadas para a obtenção de um ambiente seguro, que estão descritas na seção 2.7 do documento. Condizem com essa atividade as seguintes tarefas:

- Revisão de requisitos de segurança de Web Services, uma vez que mudanças podem ter ocorrido ao longo do processo de análise, e reúne o especialista de segurança com o arquiteto para revisar os componentes com maior risco e com impacto de privacidade maior.
- Satisfazer os requisitos mínimos de criptografia e verificar se condiz com a utilização das cifras mais atualizadas e com maior grau de proteção, levando em conta o desempenho da mesma na aplicação. A seguir são citadas algumas recomendações de criptografia pelo SDL: Usar o AES para a criptografia simétrica com a chave de 128 bits ou mais, o RSA para a criptografia assimétrica com a chave de 1024 bits ou mais e o SHA-256 para a aplicação no MAC ou *hashings*. (*MICROSOFT*, 2012)
- Analisar a superfície de ataque, que tem como procedimentos de acordo com SDL, a utilização do acesso seguro do código,o que impede que códigos não confiáveis realizem ações privilegiadas; gerência das exceções do *firewall* deve ser cuidadosamente realizada, para dificultar ataques sem prejudicar na performance do sistema; e garantir que a aplicação funcione corretamente com usuários comuns com o projeto e desenvolvimento aplicados a um usuário padrão.
- A criação dos controles recomenda a utilização das normas ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27003 para a implantação correta dos controles de segurança conforme especificado na fase de análise.

A segunda atividade adicionada é a criação da documentação de segurança, que permite manter um inventário de planos que irão auxiliar as fases seguintes e posteriormente a

manutenção e operação do sistema. No entanto, neste trabalho houve o agrupamento de alguns planos de segurança. A criação dos planos podem ser exploradas no documento NIST *SP* 800-18. Os objetivos e definições dos planos estão listados abaixo:

- Plano de monitoramento contínuo tem como objetivo manter o valor do produto para os clientes por meio da avaliação e melhoria contínua da qualidade do serviço e maturidade dos processos de gerenciamento. Utiliza combinações de princípios, práticas e métodos da gestão de qualidade, gestão de mudanças e melhoria de capacidade. (ABNT NBR, 2005)
- Plano de contingência e continuidade de negócio reúnem ações e estratégias que visam manter ou recuperar o negócio mesmo sobre eventos como falhas e desastres, planejando uma diminuição do impacto causado ou a sua prevenção. De acordo com a ABNT NBR 15999-1:2007, recomenda-se entender como a organização ou o ativo funcionam para depois utilizar a análise de impacto de negócio, com o objetivo de escalar e priorizar os ativos mais relevantes, assim como suas consequências no negócio. A avaliação de risco informa a probabilidade de comprometimento do serviço, que servem para a definição do tempo objetivado de recuperação, que determina em quanto tempo deve ser retornado a normalidade o serviço. A determinação da estratégia de continuidade de negócio indica as consequências, custos e tempos máximos de interrupção. Finalmente, o desenvolvimento e teste dos planos são os seguintes: gerenciamento e resposta a incidentes, continuidade de negócio, recuperação e comunicação. Mais detalhes sobre gerenciamento do plano de continuidade negócio podem ser encontrados na norma citada acima, ou na ABNT NBR ISO/IEC 27002.

  "Plano de Continuidade do Negócio consiste num conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área depara-se com problemas que comprometem o andamento normal dos processos e a consequente prestação dos serviços." (BRASIL, 2012)
- Plano de configuração estabelece como o ambiente de desenvolvimento deve apresentar tanto na fase de implementação como de implantação.

Em seguida, a tabela 5.3 e a figura 5.2 expõem as inserções realizadas na fase de design.

Tabela 5.3: Fase de desenho do guia proposto.

Atividades	Tarefas	Papéis	Artefatos
Transformar as assinaturas dos WS reusáveis	Realizar o mapeamento dos tipos de dados se necessários Identificar os padrões de design para o mapeamento das interfaces dos WS reutilizáveis Revisar os requisitos de segurança de WS (**SDL**)	Designer	Especificações de design
Definir a estrutura de segurança de WS (**NIST**)	Satisfazer os requisitos mínimos de criptografia (**SDL**) Analisar a superfície de ataque (**SDL**) Criar controles de segurança **(NIST)** Plano de monitoramento continuo **(NIST)**	Designer Analista de segurança	Plano de segurança do sistema (**NIST**) Arquitetura de segurança para Web Services
Criar documentação de segurança (**NIST**)	Plano de contingência e continuidade de negócio **(NIST/SDL)** Plano de configuração (**NIST**)	Analista de segurança	Rol das especificações de planos de segurança
Refinar a interface de serviços do novo WS	Refinar a assinatura de interface do WS Refinar a gramática XML na troca de mensagem	Designer	Especificações de design
Desenhar WS	Usar técnicas de modelagem para descrever a estrutura interna do WS Considerar os requisitos não-funcionais e as restrições de design	Designer	Especificações de design

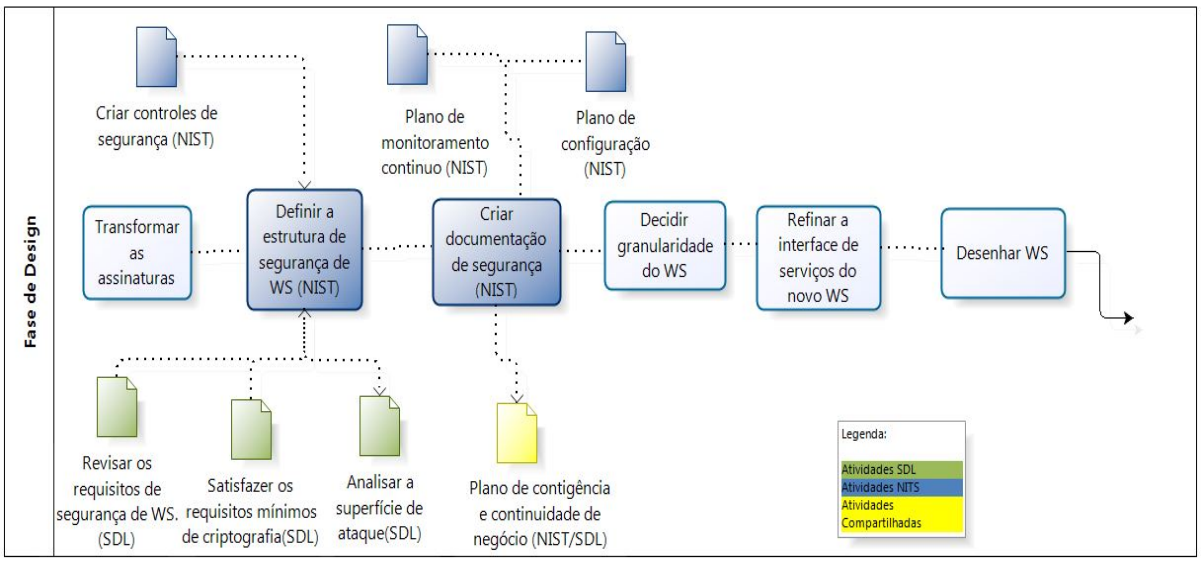

Figura 5.3. Fluxograma da fase de desenho do guia proposto.

5.4 FASE DE CODIFICAÇÃO

Na fase de codificação foram adicionadas as tarefas utilizar funções e ferramentas seguras dentro das atividades de elaboração de código do Web Service. As ferramentas devem estar atualizadas para cobrir o máximo de vulnerabilidades e proteger de novas ameaças. As funções que forem determinadas inseguras devem ser analisadas e listadas pela equipe para bani-las e criar soluções alternativas para que todos desenvolvedores tenham acesso.

A análise estática de código foi incluída como uma tarefa da atividade de teste de unidade e ajuda a verificar se os controles de segurança estão sendo seguidos. Deve ser realizada periodicamente ao longo do desenvolvimento do código para verificar antecipadamente os tipos, estilos, propriedades e bugs. O teste é realizado sem executar o código e por uma ferramenta. No entanto não deve substituir uma revisão manual do código e deve-se considerar que como um ferramenta, possui pontos fortes e fracos. É uma maneira rápida e consistente de validar o código. Seguem as tarefas adicionadas na fase de codificação exibidas na tabela 5.4 e na figura 5.4.

Tabela 5.4: Fase de codificação do guia proposto.

Atividades	Tarefas	Papéis	Artefatos
Elaborar o código do WS	Código baseado na linguagem de implementação escolhida Expor APIs públicas como interfaces Criar WSDL para o cliente Utilizar funções e ferramentas seguras (**SDL**)	Desenvolvedor	Códigos de implementação
Criar o código para o WS do usuário	Decidir o modelo de programação Criar códigos para o usuário Utilizar funções e ferramentas seguras (**SDL**)	Desenvolvedor	Códigos dos usuários
Teste de unidade	Criar o ambiente de testes Realizar os testes de unidade funcionais Realizar análise estática do código (**SDL**)	Desenvolvedor	Scripts de testes de unidade

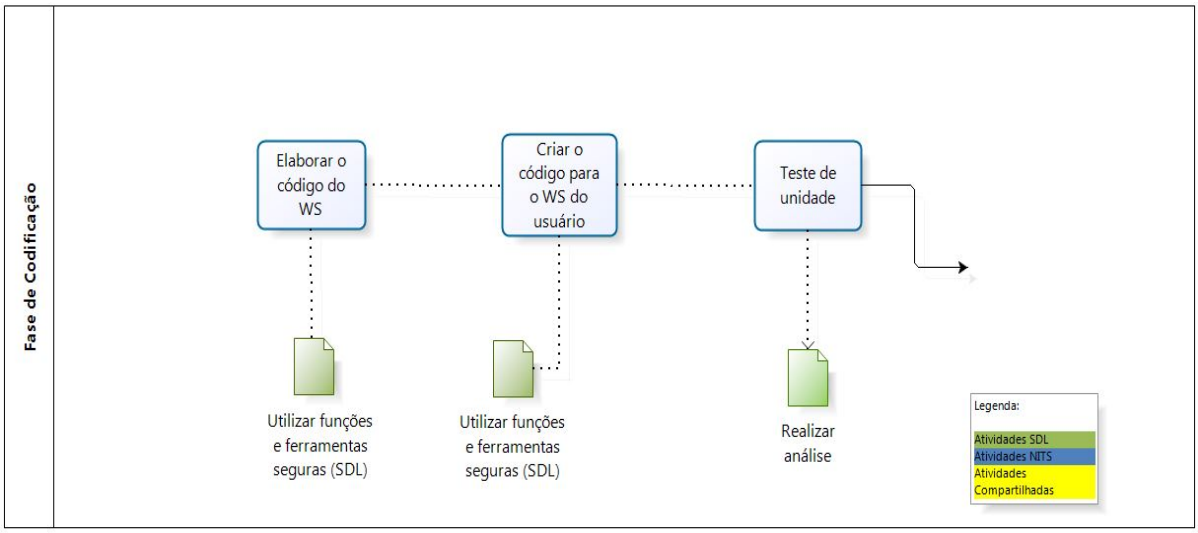

Figura 5.4. Fluxograma da fase de codificação do guia proposto.

5.5 FASE DE TESTES

Nesta fase, foram especificados dois testes que foram incluídos na atividade de testes de funcionalidade. O teste de análise dinâmica, além de verificar o comportamento da aplicação durante a execução do mesmo, verifica se os privilégios de usuário estão de acordo com o especificado ou se a performance está em um nível que é aceito pelo cliente. Esse teste ainda deve realizar procedimentos que forcem o erro com entradas inesperadas, tipos de dados improváveis, forçando o serviço a entrar em colapso ou tentando descobrir alguma falha de implementação.

A fase recebeu uma atividade de teste de segurança onde serão realizadas as verificações mais importantes garantindo que após a fase de implementação os objetivos iniciais não tenham sido desviados, e se houve alguma mudança que tenha sido autorizada e documentada. Seguem as duas tarefas da atividade:

- Antes dos testes de segurança, é realizada uma revisão na superfície de ataque, nos bug de segurança e nos modelos de ameaça, devido às frequentes alterações nos requisitos e nos critérios durante a codificação e o desenho do projeto, é necessária a contabilidade e registro das modificações.
- O objetivo dos testes de segurança é verificar se o sistema desenvolvido está dentro dos conformes dos requisitos e critérios de segurança acordados no início do projeto. Os controles de segurança devem ser testados de acordo com o documento NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.

> Os testes devem ser direcionados para a especificidade, que foca no requisitos de segurança mais relevantes após a implementação; a repetitividade, que garante que os testes possam ser realizados mais de uma vez em ambientes similares e apresentarem resultados semelhantes; e iteração que permite que os testes sejam executados em parte ou em todo o sistema reiteradamente, até atingir a conformidade com os requisitos. Os testes devem ser automatizados ao máximo e seus resultados devem ser publicados, para alcançar as características citadas acima. (NIST, 2008)

Os desenvolvedores dos testes e testadores devem ser independentes e recomenda-se que não tenham participado da construção dos códigos-fonte, garantindo mais imparcialidade. A tabela 5.5 e a figura 5.5 ilustram os procedimentos introduzidos na fase de testes.

Tabela 5.5: Fase de testes do guia proposto.

Atividades	**Tarefas**	**Papéis**	**Artefatos**
Testes de Segurança (**NIST**)	Revisão da superfície de ataque (**SDL**) Teste de segurança (**NIST**) Teste das funcionalidades básicas do WS	Planejador de testes Testador	Scripts dos testes Resultado dos testes
Testes de funcionalidades	Teste das funcionalidades do UDDI Teste da capacidade intermediaria do SOAP Realizar análise dinâmica do código (**SDL**)	Planejador de testes Testador	Códigos dos usuários Scripts dos testes Resultado dos testes
Testes de integração	Teste de conformidade com o WS-I Realizar os testes de interoperabilidade baseados em cenários variados Realizar os testes de integração baseados em cenários variados	Planejador de testes Testador Administrador dos testes de sistema	Códigos dos usuários Scripts dos testes Resultado dos testes
Testes no sistema	Checar as funcionalidades do sistema e o tempo de resposta com cargas variadas Checar as funcionalidades do sistema e o tempo de resposta de diferentes combinações de requisições válidas ou inválidas	Planejador de testes Testador Administrador dos testes de sistema	Códigos dos usuários Scripts dos testes Resultado dos testes
Testes de aceitação do usuário	Realizar os testes de aceitação do usuário	Administrador dos testes de	Códigos dos usuários

	sistema	Scripts dos testes
	Usuário	Resultado dos testes
	Gestor de testes	

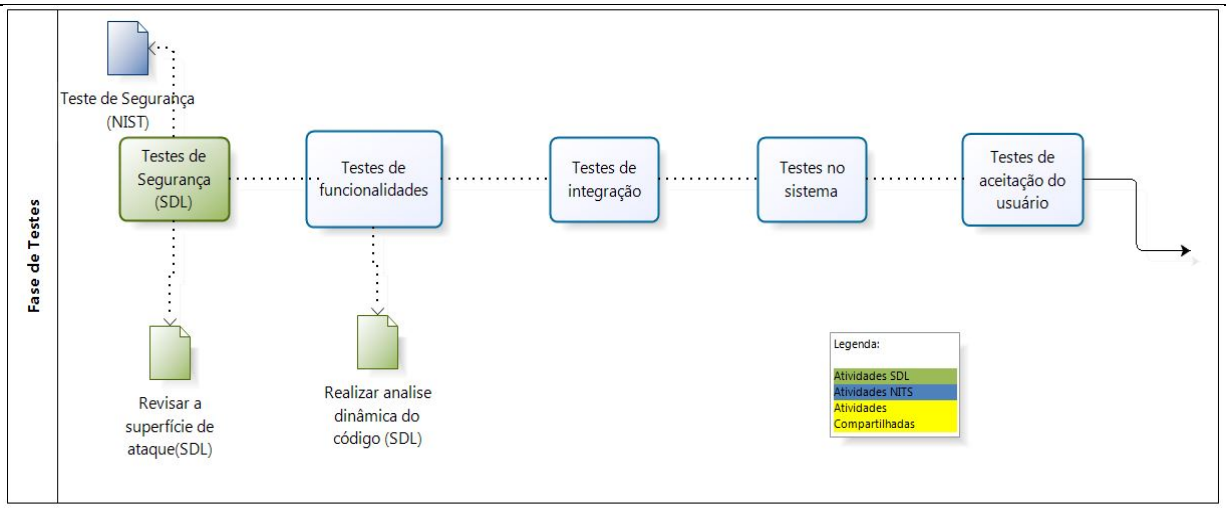

Figura 5.5. Fluxograma da fase de teste do guia proposto.

5.6 FASE DE IMPLANTAÇÃO

A fase de implantação realiza atividades para autorizar e liberar o sistema criado e para assegurar que a aplicação está segura, as tarefas foram adicionadas na atividade de teste de implementação. A revisão final de segurança é executada não com o objetivo de avaliar profundamente a segurança ou alcançar expectativas de segurança que foram ignoradas, mas verificar o que foi implementado, como as saídas do sistema, a qualidade de serviço e se existem pendências e exceções para gerar um veredito da situação final. O sistema pode passar na avaliação, que passou em todas verificações; passar com exceções, significando que existem pendências para a próxima versão do sistema e que as questões de segurança foram alcançadas satisfatoriamente ou não ser aprovado, onde o especialista em segurança não pode aprovar e liberar a aplicação. (*MICROSOFT*, 2012)

De acordo com o NIST, também deve ser realizada uma avaliação e autorização do sistema, onde a autorização se baseia na análise de risco e nos testes, plano e avaliação de segurança e deve ser executada por uma agência oficial de segurança que certificará como um sistema seguro caso o mesmo passe na apuração da agência.

A tarefa adicionada na atividade de preparação do ambiente de implantação realiza as configurações de controle de segurança que são iniciadas de acordo com as recomendações dos fabricantes e com a orientação e especificação de implementação de segurança, para a subsequente integração, testes e avalições dentro do ambiente operacional.

Complementarmente, a documentação de segurança com os planos elaborados deve ser atualizada e armazenada para a utilização após a implantação do sistema.

A tabela 5.6 e a figura 5.6, em seguida, constatam a agregação das tarefas na fase de implementação.

Tabela 5.6: Fase de implantação do guia proposto.

Atividades	Tarefas	Papéis	Artefatos
Preparar ambiente de implantação	Configurar e iniciar hardware Configurar e iniciar software Verificar/configurar controles operacionais (**NIST)**	Engenheiro de sistemas Conselheiro de segurança Desenvolvedores Analistas	Lançar notas
Implantar o WS	Determinar a URL do serviço Preparar o Script de Implantação Implantar WS Criar WSDL	Desenvolvedor	Arquivo WSDL Script de Implantação
Testes de Implantação	Criar ou reusar o código de usuário Criar WS com o código de usuário Revisão, avaliação e autorização final da segurança e do sistema (**SDL/NIST**)	Testador	Códigos dos usuários Autorização de implantação
Criar material de suporte para os usuários finais	Criar o material de suporte	Desenvolvedor	Guia de interoperabilidade Guia do usuário Serviços On-line Tutoriais Material de treinamento Documentação de segurança (**NIST)**
Publicar WS	Identificar o registro UDDI para a publicação Preparar a informação para a publicação Publicar no registro UDDI Realizar pesquisa com palavras-chave depois de realizar a publicação	Desenvolvedor	Nenhum

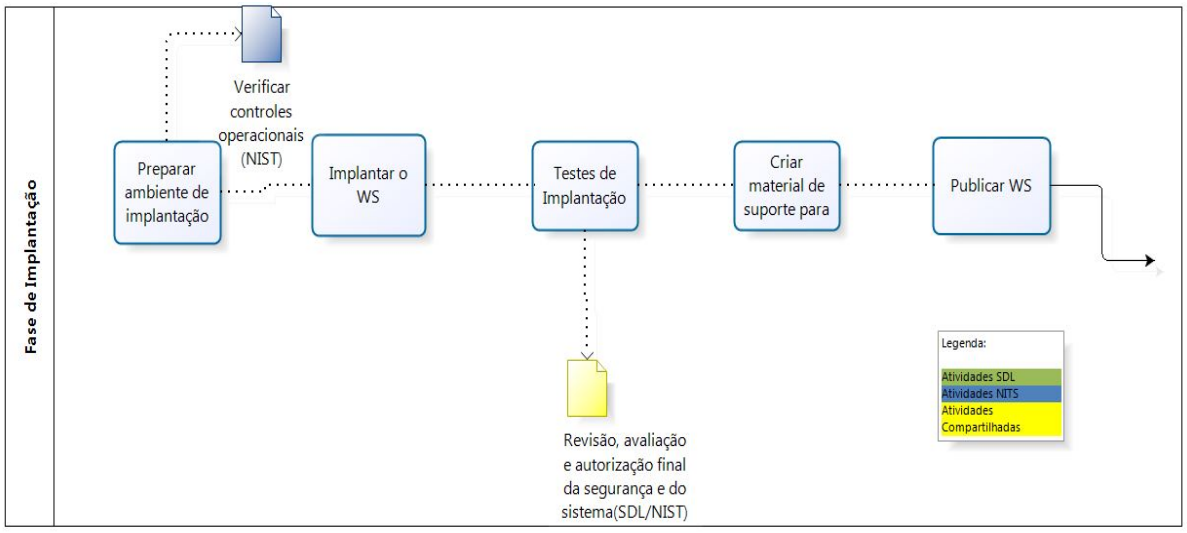

Figura 5.6. Fluxograma da fase de implantação do guia proposto.

5.7 CONSIDERAÇÕES FINAIS E RESULTADOS

Após a liberação e conclusão do sistema, recomenda-se realizar um monitoramento durante a operação e utilização do produto, a fim de verificar se o comportamento do serviço está adequado ás necessidades para o cliente. Este monitoramento deve ser baseado no plano de monitoramento contínuo produzido. As modificações e manutenções devem ser priorizadas, administradas, analisadas, implementadas e testadas antes de serem incluídas no produto, para manter parâmetros de qualidade de serviço, interoperabilidade e segurança. Para um melhor entendimento de como gerenciar a operação, manutenção e descarte do sistema, o documento NIST SP 800-64 possui duas fases que não foram exploradas nesse trabalho, mas que auxiliam nessa etapa do projeto.

Ao final da construção foram complementadas atividades, tarefas e artefatos as fases do guia com a seguinte distribuição:

- Fase de requisitos: uma atividade, seis tarefas e dois artefatos.
- Fase de análise: uma atividade, sete tarefas e um artefato.
- Fase de design: duas atividades, sete tarefas e um artefato.
- Fase de codificação: três tarefas.
- Fase de testes: uma atividade e três tarefas.
- Fase de implantação: duas tarefas e um artefato.

A figura 5.7, ilustra a distribuição das adições realizadas neste capítulo.

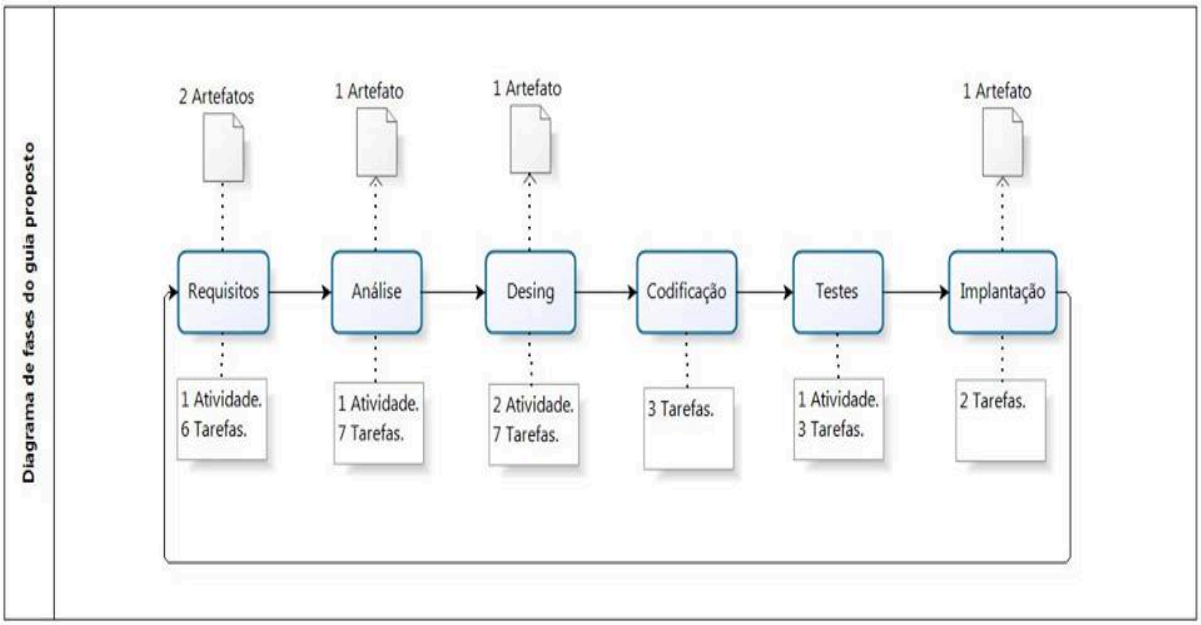

Figura 5.7. Processo de atividades do guia proposto.

As complementações no modelo de desenvolvimento de Web Services proposto pela OASIS tornou-o mais robusto e consistente nos aspectos que tangem a segurança da informação, onde em todas as fases foram adicionados procedimentos que agregam proteção tanto para o desenvolvimento do Web Service como para a própria arquitetura interna. As práticas e atividade do NIST e *Microsoft* SDL foram analisadas para verificar se eram adicionadas a uma fase, como uma atividade nova ou como uma tarefa nova, dependendo do seu grau de importância e nível de detalhamento. Algumas tarefas foram agrupadas para formar uma nova atividade ou apenas inseridas em atividades já existentes. Parte das atividades foram consideradas pertencentes a atividades ou tarefas já existentes e forma mapeadas para a mesma, no entanto não foi retratado nas análises explicitamente. Os artefatos foram adicionados de acordo com o que foi considerado mais relevante. Cada fase do guia recebeu uma tabela e um fluxograma, totalizando seis tabelas e seis fluxogramas, que esclarecem a análise realizada.

Esta análise demonstrou que a complementação de procedimentos de segurança no modelo original de desenvolvimento de sistemas do OASIS, possibilitou abordagens de proteções e de segurança no ciclo de vida do projeto. Verificamos que as atividades que receberam mais agregações foram as iniciais, onde o planejamento é mais contemplado, exigindo trabalho e conhecimento de gestores, analistas e arquitetos. Essas fases são essenciais para o bom andamento do projeto e para a certificação da segurança na implementação e na estrutura de um Web Service. As atividades de planejamento da segurança tanto na etapa de requisitos como na de análise, em conjunto com as atividades de

extração e gerencia de requisitos são fundamentais para a elaboração de uma arquitetura confiável que esteja conforme os requisitos e expectativas de segurança demandadas pelos clientes e usuários. A determinação das necessidades de Web Service da fase de requisitos, agregada à análise de risco da fase seguinte e a criação da documentação de segurança na etapa de design, fornecem um processo consistente para a estratégia de negócio onde são contextualizados os escopos e limites do sistema para a identificação e avaliação das ameaças e vulnerabilidades, com o objetivo de criar planos de segurança que garantam a continuidade do negócio após a construção do sistema.

A definição da arquitetura de segurança da fase de design, produz os controles de segurança que são utilizados juntamente com as ferramentas e funções recomendadas e com os resultados da análise da superfície de ataque e da modelagem de ameaças, para auxiliar nas considerações de implementação segura, fornecendo as informações necessárias para o codificador desenvolver os códigos do Web Service corretamente e protegê-los de possíveis ataques. Os resultados dos testes de segurança, de funcionalidade, de integração e de aceitação do usuário permitem que o sistema seja revisado quanto ao seu comprometimento com a sua finalidade e a qualidade de serviço, baseada no planejamento de qualidade, submetendo-se à avaliações finais que providenciarão a autorização da operação do Web Service e a certificação de segurança da aplicação. A análise dos procedimentos adicionados ao modelo original do OASIS, oferece um processo de desenvolvimento de Web Services compromissado com a segurança da informação, as expectativas de negócio, as estratégias de implementação segura e a comprovação do bom funcionamento e da proteção do sistema.

6 CONCLUSÃO

O estudo realizado enfocou no tratamento de segurança de Web Services, a fim de verificar os padrões de segurança que são recomendados para os desenvolvedores de Web Services e propor um guia de recomendações com práticas de segurança da informação para a implementação de Web Services voltada para a APF. Para alcançar esse objetivo foi realizada uma revisão bibliográfica, um estudo exploratório e uma análise documental comparativa.

Com a revisão dos principais conceitos de segurança da informação, de Web Services e de segurança aplicada a Web Services, verificamos que a segurança da informação apresenta para cada nova tecnologia desafios que devem ser solucionados ou mitigados para a continuação da evolução dos serviços prestados pela *Internet.* As tecnologias de ambientes distribuídos progridem para gerar informações e serviços mais rapidamente e com custos menores de implementação, que são aspectos presentes na abordagem de Web Services. A segurança para Web Services considera diversas dimensões de aplicação da segurança e possui vários padrões que especificam como deve ser implementada e os conceitos de segurança em um Web Service. Entretanto, deve ser complementada com outros processos de gestão de segurança como a gestão de risco e o desenvolvimento seguro de sistemas.

Na pesquisa exploratória das principais recomendações de segurança de TI elaboradas pela APF, apuramos que a mesma possui variadas recomendações relacionados a tecnologia da informação e a segurança da informação, assim como diversas entidades que coordenam e gerenciam os recursos de TI no governos federal, que aconselham a utilização de Web Services para determinados serviços. Mesmo com guias de boas práticas de segurança da informação como e-PING, que referencia documentos e especificações de entidades e organizações internacionais não traduzidos, verificamos a carência de modelos nacionais de desenvolvimento seguro de Web Service e outras tecnologias que surgiram nas últimas décadas.

A análise realizada no documento OASIS Web Service *Implementation Methodology* apresentou um modelo focado no desenvolvimento de Web Services baseado em modelos ágeis de construção de software, possuindo seis fases no total e diversas atividades e tarefas. As atividades e tarefas são centralizadas nas necessidades de negócio como a gerência de requisitos e a determinação das necessidades, na funcionalidade como os testes de aceitação do usuário e de funcionalidades, de implementação como a seleção da plataforma tecnológica e a elaboração dos códigos fonte do usuário e nas características de um Web Service como a seleção de Web Services reutilizáveis e das interfaces, a definição da granularidade e a

publicação do serviço no UDDI. No entanto apresentou poucas informações relativas a segurança da informação. O modelo de ciclo de vida de desenvolvimento seguro da Microsoft, apresenta procedimentos de alto e baixo nível que auxiliam na garantia de implementação e projeto de maneira segura, onde são expostas cinco fases com três atividades em cada uma delas e mais uma para o treinamento. O último documento analisado foi o guia de recomendações de segurança no ciclo de vida do desenvolvimento de sistemas criado pelo NIST (NIST, 2008), que apresenta atividade de alto nível de segurança da informação e assim como o comprometimento com os objetivos da organização que deseja criar a aplicação. Possui ainda cinco fases com diversas atividades, porém nesse trabalho foram consideradas apenas as três primeiras. O documento é apoiado por diversos outros documentos do NIST, que fornecem os detalhamentos das atividades propostas.

O resultado alcançado no último capítulo desse trabalho foi o guia de desenvolvimento seguro de Web Services, sendo recomendadas seis fases para o ciclo de vida de desenvolvimento, que está de acordo como o documento de implementação de Web Services proposto pela OASIS (OASIS, 2005), descrito na seção 4.1, que receberam cinco novas atividades, 28 tarefas, cinco artefatos distribuídos entres as etapas do guia que complementaram o modelo original e um diagrama de atividades demonstrando a organização final das recomendações. Além disso cada fase herdou uma tabela e um fluxograma contendo as informações adicionadas, para ilustrar e representar as alterações.

As recomendações da fase de requisitos são a iniciação do planejamento de segurança que identifica o especialista e as responsabilidades de segurança da equipe, conscientiza os *stakeholders* com determinação dos critérios de segurança e a categorização da informação. Após extrair os requisitos e determinar as necessidades do sistema, cria-se um planejamento de qualidade determinando os níveis aceitáveis de performance, segurança, dentre outros. Em seguida, a fase de análise recomenda a atividade de análise risco, onde seus processos estão conforme a norma ABNT NBR ISO/IEC 27005:2011, a exceção da prática de modelagem de ameaças fornecida pelo modelo do SDL (*MICROSOFT*, 2012), que analisa mais detalhadamente os riscos mais relevantes. A verificação de riscos compartilhados é uma recomendação na atividade de identificação dos Web Services reutilizáveis, para descobrir a existência de algum componente inseguro de terceiros. A tarefa de planejar a estrutura de segurança de Web Services recomenda a fundamentação da arquitetura com base na figura 2.6 da seção 2.7 deste trabalho.

Na fase de design é definida a estrutura da segurança de Web Services, que deve ser precedida da revisão de requisitos e dos critérios criptográficos, pois mudanças são comuns durante o projeto. A análise de superfície de ataque e a criação dos controles de segurança

auxiliam na implementação segura da aplicação. A segunda recomendação desta fase é a atividade de criação da documentação de segurança, que consiste na elaboração dos planos de monitoramento contínuo, de configuração e de contingência e continuidade de negócio, que ajudam no bom funcionamento do sistema nos casos de falhas e desastres.

A fase codificação recebe apenas as tarefas de utilizar ferramentas e funções seguras, que protegem os códigos elaborados pelo desenvolvedor e a tarefa de análise estática do código, que permite validação rápida e consistente do mesmo. Na fase de testes, é realizada a revisão da superfície de ataque e da ameaça, a fim de verificar se a codificação foi bem executada, e os testes de segurança que foca nos requisitos mais importantes, na repetitividade e na iteratividade. A recomendação da análise dinâmica do código contém o teste com estradas improváveis, forçando um comportamento atípico do sistema.

Por fim, a fase de implantação recomenda a verificação dos controles operacionais do ambiente de operação, iniciando-o e configurando-o. A última recomendação é a realização de uma revisão final da segurança e do sistema, que serão avaliados pelo especialista de segurança ou por um órgão externo, para ser aprovada ou não a liberação e operação do sistema. Depreende-se do resultado da análise das recomendações que as atividades e tarefas de fases distintas estão relacionadas formando processos paralelos que fornecem diferentes benefícios como a segurança informação da arquitetura de Web Service, a implementação segura, a conformidade com as funcionalidades e a superação da expectativa de negócio.

A proposta de recomendação de um guia de implementação de Web Service seguro, de acordo com os padrões da OASIS e também padrões de desenvolvimento de softwares seguros, que atendam as necessidades atuais e futuras da Administração Pública Federal brasileira, dentro do contexto de Web Services, foi o resultado final da pesquisa. Entretanto, não foi elaborado um modelo formal de desenvolvimento de software com diagramas de fluxo de atividades com especificações bem definidas e relacionadas, assim como não foram considerados todos os elementos do documento do NIST SP 800-64, como as interdependências e sincronizações.

Concluímos que a segurança da informação é essencial para o desenvolvimento e operação de Web Services e por ter componentes distribuídos torna sua efetivação complicada, por isso deve ser embasada nos padrões internacionais que mantém as pesquisas e inovações atualizadas para a indústria e usuários, além de outros procedimentos de gestão segurança da informação como a análise de risco e a implementação segura. Verificamos na APF a necessidade de recomendações mais sucintas na abordagem de Web Services, o que incentivou a pesquisa dentro dos modelos internacionais de desenvolvimento de sistemas e de Web Services, com a intenção de elaborar uma sugestão de implementação segura de Web

Services para o governo brasileiro, que foi a contribuição final alcançada ao término deste trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. NBR ISO/IEC 27001 - **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação** – Requisitos. Rio de Janeiro: ABNT, 2006.

ABNT. NBR ISO/IEC 27002 - **Tecnologia da informação: código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005.

ABNT. NBR ISO/IEC 27005 - **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. Rio de Janeiro: ABNT, 2011.

BRANDÃO, José Eduardo Malta de Sá – **Gestão de risco de segurança aplicada a Web Services** - OWASP – 2009.

BRASIL, **Boas práticas de segurança da informação**, TCU 4ª edição. Secretaria de Fiscalização de Tecnologia da Informação, 2012.

BRASIL, **Cartilha de Segurança para Internet, versão 4.0 / CERT.br** – São Paulo: Comitê Gestor da Internet no Brasil, 2012.

BRASIL, Cartilha técnica SLTI. **Guia de interoperabilidade, Brasília** 2013.

BRASIL, **Guia de Orientação para Implementação de Web Services** disponível em http://www.governoeletronico.gov.br/anexos/guia-de-orientacao-para-implementacao-de-web-services/view Acesso: Setembro de 2013.

BRASIL, Ministério de Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação. **Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação.** V 1.1, Brasília, 2011.

BRASIL, Ministério do Planejamento Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação. Departamento de Serviços de Rede. **Guia de referencia para a segurança da informação usuário final.** Brasília, 2005.

BRASIL, **Norma Complementar** IN-GSI/PR nº 1 de 15 de Outubro de 2008.

BRASIL, Presidência da Republica. Casa Civil. **Decreto nº 3.505** de 13 de Junho de 2000.

BRASIL, Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde : segurança cibernética no Brasil** – Brasília, 2010.

BRASIL, **Sistema de administração de recursos de tecnologia da informação – SISP**. Sítio: http://www.governoeletronico.gov.br/sisp-conteudo Acesso: setembro de 2013.

BRASIL, Sumários Executivos. **Auditoria nos Sistemas de Informação do Diário Oficial da União**. Brasília, 2010.

BREITMAN, K.K - **Web Semântica: a internet do futuro** – 2005.

BRINHOSA, Rafael Bosse **WSIVM: modelo de validação de entradas de dados para Web Services.** Florianópolis, 2010.

CHASE, Nicholas - **Entendendo Especificações de Serviços da Web** - http://www.ibm.com/developerworks/br/Web Services/tutorials/ws-understand-web-services4/: IBM Acesso: Setembro de 2013.

DINIZ, Flávio Luiz Ribeiro. **Avaliação preliminar da gestão de segurança da informação em duas organizações públicas**. Brasília : UnB, 2009.

FERNANDES, Jorge Henrique Cabral - **Gestão da segurança da informação e comunicações** v1 / - Brasília :Faculdade de Ciência da Informação, c2010.

FRANZOSI, Ednylton Maria - **Uma Proposta de Arquitetura Referencial SOA para Desenvolvimento de Sistemas para o Governo**. Rio de Janeiro, 2009.

FRANZOSI , Ednylton Maria, GARCIA, Ana, RODRIGUES, Sérgio Assis, BLASCHEK, José Roberto, SOUZA, Jano Moreira de - **Uma Proposta de Arquitetura Referencial SOA para Desenvolvimento de Sistemas para o Governo.** Disponível em http://www.lbd.dcc.ufmg.br/colecoes/wcge/2009/004.pdf Acesso: Setembro de 2013.

GUALBERTO, Éder Souza – **Um estudo de caso sobre a gestão da segurança da informação em uma organização pública**. Brasília: UnB, 2010. ISBN.

HARTMAN, B; FLINN, D.J; BEZNOSOV, K; KAWAMOTO, S - ***MAstering Web Services Security***, 2003 ISBN-10: 0471267163 primeira edição.

IBM, International Business Machines - **Web Services Conceptual Architecture** (WSCA 1.0) – 2001.

IBM, International Business Machines - **RESTful Web services: The basics –** 2008.

KIM, Y.J. – ***Access Control Service Oriented Architecture Security*** – Artigo - 2009

MATHIAS-PEREIRA, J**. Manual de Metodologia de Pesquisa Científica** (NBR 6022/2003). 3 ed. São Paulo: Atlas, 2012.

MICROSOFT, *Security Fundamentals for Web Services* **http://msdn.microsoft.com/en-us/library/ff648318.aspx** Acesso: Setembro de 2013.

MICROSOFT, ***Microsoft Security Development Lifecycle Process*** 5.2 – 2012.

NIST, ***National Institute of Standards and Technology Special Publication 800-95*** (Aug. 2007)

NIST, ***National Institute of Standards and Technology Special Publication 800 -30*** (July 2002)

NIST, ***National Institute of Standards and Technology Special Publication 800-64*** (Oct. 2008).

OASIS, ***Web Services Implemetation Methodology*** – 2005.

OASIS, ***Web Services Security SAML Token Profile Version 1.1.1****, 8 May 2012*.

OASIS, ***Web Services Security: SOAP Message Security 1.1 (WS-Security 2004). OASIS Standard Specification****, 1 February 2006.*

ORACLE, ***Understanding Web Services Security Concepts*** http://docs.oracle.com/cd/E17904_01/web.1111/b32511/intro_security.htm Acesso: Outubro de 2013.

SANTOS, C.A. **Segurança em Web Services** – Mestrado em Sistema de Dados e Processamento Analítico. Brasil, 2008.

SCHNEIER, B. ***Applied Cryptography***. Ed. John Wiley & Sons, 2nd Edition, 1996.

SILVA, L.R.C; DAMACENO, A.D; MARTINS, M.C.R; SOBRAL, K.M; FARIAS, I.M.S – **Pesquisa Documental: alternative investigative na formação docente**.- 2009.

STALLINGS, ***W. Cryptography and Network Security*** – 4º Edição - New Jersey – 2008.

TANENBAUM, A.S. ***Computer Network*** – 4º Edição - Amsterdam – 2003.

WATHIER, A.J. **Segurança em Web Services com WS-Security** – Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre - 2005.

W3C, Working Group Note **www.w3.org/TR/xkms/** Acesso: Setembro de 2013.

W3C, Working Group Note ***Web Services Architecture*** http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/ Acesso: Setembro de 2013.