Ministério da Justiça

UnB

Centro de Apoio ao Desenvolvimento Tecnológico

latitude
Laboratório de tecnologias da tomada de decisão

Termo de Cooperação/Projeto:

Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Replanejamento e Novo Projeto Piloto

Documento:

RT - Diretrizes em Segurança da Informação

Data de Emissão:

15/05/2015

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Marivaldo de Castro Pereira
Secretário Executivo

Helvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

EQUIPE TÉCNICA
Ana Maria da Consolação Gomes Lindgren
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Elaine Fabiano Tocantins
Fernando Saliba Oliveira
Fernando Teodoro Filho
Guilherme Braz Carneiro
Joaquim de Oliveira Machado
José Alberto Sousa Torres
Marcelo Martins Villar
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alysson Fernandes de Chantal
Amanda Almeida Paiva
Andréia Campos Santana
Antônio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Caio Rondon Botelo de Carvalho
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Diogenes Ferreira Reis Fustinoni
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Heverson Soares de Brito
Johnatan Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antônio de Souto Evaristo
Luiz Claudio Ferreira
Marcos Vinicius Vieira da Silva
Marco Schaffer
Pedro Augusto Oliveira de Paula
Roberto Mariano de Oliveira Soares
Sandro Augusto Pavlik Haddad
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martins
Vera Lopes de Assis
Wladimir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
01/08/2014	0.1	Versão Inicial – Segurança Física
04/08/2014	0.2	Adaptações e Correções de Estrutura – Segurança Física
06/08/2014	0.3	Inserção e Revisão – Segurança Física
07/08/2014	0.4	Modificação Estrutural – Segurança Física
28/08/2014	0.6	Analise de Itens de Contrato – Segurança Física
18/08/2014	0.5	Analise das Normas ABNT – Segurança Física
31/08/2014	1.0	Conclusão – Segurança Física
10/09/2014	1.1	Reestruturação – Segurança Física
20/09/2014	1.2	Acordos de Níveis de Serviço – Segurança Física
13/10/2014	1.3	Revisão Inicial – Segurança Física
01/12/2014	1.4	Versão Inicial – Desenvolvimento Seguro
30/12/2014	1.5	Ciclo de Vida de Desenvolvimento de *Software*
05/01/2015	1.6	Normas e Modelos de Segurança – Desenvolvimento Seguro
10/01/2015	1.7	Modelos de Maturidade para Segurança de *Software* – Desenvolvimento Seguro
12/01/2015	1.8	Atividades de Acordo com Modelo de Maturidade BSIMM
20/01/2015	1.9	Requisitos – Desenvolvimento Seguro
07/02/2015	1.9	Considerações Finais – Desenvolvimento Seguro
08/02/2015	1.9	Revisão – Desenvolvimento Seguro
20/02/2015	1.9	Revisão Técnica – Desenvolvimento Seguro
01/03/2015	2.0	Versão Inicial – Protocolo de Comunicação Segura
10/03/2015	2.1	Atualização – Protocolo de Comunicação Segura
15/03/2015	2.2	ePING Adicionado – Protocolo de Comunicação Segura
28/03/2015	2.3	Políticas Técnicas – Protocolo de Comunicação Segura
15/04/2015	2.4	Revisão – Protocolo de Comunicação Segura
20/04/2015	2.5	Finalização de Versão – Protocolo de Comunicação Segura
01/05/2015	2.6	Revisão por Rodrigo Borges – Protocolo de Comunicação Segura
10/05/2015	2.7	Revisão e Finalização – Protocolo de Comunicação Segura
15/05/2015	3.0	Finalização do Documento para Revisão

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

SUMÁRIO

1 INTRODUÇÃO

Certo de que o Projeto RIC visa aperfeiçoar o sistema de identificação e individualização do cidadão brasileiro nato e naturalizado com vistas a um perfeito funcionamento da gestão de dados da sociedade, agregando valor à cidadania, à gestão administrativa, à simplificação do acesso aos serviços disponíveis ao cidadão e à segurança pública do país, o termo de cooperação entre MJ/SE e FUB/CDT define um projeto que objetiva identificar, mapear e desenvolver parte dos processos e da infraestrutura tecnológica necessária para viabilizar a implantação do número único de Registro de Identidade Civil – RIC no Brasil.

Neste contexto, e em consonância com os resultados de um subconjunto das atividades previstas no termo de cooperação, o principal objetivo deste relatório técnico é fornecer requisitos funcionais e não funcionais em segurança da informação que irão compor o Termo de Referência para contratação das empresas que irão operacionalizar a infraestrutura tecnológica do Sistema Nacional do Registro de Identificação Civil.

O presente relatório contempla a análise da segurança da informação sobre três aspectos: Segurança Física, Recomendações de Segurança da Informação para desenvolvimento de *softwares* e Políticas e Recomendações Técnicas e Operacionais para Protocolo de Comunicação Segura.

2 SEGURANÇA FÍSICA

O aspecto da Segurança Física engloba os requisitos de segurança relacionados ao espaço físico e à infraestrutura necessários para a instalação, hospedagem e operação de equipamentos de infraestrutura tecnológica sob condições determinadas. Abrange, dentre outros elementos, infraestrutura, piso elevado com fornecimento de energia elétrica estabilizada e redundante, climatização, sistema de prevenção e extinção de incêndio, alta disponibilidade, rede lógica e física, segurança física e monitoramento ininterrupto, entre outros. Esses elementos permitem o funcionamento dos equipamentos abrigados, observadas as características pré-estabelecidas, normas, padrões nacionais e internacionais e acordos de níveis de serviços (*Service Level Agreement* – SLA).

Na contratação do parceiro responsável pela hospedagem da Solução Tecnológica do RIC, devem ser levados em conta, em relação a segurança física, especificações e condições técnicas pré-estabelecidas, os acordos de Níveis de Serviço, a descrição dos serviços de manutenção técnica e "condominial", a solicitação da infraestrutura necessária, o tempo de locação e o valor total do contrato.

Os acordos de níveis de serviço são partes integrantes do contrato, compatíveis e coerentes com a especificidade de um *datacenter* de total segurança e disponibilidade, pelo qual o parceiro contratado se obriga a manter determinados níveis de serviços visando permitir o perfeito funcionamento dos equipamentos do **contratante**.

Já a descrição dos serviços de manutenção técnica e "condominial" tratam sobre a manutenção da infraestrutura predial e eletromecânica necessária ao funcionamento ininterrupto dos equipamentos alocados pela **contratante** nas áreas que lhe forem destinadas. Esses serviços compreenderão, de modo abrangente, a operação e a manutenção da infraestrutura predial e eletromecânica, vigilância, brigada de incêndio, limpeza, além de toda a estrutura administrativa predial, como recepção, portaria etc.

Esse relatório tem como base os seguintes contratos e editais.

- Contrato de Prestação de Serviço n° 2008/8558-0569 – Serviços de *Colocation* Site Alternativo – entre o Banco do Brasil S.A. e o Serviço Federal de Processamento de Dados – SERPRO.
- Contrato Padrão de Prestação de Serviços de *Colocation* da Global Village Telecom Ltda (GVT).

- Edital de Licitação (Pregão Eletrônico n° 22/2013) do Ministério do Planejamento, Orçamento e Gestão para contratação de empresa especializada para o fornecimento e instalação de solução de ambiente seguro de *datacenter* nas dependências do Ministério.
- Contratação Direta nº 059/10/PDPE da Procuradoria-Geral do Estado do Rio Grande do Sul.
- Contrato de Prestação de Serviços nº 013/2011/FERMP do Ministério Público do Estado de Santa Catarina.
- Processo de Compra nº RJ-2013-9991 (Edital do Pregão Eletrônico Nº 30/2013) da Comissão de Valores Mobiliários.
- Minuta do Termo de Referência do documento de Planejamento de Contratação de Bens e Serviços de TI da Agência Nacional de Telecomunicações (Anatel).

Foram escolhidos estes contratos e editais, pois se assemelham em características, capacidades e porte ao pretendido pelo Sistema Nacional do Registro de Identificação Civil.

2.1 Glossário de acordos de nomenclaturas

Embora não seja a escolha de todos os contratos analisados, o significado de cada item ou palavras usadas no contrato, como “equipamentos”, “acordos de níveis de serviços”, “nomenclaturas” e “adendos de contrato”, chama a atenção pela transparência obtida com uma descrição simples e objetiva de cada uma delas, descritas em ordem no início do contrato.

Ao tratar sobre os equipamentos, por exemplo, os contratos referem-se a qualquer bem como servidores, *switches*, roteadores de rede, unidades de *backup*, sistemas operacionais, *softwares*, dentre outros, de propriedade do cliente ou sob sua responsabilidade. A relação de anexos do contrato também é estabelecida, geralmente nas primeiras páginas, para garantir a concordância de todas as especificações.

2.2 Obrigações do Parceiro Tecnológico

Nos itens declarados para listar as diversas obrigações da **contratada**, há menção a

obrigações fiscais, trabalhista, técnicas e profissionais. Essas obrigações abrangem os seguintes aspectos: obras, infraestrutura, sala-cofre ou sala segura, acesso da **contratante**, cumprimento dos acordos de níveis de serviço, investimentos em tecnologia e manutenção, capacitação de pessoas, manutenção etc.

Entre as obrigações mais básicas, podemos citar:

- responsabilizar-se integralmente pela prestação dos serviços, ainda que os mesmos sejam prestados através de subcontratadas ou coligadas;
- resguardar, conservar e manter a infraestrutura em que se encontrem os equipamentos;
- prestar os serviços conforme contratado, devendo observar os níveis de serviço acordados;
- prestar esclarecimentos ao cliente, livre de ônus, considerando eventuais reclamações e dúvidas relativas à fruição dos serviços;
- manter a confidencialidade das informações fornecidas ou obtidas junto à outra parte, sejam estas classificadas como “informações confidenciais” ou não, abrangendo, inclusive, quaisquer informações cadastrais de contratantes e/ou fornecedores, estratégias de negócios, produtos em desenvolvimento, dados financeiros e estatísticos, negociações em andamento, senhas etc.;
- manter as condições de habilitação e qualificação exigidas durante toda a vigência do contrato estabelecido;
- não ceder ou transferir, total ou parcialmente, parte alguma do objeto contratado;
- dar ciência, imediatamente e por escrito, de qualquer anormalidade que verificar na execução do objeto;
- manter sigilo absoluto sobre informações, dados e documentos provenientes dos fornecimentos e serviços realizados e, também, as demais informações internas;
- alocar profissionais devidamente capacitados e habilitados para a execução do objeto contratado;
- aplicar políticas de segurança de informação para atender aos requisitos de sigilo e segurança definidos pelo contrato;
- responder por eventuais problemas relacionados à execução dos serviços durante todo o período de contratual, solucionando-os conforme estabelecido no

2.2.1 Qualificações Técnicas

Este é um dos itens importantes do contrato e visa garantir que a empresa prestadora do serviço de hospedagem está comprovadamente apta a prover toda a gama de serviços envolvidos no contrato.

É imprescindível documentar a obrigatoriedade da **contratada** em possuir ambientes de *datacenter* (conhecido como sala-cofre ou sala segura) seguindo os padrões nacionais e internacionais, além de manter em seu quadro técnico-funcional especialistas em sistemas elétricos e eletrônicos de precisão.

A comprovação documental pode abranger todos os itens pertinentes aos serviços que serão prestados, no entanto, pode ser feita uma avaliação da criticidade de cada item e determinação das prioridades.

Poderá ser pedida também uma comprovação de experiência em manutenção de salas cofre de forma integral, abrangendo também todos seus subsistemas, como o subsistema de climatização, monitoramento, subsistema de provimento interrupto de energia e iluminação, sistema de detecção e combate a incêndios, controle de acesso, cabeamento estruturado etc.

A comprovação de experiência na execução dos serviços devem ser obviamente compatíveis com as características dos itens do contrato, como quantidades, porte, capacidade e prazos.

2.2.2 Especificações de Infraestrutura

A especificação completa de cada item não é obrigatória em um contrato deste tipo, porém é essencial detalhar, além dos itens mais críticos, aqueles que contêm especificações diferentes das normas técnicas padrões nacionais e internacionais ou possuam requisitos mínimos estabelecidos contratualmente. Neste caso, o detalhamento poderá ser constituído diretamente no contrato ou em forma de um Acordo de Nível de Serviço.

Caso seja necessário, o detalhamento de itens do contrato que possuem requisitos mínimos deve detalhar suas características o mais especificamente possível, já que este determinado item terá que ser cumprido. A seguir, alguns exemplos.

- Especificação de área útil (m²) a ser disponibilizada.
    - Definição de área útil total.
    - Definição de área útil para sala segura.
    - Definição de área útil para salas de segurança, telecomunicações, monitoramento, etc.
- Especificação da potência de KVA (*Kilovoltampere*) de energia elétrica a ser disponibilizada na infraestrutura.
- Especificação da capacidade de refrigeração em TR (toneladas de refrigeração) que a infraestrutura deverá possuir.

Deverá constar do contrato a descrição da obrigação da **contratada** com o perfeito funcionamento da infraestrutura disponibilizada, mas é opcional documentar a obrigação em possuir os seguintes intens.

- Sala segura e sala de telecomunicações.
- Sala de quarentena.
- Sala de *nobreaks*/UPS.
- Centro de monitoramento de redes ou NOC (*Network Operation Center*).
- Subsistema de climatização de precisão.
- Subsistema de climatização de Conforto.
- Subsistema de provimento interrupto de energia e iluminação.
- Subsistema de detecção e combate a incêndios.
- Subsistema de controle de acesso biométrico.
- Subsistema de monitoração ambiental e vigilância CFTV.
- Subsistema de cabeamento estruturado.
- Serviços de manutenção e suporte técnico *on-site*.

Pode-se também, se necessário, especificar os seguintes itens de infraestrutura.

- Sistemas de alimentação, transformação e geração de energia elétrica.
- Sistema de interligação redundante de energia.
- Especificação técnica da distribuição interna de energia elétrica.
- Sistema de energia ininterrupta.
- Sistema de condicionamento de ar.

- Sistema de supervisão predial.
- Sistema de segurança, incluindo vigilância eletrônica, controle eletrônico de acesso, monitoramento e detecção e extinção de incêndio.
- Pisos elevados e divisórias.
- *Racks*, caso haja.
- Interconexão de equipamentos e conexão usada.

2.2.3 Sistema ininterrupto de Energia Elétrica

A descrição abaixo, contendo algumas informações sobre o sistema de energia elétrica, foi escrito apenas como forma de garantir um conhecimento prévio sobre o assunto, antes de tratá-lo contratualmente.

O sistema elétrico de um *datacenter* é constituído pelo Sistema Ininterrupto de Energia UPS (*Uninterruptible Power Supply*). Ele tem a função de fornecer energia para todos os equipamentos de um *datacenter*, incluindo equipamentos de detecção, alarme de incêndio e segurança. É composto por conjuntos de *nobreaks*, contendo baterias, inversores e retificadores [20]. Os *nobreaks* redundantes, ligados em paralelo, irão assegurar o suprimento contínuo de energia, mesmo em caso de falha de transformadores ou a falta de energia elétrica [20]. As baterias são dimensionadas para garantir uma autonomia por um período mínimo de 15 minutos. Este tempo é suficiente para partida e conexão dos geradores a diesel em caso de falta de energia elétrica da concessionária [21].

O sistema de energia de emergência consiste de um grupo de geradores a diesel que entrarão em funcionamento e se conectarão ao sistema elétrico do *datacenter* automaticamente e os geradores precisam ser dimensionados para suportar todas as cargas necessárias ao funcionamento dos equipamentos durante uma possível falta de energia da concessionária.

Datacenters são, na sua essência, grandes aparelhos que consomem energia elétrica e produzem calor. O sistema de refrigeração do *datacenter* remove o calor gerado pelo consumo de energia – consumindo assim, mais energia no processo. Desta forma, não se pode estranhar que a maior parte dos custos de construção de um centro de dados deste porte sejam proporcionais à quantidade de energia fornecida e a quantidade de calor a ser removida. Em outras palavras, a maior parte do dinheiro é gasto tanto no condicionamento de potência e de distribuição, como em sistemas de refrigeração. Custos

de construção para um grande *datacenter* estão na faixa de US$ 10 - US$ 20 / Watts, mas variam consideravelmente, dependendo o tamanho, localização e *design* [30].

A Figura 3.1 abaixo, demonstra os principais componentes de um datacenter.

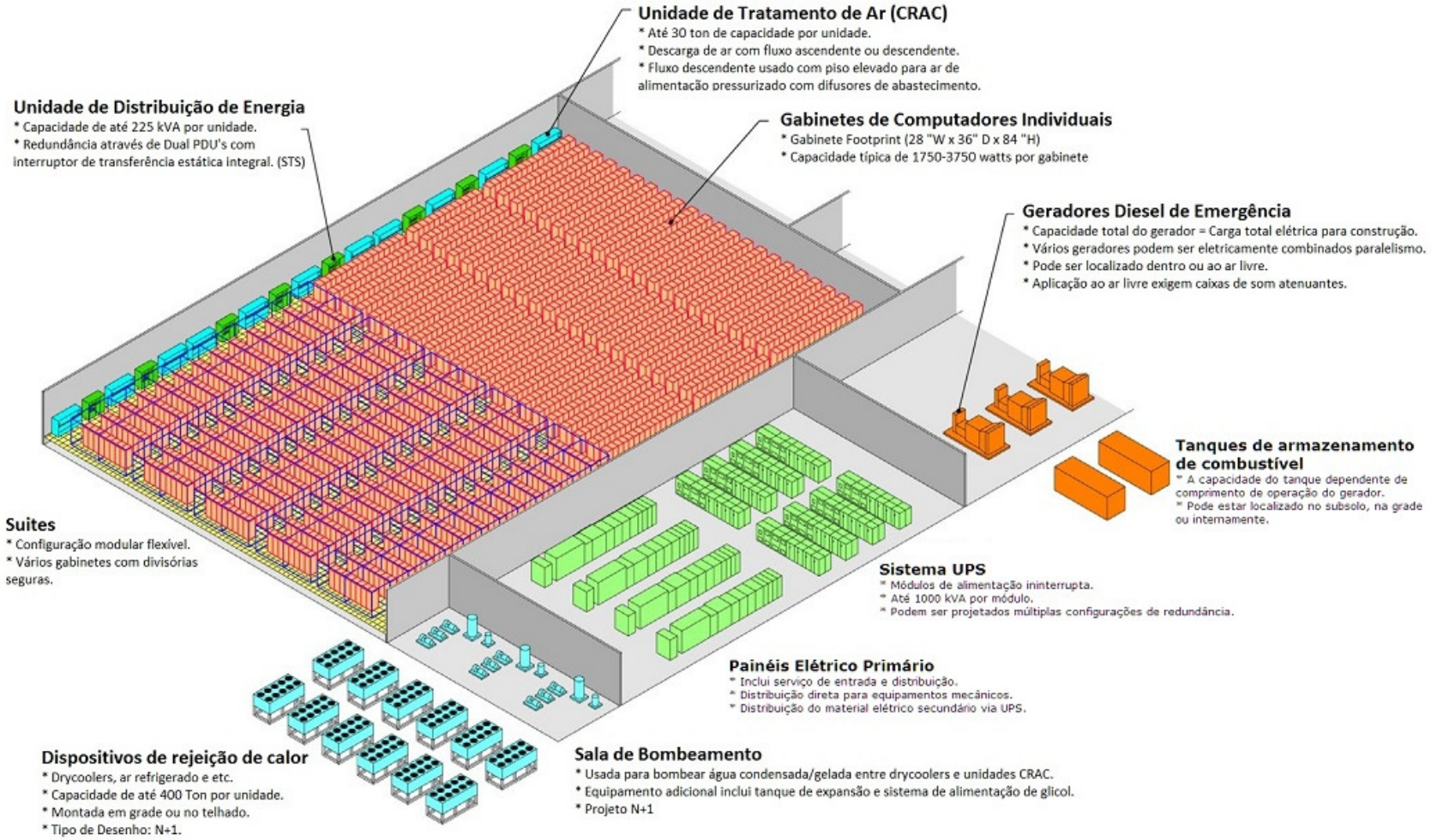

Figura 3.1: Os principais componentes de um típico *datacenter*. [30]

2.2.4 Sala-Cofre

A sala-cofre é um produto fabricado com tecnologia alemã pela empresa Lampertz GmbH & Co. [22]. No Brasil, a empresa Sismetal (http://goo.gl/zq9ebZ) é importadora e fabricante exclusiva dos produtos da Lampertz, sendo a Aceco TI [21] sua representante exclusiva para a distribuição, manutenção, assistência técnica e construção de sala-cofre.

A Sala-Cofre da Aceco TI é produzida no Brasil e é um ambiente estanque, testado e certificado, que protege o *datacenter* contra fogo, calor, umidade, gases corrosivos, fumaça, água, roubo, arrombamento, acesso indevido, sabotagem, impacto, pó, explosão, magnetismo e armas de fogo.

Segundo a norma NBR 11515 - Item 2.3, cofre e sala-cofre são definidos como um espaço delimitado que mantém um ambiente interno dentro de certas condições, mesmo quando sujeito a situações adversas, tais como incêndio e seus derivados (calor, vapor e gases), avarias mecânicas e demais riscos físicos.

Segundo a Associação Brasileira de Normas Técnicas - ABNT, a empresa Aceco TI é a única detentora no Brasil da Certificação ABNT NBR 15247 e seus Procedimentos de Certificação PE 047-1. Somente a ABNT está creditada pelo INMETRO para certificação de Salas Cofre.

Segundo a Aceco TI, o produto é o único que atende as recomendações da NBR 11515, NFPA 75 e NBR ISO IEC 27002 [17], sendo:

- testada integralmente de acordo com a NBR 15247 e EN 1047-2;
- certificada pela ABNT conforme o procedimento PE 047.01, devidamente acreditado pelo INMETRO para o escopo Sala-Cofre;
- certificada pelo ECB-S, devidamente acreditado pelo DAR para o escopo Sala-Cofre;
- possui estrutura autoportante, constituída de painéis de paredes, teto, elemento de fundo e estrutura auxiliar interna (vigas e pilares);
- é desmontável, realocável e expansível a qualquer momento, com um mínimo de interferência no ambiente de trabalho.

2.3 Aderência à Normas Técnicas

É interessante certificar-se de que o serviço ofertado pela empresa **contratada** atende não somente às normas técnicas e legais aplicáveis, mas também, a todas aquelas que representam as melhores práticas vigentes para cada item da solução.

A ABNT é o órgão responsável pela normalização técnica no país, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro. É uma entidade privada, sem fins lucrativos, reconhecida como único Foro Nacional de Normalização através da Resolução n.º 07 do CONMETRO, de 24.08.1992.

É também a única e exclusiva representante no Brasil das seguintes entidades internacionais: ISO (*International Organization for Standardization*), IEC (*International Electrotechnical Commission*); e das entidades de normalização regional COPANT (Comissão Panamericana de Normas Técnicas) e a AMN (Associação Mercosul de Normalização).

Segundo a ABNT, as normas que devem ser seguidas na construção de um *Datacenter* seguro e com proteção total contra sinistros, a fim de garantir a proteção e continuidade dos serviços informatizados, resulta da combinação de fatores físicos e ambientais que tem seus parâmetros previstos nas Normas ABNT NBR ISO/IEC 27002 [17], NBR 11515 e NBR 15247.

A NBR ISO/IEC 27002: Tecnologia da Informação – Técnicas de Segurança – é conhecida como uma norma para os códigos de práticas para gestão de segurança da informação e refere-se a quais requisitos devem ser implementados pela organização, sendo também um guia que orienta a utilização dos controles de segurança.

A ISO 27002 é baseada na BS 779-1:1999, essa é utilizada como documento de referência e fornece um conjunto completo de controles de segurança. Não é usada para auditorias e certificações, porém grande parte de seu *framework* está consistente em diversos alicerces de boas práticas de gestão em projetos, organização de processos e pessoas, assim como na metodologia de ferramentas adequadas.

A Certificação ABNT NBR 15247 (Unidades de Armazenagem Segura – Salas-Cofres e Cofres para *Hardware* – Classificação e Métodos de Ensaio de Resistência ao Fogo) que este relatório faz referência é uma norma brasileira utilizada para testar as Salas-Cofres. Ela define os critérios de testes, sendo a mais ampla certificação e o mais alto nível de

proteção de sala-cofre vigente no mercado.

A NBR 15247 foi elaborada no Comitê Brasileiro de Segurança contra Incêndio pela Comissão de Estudo de Salas-Cofres, cofres, armários e recipientes de proteção contra incêndios e passou a vigorar no Brasil 2005. Sendo certificado conforme esta norma, qualquer compartimento dá a certeza de que os equipamentos e dados contidos na sala-cofre estarão preservados contra sinistros e seus efeitos.

A ABNT NBR 11515:2007 – Critérios de segurança física relativos ao armazenamento de Dados fixa as condições ambientais exigíveis para os ambientes de *datacenter* e orienta a adoção de salas-cofres para a proteção de *hardware*, onde estabelece limites críticos de resistência destes equipamentos.

Ela também faz referência direta às ameaças a serem consideradas e informa que os riscos devem ser identificados através de uma análise de riscos dos ambientes onde as informações são geradas e armazenadas para fins operacionais e do local onde são guardadas as cópias de segurança (*back up*). Estes locais devem ser analisados levando em consideração, no mínimo, as seguintes ameaças.

a) Incêndio (dentro e fora do local) e suas consequências.

b) Explosão, considerada em relação ao ambiente externo.

c) Intempéries (raio, vendaval, granizo).

d) Água (vazamento, transbordamentos, derrame) e outros líquidos.

e) Impacto de veículos ou aeronaves.

f) falta de energia, curtos-circuitos, variações de tensão e outros eventos.

g) Atos ilícitos (roubo, assalto, desvio etc.).

h) Interrupção no fornecimento de utilidades ou distinção em sistema de climatização.

i) descarga eletrostática.

j) emissões eletromagnéticas (luz, raios-x, raios-gama).

k) campos magnéticos.

l) umidade, fungo.

m) roedores, insetos.

n) poeira.

o) vibração.

p) efeitos químicos.

q) disparo de armas de fogo.

Em complementação às normas descritas acima, a ABNT criou um programa de certificação de salas-cofres ABNT NI 09.113.01 que tem como base todas as exigências da NBR ISO/IEC 27002, NBR 11515 e NBR 15247.

Este procedimento de certificação foi desenvolvido para garantir ao consumidor que o produto adquirido proteja contra os riscos recomendados pela ABNTNBR ISO/IEC 27002 e as condições ambientais recomendadas pela ABNT NBR 11515, atendendo também a todas as especificações e requisitos das normas ABNT NBR ISO 9001, ABNT NBR 15247, ABNT NBR 5628, ABNT NBR 6118, ABNT NBR 10636, ABNT 10897, ABNT NBR IEC 60529, ASTM E779 E NFPA 2001, dentre outras.

Abaixo estão relacionados, como exemplo, algumas características e especificações técnicas mínimas que as sala-cofres devem prover. Estes itens não precisam estar relacionados no contrato, uma vez que estão implícitos nas certificações.

- Capaz de prover proteção contra fogo por, no mínimo 90 minutos, comprovada por certificação obtida a partir de ensaios normatizados, conforme norma ABNT NBR 10636 (classe CF90), similar ou superior, emitida por Organismo Certificador de Produto (OCP) acreditado pelo INMETRO. A resistência ao fogo deverá englobar os testes de isolamento térmico, estanqueidade (chamas e gases quentes) e estabilidade (choques) nos termos da referida norma.
- O piso, o teto e as paredes deverão ser adequados aos mecanismos do sistema de detecção e combate a incêndio, aos recursos do sistema de controle de acesso biométrico, aos recursos de climatização de precisão, aos recursos do sistema de vigilância e aos recursos do sistema de cabeamento estruturado lógico e elétrico do *datacenter*.
- A sala deverá possuir sistema de refrigeração com corredores de ar quente e ar frio, em conformidade com a norma ANSI/TIA 942 [24].
- Deverá ser provida de iluminação adequada dentro da sala, conforme padrão indicado na norma ANSI/TIA 942 [24].
- A sala deverá apresentar estanqueidade contra trocas gasosas com o ambiente externo, mantendo os parâmetros mínimos de renovação de ar estabelecidos na norma NBR 16401, norma similar ou superior.
- A sala deverá ser dotada de subsistema de monitoramento e controle do ambiente através de painel de monitoração.

- A porta de acesso deverá ser dotada de fechadura com travamento eletromecânico e acionamento automático por leitura biométrica de entrada, conforme Subsistema de Controle de Acesso Biométrico.

Desta maneira, podemos considerar que os métodos construtivos a serem utilizados, tais como equipamentos, materiais, dispositivos e serviços a serem fornecidos pela empresa **contratada**, bem como a execução propriamente dita da solução, deverão atender, no que for pertinente às suas respectivas finalidades e aplicações, ao estabelecido nos padrões e normas.

2.3.1 *Datacenters*

Como é explicado em Romer [12], assim como grande parte dos serviços oferecidos no mercado, *datacenters* também possuem uma classificação própria indicando quão preparados estão para lidar com problemas e quão sólidas são suas infraestruturas.

A norma ANSI/BICSI-002 [23]: Projeto de *Datacenter* e Melhores Práticas de Implementação (*Datacenter* Design and Implementation *Best* Practices) foi publicada em março de 2011 e tem cinco classificações de disponibilidade de *datacenter*, F0 a F4 sendo a F0 a classe mais básica e a F4 a classe mais tolerante as falhas [15].

A norma que se aplica na infraestrutura de um *datacenter*, de acordo com a sua disponibilidade e a sua redundância, é a ANSI/TIA 942 [24]: Infraestrutura de Telecomunicações para *Datacenters* (*Telecommunications Infrastructure Standard for Datacenter*), a qual atualmente é a mais utilizada e a única que aplica o conceito de *Tiers* para a classificação de *datacenters*.

Chamado de "*Tier*" (literalmente, "camada" em inglês), o padrão mundial de classificação foi criado especialmente para *datacenters* pelo consórcio *Uptime Institute* e validado pelo comitê *Owner Advisory Committee*.

O padrão hoje é aceito em mais de 40 países e serve para diferenciar os *datacenters* conforme sua infraestrutura, baseado em classes crescentes de redundância, que variam de *Tier* I a *Tier* IV (sendo I o menos e IV o mais complexo).

Segundo VERAS [13], pela norma ANSI/TIA 942 [24], existem regras aplicáveis para a classificação do *datacenter* em quatro níveis independentes de *Tiers*, são eles:

Redundância; Telecomunicação; Arquitetura e Estrutural; Elétrica; Mecânica.

Ela estabelece também nomenclaturas para as definições da redundância, utilizando como base a classificação *Tier*. As classificações são as seguintes [15].

- *Datacenter* N: sem nenhum tipo de redundância.
- *Datacenter* N+1: existe pelo menos uma redundância (*nobreak*, gerador).
- *Datacenter* N+2: existe uma redundância a mais, por exemplo: será suprido na falta de energia por um *nobreak* e um gerador, sendo assim duas redundâncias. Podendo se estender para os outros equipamentos, *links*, refrigeração, sistema de prevenção de incêndios etc.
- *Datacenter* 2N: neste caso seria uma redundância completa, por exemplo: duas empresas de distribuição de energia (sendo que essas empresas devem vir de diferentes subestações) para alimentação.
- *Datacenter* 2(N+1): existe uma redundância para cada equipamento, utilizando o exemplo anterior.

Abaixo, serão citadas algumas das principais informações sobre cada uma das classes *Tier*, que podem ser encontradas em ANSI/TIA 942 [24].

- *Tier* I (infraestrutura básica): é o primeiro nível possível. Nele não há preocupações especiais com os serviços processados e o desligamento de todo o site é necessário para trabalhos de manutenção. Além disso, falhas de distribuição e capacidade irão afetar os serviços ofertados.
- *Tier* II (Componentes Redundantes): além das funções do primeiro nível, existe a preocupação com elementos redundantes. Ainda é necessário o desligamento de todo o sistema para a manutenção, já que falhas de capacidade e falhas de distribuição podem surgir.
- *Tier* III (Sistema Auto Sustentado): é o primeiro que permite remover componentes de maneira planejada para a chamada Manutenção Concorrente, ou seja, que não afeta as operações totais do site hospedado. Ainda assim, o site ainda está exposto a falhas de equipamento ou a erros do operador.
- *Tier* IV (Alta Tolerância a Falhas): além de atender todas as exigências do *Tier* anterior, são os únicos capazes de tolerar falhas de equipamento individual ou a interrupção no caminho de distribuição, sem afetar as operações. São de alto

custo de construção e operação e se justificam apenas quando falamos de processamentos que exigem alto sigilo e disponibilidade (99.995% - Possui um *downtime* de 0.4horas/ano e 96 horas de proteção contra interrupção de energia).

A tabela 1 abaixo mostra a comparação entre os *Tiers*, citando de maneira mais objetiva alguns parâmetros mais importantes, a saber.

Tabela 1: Comparação das classes *Tier*. [14]

Características	**TIER I**	**TIER II**	**TIER III**	**TIER IV**
Número de caminhos de entrega de energia	1	1	1 Ativo 1 Passivo	2 Ativos
Componentes redundantes	N	N + 1	N + 1	2 (N+1)
Support Space to Raised Floor Ratio	20%	30%	80-90%	100%
Watts iniciais por m^2	60-90	120-150	120-180	150-240
Watts finais por m^2	60-90	120-150	300-450	450 +
Altura de piso elevado	30cm	45cm	80-90cm	80-90cm
Carga do piso (kg/m^2)	415	488	732	732+
Tensão da rede	208, 480	208, 480	12-15 kV	12-15 kV
Meses para implementar	3	3 to 6	15 to 20	15 to 20
Primeiro ano implantado	1965	1970	1985	1995
Tempo de inatividade anual	28,8 hrs	22,0 hrs	1,6 hrs	0,4 hrs
Disponibilidade	99,671%	99,749%	99,982%	99,995%

Para otimizar o espaço do *datacenter*, normalmente, são utilizados servidores para *Rack*. A altura dos módulos eletrônicos também é padronizada em múltiplos de 1,752 polegadas (44,50 milímetros) ou uma "Unidade de *Rack*", ou "U" (do termo em inglês, *Rack Unit*). O gabinete de *rack* padrão da indústria é de 42U de altura. [28]

A maioria dos *racks* comporta 42U, ou seja, permitem a instalação de até 42 servidores de 1U. Alguns servidores mais potentes podem ocupar mais de 1U de altura,

principalmente se ele tiver capacidade para a instalação de vários discos rígidos e processadores. Além de servidores, também é possível armazenar nos *racks* uma série de outros equipamentos, como roteadores de rede e unidades de *backup* em fita, por exemplo. [29]

O tamanho da unidade U é baseado em uma especificação padrão definida no padrão EIA/ECA-310 (*Electronic Industries Alliance Standards*) - *Cabinets*, *racks* (*including 19-inch racks, rack units*), *panels and associated equipment standard*.

2.3.2 Localização e Infraestrutura

A localização física e infraestrutura de um *datacenter* é um dos pontos-chave a se observar em relação a segurança da informação. Segundo as normas NBR 14565:2001, ANSI/BICSI-002 e ANSI/TIA-942, algumas recomendações para a escolha da localização devem ser levadas em consideração, a saber.

- Acessibilidade externa e interna.
- Proximidade a uma rede elétrica de alta prioridade.
- Resistência predial (saber se o prédio foi construído para ser um *datacenter* ou adaptado para tal propósito).
- Tempo de construção da infraestrutura fornecida.
- Existência de problemas estruturais aparentes.
- Local onde está situado e conhecimento sobre quem são seus vizinhos mais próximos.

São locais inadequados para construção [16] os seguintes.

- Próximos a rios, lagos, oceanos e fundos de vale, pois estes locais têm riscos de inundações, enchentes, tsunamis etc.
- Próximos a cabeceiras de pistas de aeroportos, pois existe o risco de acidente em potencial.
- Locais com riscos de desmoronamentos e perigo de incêndio.
- Locais propícios a abalos sísmicos e/ou tornados.
- Locais próximos a linhas de transmissões elétricas.

- Países ou locais com guerrilhas.

São locais recomendados para a construção, a saber.

- Próximos de acessos a estradas principais.
- Próximos a concessionárias de energia.
- Próximos a centros de serviços.
- Condomínios comerciais específicos para *Datacenters*.

2.3.3 Normas

A seguir, como forma de exemplificar o quão abrangente podem ser as exigências, é listada as normas e padrões nacionais e internacionais utilizadas na construção, manutenção e certificação de d*atacenters* (e toda sua abrangência), sempre considerando a versão mais recente das respectivas normas.

- ABNT NBR 5410 - Instalações elétricas de baixa tensão.
- ABNT NBR 5413 - Iluminância de interiores.
- ABNT NBR 5471 - Condutores elétricos.
- ABNT NBR 9442 (Materiais de construção) - Determinação do índice de propagação superficial de chama pelo método do painel radiante - Método de ensaio.
- ABNT NBR 10151 (Acústica) – Avaliação do ruído em áreas habitadas visando o conforto da comunidade – Procedimento.
- ABNT NBR 10636 (Paredes divisórias sem função estrutural) – Determinação da resistência ao fogo - Método de ensaio.
- ABNT NBR 10898 - Sistema de iluminação de emergência.
- ABNT NBR 11515 - Guia de Práticas para Segurança Física relativas ao armazenamento de dados.
- ABNT NBR 11802 (Pisos elevados) – Especificação.
- ABNT NBR 13532 - Elaboração de projetos de edificações (Arquitetura).
- ABNT NBR 13966 (Móveis para escritório) – Mesas, classificação e

características físicas dimensionais e requisitos e métodos de ensaio.

- ABNT NBR 13967 (Móveis para escritório) – Sistemas de estação de trabalho, classificação e métodos de ensaio.
- ABNT NBR 14565 - Cabeamento estruturado para edifícios comerciais e d*atacenters*.
- ABNT NBR 15014 - Sistemas de alimentação de potência ininterrupta (*nobreaks*) *online*, interativo e *stand-by*, que utilizam bateria como fonte de energia armazenada.
- ABNT NBR 15141 - Móveis para escritório: Divisória modular tipo piso-teto.
- ABNT NBR 17240 (Sistemas de detecção e alarme de incêndio) – Projeto, instalação, comissionamento e manutenção de sistemas de detecção e alarme de incêndio – Requisitos.
- ABNT NBR 5261 (Símbolos gráficos de eletricidade) – Princípios gerais para desenho de símbolos gráficos.
- ABNT NBR 5410 - Instalações elétricas de baixa tensão.
- ABNT NBR 5419 - Proteção de estruturas contra Descargas Atmosféricas.
- ABNT NBR 6492 - Representação de projetos de arquitetura.
- ABNT NBR 9574 - Execução de impermeabilização.
- ABNT NBR 9575 – Impermeabilização, seleção e projeto.
- ABNT NBR IEC 60947-2 - Dispositivos de manobra e comando de baixa tensão.
- ABNT NBR ISO 7240-1 - Sistemas de detecção e alarme de incêndio Parte 1: Generalidades e definições.
- ABNT NBR ISO/IEC 27001 (Tecnologia da informação) – Técnicas de segurança, sistemas de gestão de segurança da informação e Requisitos.
- ABNT NBR ISO/IEC 27002 (Tecnologia da informação) – Técnicas de segurança e código de pratica para a gestão da segurança da informação.
- ABNT NR 16401-1 (Instalações de ar-condicionado) – Sistemas centrais e unitários - Parte 1: projetos das instalações.
- ABNT NR 16401-2 (Instalações de ar-condicionado) - Sistemas centrais e unitários - Parte 2: parâmetros de conforto térmico.

- ABNT NR 16401-3 (Instalações de ar-condicionado) – Sistemas centrais e unitários - Parte 3: qualidade do ar interior.
- ANSI/BICSI-002 - *Datacenter Design and Implementation Best Practices*.
- ANSI/EIA/TIA 942 - *Telecommunications Infrastructure Standard for Datacenters*.
- ANSI/TIA/EIA-568-B.1 - *Commercial Building Telecommunications Cabling Standard – Part 1: general requirements*.
- ANSI/TIA/EIA-568-B.1-1 - *Commercial Building Telecommunications Cabling Standard – Part 1: general requirements – Addendum 1 – Minimum 4-Pair UTP e 4-Pair ScTP Patch cable Bend Radius*.
- ANSI/TIA/EIA-568-B.1-3 - *Commercial Building Telecommunications Cabling Standard – Part 1: general requirements – Addendum 3 – Supportable Distances and Channel Attenuation for Optical Fiber applications by Fiber Type*.
- ANSI/TIA/EIA-568-B.1-4 - *Commercial Building Telecommunications Cabling Standard – Part 1: general requirements – Addendum 4 – Recognition of category 6 and 850 nm laser- Optimized 50/125 µm Multimode optical fiber cabling*.
- ANSI/TIA/EIA-568-B.2 - *Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components*.
- ANSI/TIA/EIA-568-B.2-1 - *Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components – Addendum 1 – Transmission performance Specifications for 4-Pair 100 Ohm Category 6 Cabling*.
- ANSI/TIA/EIA-568-B.2-10 - *Transmission Performance Specifications for 4-pair 100-ohm Augmented Category 6 Cabling*.
- ANSI/TIA/EIA-568-B.2-2 - *Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components – Addendum 2*.
- ANSI/TIA/EIA-568-B.2-3 - *Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components – Addendum 3 – Additional considerations for Insertion Loss and Return Loss Pass/Fail Determination*.
- ANSI/TIA/EIA-568-B.2-5 - *Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components – Addendum 5*.

- ANSI/TIA/EIA-568-B.3 - *Commercial Building Telecommunications Cabling Standard – Part 3: Optical Fiber Cabling components standard*.
- ANSI/TIA/EIA-568-B.3-1 - *Commercial Building Telecommunications Cabling Standard – Part 3: Optical Fiber Cabling components standard – Addendum 1 – Additional Transmission Performance Specifications for 50/125 µm Optical fiber cables*.
- ANSI/TIA/EIA-569-B - *Commercial Building Standard for Telecommunications Pathways and Spaces*.
- ANSI/TIA-606-B - *Administration Standard for Telecommunications Infrastructure*.
- ASTM A106 / A106M - *Standard Specification for Seamless Carbon Steel Pipe for High-Temperature Service*.
- ASTM B117-11 - *Standard Practice for Operating Salt Spray (Fog) Apparatus*.
- ASTM D257-07 - *Standard Test Methods for DC Resistance or Conductance of Insulating Materials*.
- ASTM E119-12 - *Standard Test Methods for Fire Tests of Building Construction and Materials*.
- ASTM E662 - *Standard Test Method for Specific Optical Density of Smoke Generated by Solid Materials*.
- BS EN 50173-5:2007+A1 - *Information technology. Generic cabling systems. DataCenters*.
- BS ISO 14520-11 - *Gaseous fire-extinguishing systems. Physical properties and system design*.
- DIN V 18103 – *Doors: Burglar Resistant Doors - Terms, Requirements, Tests, Marking And Labelling*.
- DIN 68761- *Specifications for particleboard*.
- ISO 1182 - *Reaction to fire tests for products – Non-combustibility test*.
- ISO/IEC 24764 - *Information technology - Generic cabling systems for DataCenters*.
- ISO/IEC-11801 - *Information Technology - Generic Cabling for Customer Premises*.

- MTE/NR N° 01 - Segurança do Trabalho: Disposições Gerais.
- MTE/NR N° 02 - Segurança do Trabalho- Inspeção Prévia.
- MTE/NR N° 04 - Serviços Especializados em Engenharia de Segurança e em Medicina do Trabalho.
- MTE/NR N°06 - Equipamentos de Proteção Individual (EPI).
- MTE/NR N°10 - Segurança em Instalações e Serviços em Eletricidade.
- MTE/NR N°11 - Transporte, Movimentação, Armazenagem e Manuseio de Materiais.
- MTE/NR N°12 - Segurança no Trabalho em Máquinas e Equipamentos.
- MTE/NR N°17 – Ergonomia.
- MTE/NR N°23 - Proteção Contra Incêndios.
- MTE/NR N°26 - Sinalização de Segurança.
- MTE/NR N°28 - Fiscalização e Penalidades.
- NFPA-2001 - *Standard on Clean Agent Fire Extinguishing Systems*.
- NFPA-75 - *Standard for the Fire Protection of Information Technology Equipment*.
- RESOLUÇÃO ANATEL nº 242, de 30/11/2000 - Regulamento para certificação e homologação de produtos para telecomunicações.
- RESOLUÇÃO ANATEL nº 299, de 24/06/2002 - Regulamento para certificação e homologação de cabos de fibras ópticas.

2.4 Responsabilidades

É interessante, mas não obrigatório, anexar ao contrato um termo de responsabilidade para ambas as partes, informando e descrevendo o que pode ou não ser feito e de quem é a responsabilidade sobre equipamentos, dados, informações etc.

Abaixo, um exemplo do que pode ser descrito.

- A **contratada** se compromete, por intermédio de um termo de confidencialidade, a não divulgar sem autorização quaisquer informações de propriedade da **contratante.**

- A **contratada** reconhece que em razão da sua prestação de serviços a **contratante**, consoante no contrato, mantém contato com informações privadas, as quais devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados.
- As informações tratadas como confidenciais, por sua natureza, são aquelas que não deveriam ser de conhecimento de terceiros, compreendendo toda e qualquer documentação que compõe os processos judiciais, informações de natureza financeira, administrativa, contábil, jurídica, pessoal e patrimonial das partes.
- A **contratada** recolherá, durante a execução do contrato, para imediata devolução, todo e qualquer registro de qualquer natureza que tenha sido criado, usado ou mantido sob seu controle ou posse, quer seja de seus empregados ou prepostos, com vínculo empregatício ou eventual com a **contratada**, assumindo o compromisso de não utilizar qualquer informação a que teve acesso enquanto vigente por este contrato.
- A **contratada** determinará a todos os seus empregados, prepostos e prestadores de serviços que estejam, direta ou indiretamente, envolvidos com a prestação de serviços objeto do contrato, a observância do presente Termo e a assinatura de Termos individuais adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.
- A **contratada** obriga-se a informar imediatamente a **contratante** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

2.5 Requisitos Obrigatórios

Abaixo são listados requisitos que são exigidos da **contratada**.

2.5.1 Requisitos de Negócio

Requisitos de negócio independem de características tecnológicas e definem as necessidades dos serviços e os aspectos funcionais da solução de TI.

A **contratada** deverá oferecer uma solução de TI que crie um ambiente redundante com capacidade para suportar um conjunto de serviços considerados como sendo de "missão crítica".

Deverá favorecer também a redução de riscos operacionais de funcionamento pleno, bem como o aprimoramento de processos de reação e tratamento de situações emergenciais e desastres.

2.5.2 Requisitos de Capacitação

Requisitos de capacitação definem a necessidade de treinamento presencial ou à distância, carga horária e entrega de materiais didáticos.

- A **contratada** deverá capacitar a equipe técnica da **contratante** para gerenciar a solução.
- Os treinamentos técnicos especializados dos componentes da solução de TI deverão ser ministrados anteriormente à instalação e configuração dos equipamentos e/ou *softwares*. Será facultado à **contratante** o agendamento do treinamento posterior à instalação, caso assim julgue conveniente.
- O treinamento referente aos componentes da solução deverá contemplar: carga horária adequada; conhecimentos necessários à instalação, configuração, administração, *troubleshooting* e utilização dos componentes da solução de TI.
- O cronograma contendo as datas e os horários para realização dos treinamentos será proposto pela **contratada** e aprovado pela **contratante**. Caso esta dê causa ao atraso do cronograma, aquela não será responsabilizada.
- O treinamento deverá contemplar atividades práticas. Para a consecução da parte prática, poderão ser utilizados equipamentos similares aos ofertados, além dos *softwares* que fazem parte da solução, ou os próprios equipamentos fornecidos, desde que o treinamento não cause impacto nas operações do ambiente corporativo da **contratante**.

2.5.3 Requisitos Legais e Normas

Requisitos legais que definem as normas, as quais a solução de TI deverá respeitar.

- Todos os componentes de telecomunicações que integrem o objeto adquirido deverão estar em conformidade com regulamentos editados pela Anatel ou com as normas por ela adotadas.
- Norma ABNT NBR 15999 e ISO 22301 que regem a Gestão de Continuidade de Negócios (GCN).
- Família de normas ABNT NBR ISO/IEC 27000 de Segurança da Informação.
- Total aderência às normas descritas no item 2.3 ADERÊNCIA À NORMAS TÉCNICAS, deste relatório técnico.

2.5.4 Requisitos de Desempenho

A solução **contratada** deverá fornecer redundância manual e automática que garanta o funcionamento de níveis mínimos de serviços corporativos, quer decorrente de situações anômalas, quer durante situações de exceção.

O site redundante deverá garantir no mínimo 75% da capacidade nominal do poder de processamento do site principal.

2.5.5 Requisitos de Segurança da Informação

Faz-se necessário estabelecer regras para garantir o sigilo de dados e a segurança das informações eventualmente compartilhadas com a **contratada**.

Entre estas regras podemos destacar:

- a **contratada** deverá manter sob sigilo as informações e comunicações de que tiver conhecimento, abstendo-se de divulgá-las, garantindo o sigilo e a inviolabilidade dos dados trafegados por meio dos enlaces eventualmente utilizados na execução das atividades, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;
- deverão ser delineados os requisitos para acesso físico ao site principal e ao site

redundante;

- os dispositivos de armazenamento substituídos em função de troca em garantia, ou ficarão retidos na **contratada** até sua exclusão, ou somente serão devolvidos após sua inutilização completa;
- a devolução do componente inutilizado ou desmagnetizado ficará a critério exclusivo da **contratante**, sem gerar direitos à **contratada**;
- a **contratada** não poderá armazenar consigo qualquer documento técnico que contemple configurações aplicadas nos equipamentos implantados na rede da **contratante**;
- a **contratada** deverá informar à **contratante** todas as senhas utilizadas para a configuração dos equipamentos, as quais deverão ser alteradas pela **contratante** com o apoio técnico da prestadora, logo após a assinatura do Termo de Recebimento Definitivo;
- a **contratada** deverá prover segurança de acesso físico e lógico aos recursos da **contratante** que estiverem sob sua guarda;
- os recursos de TI não poderão ser utilizados pela **contratada** ou seus prepostos para realização de atividades alheias aos serviços previstos ou englobados nesta contratação;
- a **contratada** deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com a **contratante**, abstendo-se de divulgá-los a terceiros sob qualquer pretexto, a menos que prévia e formalmente autorizada;
- todos os perfis de acesso e caixas postais eventualmente concedidos à **contratada** deverão ser imediatamente excluídos após o término da implantação da solução;
- a **contratante** terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;
- a **contratada** deverá respeitar as normas de segurança estabelecidas pela **contratante** durante a realização de atividades no ambiente desta. Essa sujeição não caracteriza qualquer vínculo empregatício com a **contratante**.

2.5.6 Requisitos de Sala Segura

Caso haja a necessidade de obtenção e uso de uma Sala Segura para proteção física dos equipamentos computacionais do *datacenter*, bem como dos subsistemas de segurança internos a ela, esta deverá ter, no mínimo, as especificações técnicas a seguir.

- A Sala Segura deverá apresentar área interna mínima de 33 m².
- Seja capaz de prover proteção contra fogo por, no mínimo, 90 minutos, comprovada por certificação obtida a partir de ensaios normatizados, conforme norma ABNT NBR 10636 (classe CF90), similar ou superior, emitida por Organismo Certificador de Produto (OCP) acreditado pelo INMETRO no escopo adequado. A resistência ao fogo deverá englobar os testes de isolamento térmico, estanqueidade (chamas e gases quentes) e estabilidade (choques mecânicos), nos termos da referida norma.
- Caso seja apresentada certificação em norma estrangeira similar ou superior, a certificação deverá ser emitida por Organismo Certificador de Produto do país em questão, desde que o OCP seja devidamente acreditado no escopo adequado por órgão local equivalente ao INMETRO, dotado de acreditação internacional pelo IAF (*International Accreditation Forum*).
- O piso, o teto e as paredes deverão ser adequados aos mecanismos do sistema de detecção e combate a incêndio, aos recursos do sistema de controle de acesso biométrico, de climatização de precisão, do sistema de vigilância e do sistema de cabeamento estruturado lógico e elétrico do *datacenter*, descritos neste documento.
- A sala deverá estar permanentemente limpa e livre de poeira através do auxílio de equipamentos de aspiração mecânica.
- A sala deverá possuir sistema de refrigeração, com corredores de ar quente e ar frio, em conformidade com a norma TIA-942, com duas fileiras de *racks* próprios para este sistema, em número não inferior a 12 *racks* (seis em cada fileira). Os *racks* deverão ser fornecidos pela **contratada**.
- A sala deverá apresentar estanqueidade contra trocas gasosas com o ambiente externo, mantendo os parâmetros mínimos de renovação de ar estabelecidos na Norma NBR 16401, norma similar ou superior.

- A sala deverá ser dotada de subsistema de monitoramento e controle do ambiente através de painel de monitoração, conforme item 12 - Subsistema de Monitoramento Ambiental e Vigilância (CFTV).
- A sala deverá ser modular, de modo a facilitar alterações, como ampliações e mudanças de local.
- Deverá ser provida de iluminação adequada dentro da sala, conforme padrão indicado na Norma TIA 942, distribuída em circuitos por setor, com luz de emergência e circuito autônomo, com identificação de saídas de emergência e sinais luminosos que possam ser vistos a partir de todos os pontos da sala.
- As aberturas feitas para passagem de cabos, tubulações e outros elementos que precisem entrar ou sair da sala segura devem receber tratamento de vedação.
- Este sistema de blindagem deverá ser modular e permitir o remanejamento de cabos e tubulações sempre que necessário, por vezes sem interferência na operação, e também garantir a proteção do ambiente da sala.
- No ambiente objeto da contratação, deverá ser executada impermeabilização na laje superior para todas as áreas sujeitas a contato transitório ou permanente com água. O sistema de impermeabilização adotado deverá ter sua eficiência comprovada mediante a apresentação de atestados técnicos referentes a sua aplicação em soluções similares, realizadas há mais de cinco anos. A impermeabilização deverá ser projetada para um prazo mínimo de vida útil de 20 (vinte) anos.
- Deverá possuir ponto de telefone integrado à central telefônica do prédio com aparelho fornecido pela **contratada**.
- A sala segura deverá possuir porta adequada a ambientes seguros, com dimensões suficientes para movimentação de equipamentos de TI, com largura entre 1,20 m e 1,30 m, e altura mínima de 2,10 m, confeccionada com elementos construtivos compatíveis com a sala segura.
- A porta deverá prover proteção contra fogo por, no mínimo, 90 minutos, comprovada por certificação obtida a partir de ensaios normatizados, conforme Norma ABNT NBR 6479, similar ou superior, emitida por Organismo Certificador de Produto (OCP) acreditado pelo INMETRO no escopo adequado. A resistência ao fogo deverá englobar os testes de isolamento térmico, estanqueidade (chamas

e gases quentes) e estabilidade (choques mecânicos), nos termos da referida norma.

- Para a comprovação da proteção descrita no item anterior, será permitida certificação na Norma ABNT NBR 10636, desde que a porta seja integrada ao corpo de prova, conforme prevê o item 5.3.1 da referida norma, e desde que as verificações de estabilidade, estanqueidade e isolamento térmico na porta sejam feitas de acordo com os métodos específicos descritos na Norma ABNT NBR 6479, conforme prevê o item 5.5.4.2 da Norma ABNT NBR 10636.
- Caso seja apresentada certificação em norma estrangeira similar ou superior, a certificação deverá ser emitida por Organismo Certificador de Produto do país em questão, desde que o OCP seja devidamente acreditado no escopo adequado por órgão local equivalente ao INMETRO, dotado de acreditação internacional pelo IAF (*International Accreditation Forum)*.
- A porta de acesso deverá ser dotada de fechadura com travamento eletromecânico e acionamento automático por leitura biométrica de entrada, conforme Subsistema de Controle de Acesso Biométrico.
- A porta deverá possuir sistema anti-pânico que permita livre saída em caso de eventual emergência.
- A porta deverá permitir a abertura e o fechamento de forma automática, sem auxílio manual.

2.5.7 Requisitos de Infraestrutura

Características de infraestrutura física de acordo com o padrão mundial de classificação de *datacenter* TIER III ou TIER IV.

2.5.8 Requisitos para Piso

Deverá ser implantado piso de cor clara em todos os ambientes propostos, incluindo a sala segura, sala de telecomunicações, NOC e sala de UPS, com, no mínimo, as especificações técnicas a seguir.

- Ser resistente ao tráfego de pessoas e adequado à movimentação de equipamentos de TI.
- Deverá apresentar característica fogo retardante e auto-extinguível, com Ip<=25 segundo a Norma ABNT NBR 9442, Dm < 450 segundo a Norma ASTM E662 ou apresentar característica de incombustibilidade nos termos da Norma ISO 1182. A comprovação dos parâmetros acima far-se-á por laudo técnico emitido por laboratório acreditado pelo INMETRO no escopo adequado, atestando de forma inequívoca que as características preconizadas na referida norma são atendidas pelo material ofertado. Será aceita ainda comprovação por laboratório estrangeiro, desde que acreditado por órgão do país em questão equivalente ao INMETRO dotado de acreditação internacional pelo ILAC (*International Laboratory Accreditation Cooperation*).
- Possuir acabamento antiderrapante e anti-estático.
- Possuir capacidade dissipativa de cargas eletrostáticas conforme Norma ASTMD257, norma similar ou superior.

2.5.9 Requisitos para Segurança Elétrica

- O *datacenter* deverá ter infraestrutura de entrada de energia atendida pela companhia energética local por meio de circuito AC de alta tensão.
- O provimento interno de energia deverá ser feito de tal forma que estejam disponíveis duas réguas de energia com alimentação redundante. Caso haja falha no fornecimento de energia em uma régua por qualquer motivo físico ou elétrico, a outra régua deverá continuar fornecendo energia.
- Cada régua de energia deverá ter a quantidade de pontos de energia requisitados no contrato e suportar o consumo da potência nominal prevista nos equipamentos fornecidos pela mesma.
- Para fins de redundância no fornecimento de energia, o *datacenter* deve complementar a infraestrutura de energia elétrica através de grupo motor-gerador (redundância N+1) e independente, com acionamento automático na eventualidade de interrupção no fornecimento de energia e com testes diários de funcionamento e nobreak (redundância N+1).

- O *nobreak* deve assumir a alimentação dos equipamentos do *datacenter* na falta de energia da concessionária até que o grupo motor-gerador entre em operação, garantindo assim o suprimento contínuo e ininterrupto de energia elétrica.
- O grupo motor-gerador deverá possuir a autonomia para suprir a energia necessária aos equipamentos enquanto a concessionária de energia não voltar a fornecer a energia.
- Deverá possuir sistema de energia totalmente gerenciado, com circuitos e quadros redundantes, com sistema de proteção e aterramento de acordo com a norma ANSI TIA J-STD-607_A.
- Deverá possuir réguas de alimentação do tipo PDU (*Power Distribution Unit*) redundantes por *rack*.
- Garantir total independência no suprimento de energia elétrica para a eventualidade de falta prolongada na rede da concessionária local.
- Deverá possuir os componentes necessários para garantir autonomia plena de energia elétrica para o *datacenter* em regime de tempo integral.
- Deverá garantir alimentação elétrica independente para os setores de computadores e áreas administrativas.
- Deverá possuir sistema redundante de UPS's para garantir a transição entre o fornecimento normal de energia e o grupo gerador.

2.5.10 Requisitos para Segurança Física

- O *datacenter* deverá ter infraestrutura de entrada de energia atendida pela companhia energética local por meio de circuito AC de alta tensão.
- O *datacenter* deverá possuir vigilância armada patrimonial 24 horas por dia, 7 dias por semana, 365 dias por ano, permitindo apenas a entrada de pessoas autorizadas e devidamente identificadas através de sistema de controle de acesso eletrônico que possibilite a geração de relatórios de acesso quando solicitado.
- O *datacenter* deverá estar equipado com sistema de climatização de alta disponibilidade (Ar-condicionado de precisão com redundância N+1 e renovação de ar de modo a garantir o correto condicionamento térmico para os equipamentos

conforme especificação dos fabricantes) e o sistema deve possuir filtros de poeira e abafador de ruído.

- O *datacenter* deverá possuir dispositivos de detecção precoce de incêndio pela análise do superaquecimento de cabos ou *hardwares*, de maior sensibilidade que os tradicionais detectores de fumaça e sistema de detecção precoce de incêndio por sensores termovelocimétricos tipo – VESDA (*Aspirating Smoke Detection System*) e solução de combate a incêndio com sensores de fumaça, extintores de incêndio e sistema gasoso e disponibilizar mecanismos automáticos de extinção de fogo por agentes gasosos não poluentes do tipo FE227, com ação baseada na quebra de moléculas de oxigênio, que não danifiquem os equipamentos eletroeletrônicos e sejam inertes e não tóxicos aos seres humanos; e, que permita uma ação rápida e eficiente no combate a possíveis focos de incêndio. A extinção de incêndio deverá ser feita com métodos que não prejudiquem ou acabem com o funcionamento dos equipamentos contratados.
- Possuir integração com sistema de alarme e ser monitorado em tempo integral.
- Possuir sistema de cabeamento estruturado com, no mínimo, três camadas de cabeamento com vias independentes de cabos de energia, lógicos e óticos.
- Possuir sistema de segurança, climatização, quadros de distribuição elétrica, suprimento ininterrupto de energia elétrica, proteção contra descargas atmosféricas, indução eletromagnética e aterramento.
- Possuir ambiente seguro para fitoteca com controle de acesso 24 horas por dia, para armazenamento das fitas para *backups*, com proteção para riscos de incêndio, calor, água, gases corrosivos e tóxicos e magnetismos, com suprimento de energia elétrica e climatização independentes das demais áreas do *datacenter*.
- Manter 24 horas por dia, 7 dias por semana, 365 dias por ano, pessoas treinadas e responsáveis pela vigilância dos ambientes interno e externo, segurança de acesso ao prédio e controle de entrada e saída de veículos.
- Possuir rígido controle de acessos aos equipamentos do *datacenter*, mesmo por pessoas credenciadas pela **contratante**.
- Disponibilizar mecanismos efetivos de controle de entrada e saída de pessoas, que acessam e fazem uso do *datacenter*, cartões magnéticos bem como de registros passíveis de posterior pesquisa.

- Possuir travas eletrônicas que, de acordo com a política de segurança estabelecida para o *datacenter*, o divide em regiões com níveis de restrição diferenciados.
- Eventuais tentativas de acesso indevido devem ser monitoradas e verificadas.
- Exigência de piso elevado no ambiente de produção com capacidade para 1200 kgf/m2 no mínimo.

2.5.11 Requisitos para Subsistema de Provimento Ininterrupto de Energia Elétrica e Iluminação

Deverão ser fornecidas, no mínimo, duas unidades redundantes e modulares de *no-breaks* UPS, sendo cada unidade dimensionada de forma a suportar a demanda de energia de todo o *datacenter*, inclusive subsistemas de climatização de precisão e de conforto, com autonomia de 30 minutos a plena carga. As unidades deverão, ainda, ser dimensionadas para uma carga pelo menos 50% acima da demanda atual e possuir, no mínimo, as seguintes características:

- os UPSs deverão permitir monitoração via *software* do conjunto de baterias;
- os UPSs deverão manter automaticamente a energia AC dentro dos padrões de tolerância especificados para carga crítica, sem interrupções, durante falha ou anormalidades da rede elétrica;
- os UPSs deverão conter *bypass* estático eletrônico independente, além de interruptores manuais de *bypass* para manutenção;
- as unidades de UPS deverão possuir baterias do tipo estacionárias, válvulas reguladas, com vaso retardante a chama, dispostas em armário próprio ou em gabinete, com expectativa de vida útil mínima de 5 anos;
- as unidades de UPS deverão possuir as seguintes características complementares:
    - lógica digital para memorização de eventos, mostrando em *display*: eventos e grandezas de tensões, correntes e frequências;
    - alarme sonoro para bateria em descarga, final de descarga, sobrecarga, *bypass* e sobretemperatura;
    - chave *bypass* manual sem interrupção de carga;
    - sensores de falta de fase, sub e sobre tensão na saída;

- proteção eletrônica no inversor contra sobretensão, sobrecarga e curto-circuito;
- *bypass* automático;
- supressor de transientes;
- redundância do sistema de ventilação;
- proteção contra descarga total das baterias;
- eficiência do sistema > 93% (a 100% de carga), > 91% a operação normal de 50% em dual bus.

- lógica digital para memorização de eventos, mostrando em *display*: eventos e grandezas de tensões, correntes e frequências.

Deverá apresentar as seguintes características para o sistema de quadros e distribuição de energia elétrica essencial e de emergência:

- deverá haver um quadro (QD1) de comando entre a rede concessionária de energia e o grupo gerador 1, e um quadro de integração (QD2) entre esses dois primeiros e o grupo gerador 2, ambos usados para manter as funções essenciais. No caso de falha da concessionária, o gerador 1 deverá partir e alimentar os painéis do *datacenter* através de chaves de transferência automática. Já em caso de falha do gerador 1, o quadro QD2 deverá ser responsável pela transferência de carga automaticamente para o gerador 2. Esses conjuntos deverão ser travados para impedir o paralelismo dos grupos geradores entre si e destes com a rede da concessionária de energia. O sistema também deverá permitir a execução de manutenção dos componentes sem que seja necessária a interrupção da carga crítica;
- a sala segura deverá receber energia limpa e ininterrupta por meio de dois quadros (*dual bus*) a serem instalados dentro da sala e denominados nesse projeto como QDX para a linha "X" e QDY para a linha "Y". O sistema *dual bus* consiste na duplicação do sistema elétrico, tornando-o redundante 1+1, ou seja, cada linha de alimentação dos UPSs e quadros de distribuição internos à sala, em condições normais, assumem 50% da carga total do ambiente. Em caso de falha de um dos sistemas o outro assume imediatamente a carga da sala em 100%;

- a partir dos conjuntos de UPS, as alimentações deverão ser recebidas pelos painéis de distribuição de tomadas QDX e QDY, que têm a função de distribuir a energia aos *racks* e equipamentos da sala segura, através de circuitos distribuídos por eletrocalhas;
- os quadros de distribuição dentro da sala segura deverão possuir as seguintes características mínimas:
    - ser projetados para minimizar interrupções. Os disjuntores de proteção das cargas parciais deverão ser do tipo *plug-in*, com montagem de forma a minimizar tempos de manutenção;
    - os componentes internos dos quadros deverão ser compostos por:
        - interruptores de carga (chaves seccionadoras) na entrada dos quadros. Os interruptores deverão permitir abertura em carga, montagem fixa, corrente nominal conforme diagrama unifilar do projeto a ser aprovado;
        - disjuntores parciais, conforme IEC 947-2 e NBR IEC 60947-2. Os disjuntores deverão ser montados em bases especiais que permitam instalação e retirada com o quadro energizado, sem uso de ferramentas;
        - medidor de energia digital, multifunção, com, no mínimo, os seguintes recursos de medição/indicação: indicação de correntes monofásica e de neutro, indicação de tensões fase-fase e fase-neutro, medição de energias ativa, reativa e aparente, indicação de potências ativa, reativa e aparente, indicação de fator de potência e indicação de frequência;
        - transformadores de corrente, classe de isolamento 600V, isolamento de epóxi;
        - blocos de aferição para circuito de corrente, classe de isolamento 600V;
        - supressores de surto.

O sistema de distribuição elétrica para iluminação e tomadas de uso geral deverão possuir as seguintes características mínimas:

- a partir dos quadros QD1/QD2 (especificados em item anterior), deverão sair circuitos elétricos que alimentarão os quadros de iluminação e de tomadas em geral para as salas do *datacenter*;
- o sistema deve estar em conformidade com a Norma ABNT NBR 5410, norma similar ou superior;
- as luminárias autônomas das salas de *nobreak*, sala segura e demais ambientes deverão ter autonomia mínima de uma hora. Essas luminárias deverão ser ligadas nos circuitos das tomadas de serviço.

O sistema de distribuição de energia elétrica para equipamentos de climatização de precisão da sala segura deverá possuir as seguintes características mínimas:

- a partir dos quadros elétricos de saída dos UPSs, os cabos destinados à alimentação dos equipamentos deverão seguir até a sala segura;
- para interligação entre os evaporadores e os condensadores, deverão ser utilizados eletrodutos;
- os circuitos elétricos deverão ser identificados, em suas extremidades e ao longo das eletrocalhas, por meio de marcadores alfanuméricos;
- após conclusão da passagem de cabos, deverá ser efetuado teste de faseamento para que sejam liberadas as instalações dos equipamentos.

O sistema de aterramento deverá possuir as seguintes características mínimas:

- os leitos aramados deverão estar sob o mesmo potencial de terra da sala segura e das demais massas metálicas e subsistemas do prédio;
- para a sala segura e demais salas de apoio ao *datacenter*, deverá existir aterramento destinado a aterrar massas metálicas diversas, tais como carcaças de *racks*, eletrocalhas, eletrodutos e estruturas metálicas diversas;
- possuir aterramento elétrico, destinado a aterrar os equipamentos de ar-condicionado, quadros de energia não estabilizada e equipamentos não estabilizados;
- os dois sistemas de aterramento poderão ter a mesma origem, isto é, o aterramento do edifício;

- o esquema de aterramento deverá seguir o descrito em aterramento e condutores de proteção, contido na Norma NBR-5410.

O subsistema de provimento ininterrupto de energia deverá possuir, ainda, as seguintes características gerais:

- englobar todas as adequações necessárias para a implantação dos *nobreaks* e integração com os atuais grupos geradores, de acordo com as normas técnicas exigíveis ou Especificadas neste documento, tais como fechamento de paredes, acabamentos, pinturas, revestimentos, abertura para cabos em eletrocalhas, quadro de distribuição elétrica, infraestrutura de cabos de alimentação e isolamento, tomadas elétricas, recursos de detecção e combate a incêndios, dentre outros;
- obedecer ao padrão de cores da ABNT para cabos elétricos;
- com relação ao subsistema de provimento ininterrupto de energia, a **contratada** deverá, ainda:
    - efetuar testes de fases, após a conclusão da passagem de cabos e instalação de interruptores e tomadas;
    - prover a seguinte classificação de cargas, conforme sensibilidade, qualidade de energia e importância dentro do sistema:
        - **cargas essenciais:** cargas de equipamentos que não podem sofrer qualquer tipo de alteração na energia elétrica, sendo sua parada extremamente prejudicial. Nessa classificação, estão os equipamentos de processamento de dados e telecomunicações da sala segura, da sala de telecomunicações e do NOC. Pela sua importância, as cargas essenciais deverão ser assistidas pelos UPS;
        - **cargas de emergência:** cargas de equipamentos que deverão ser alimentados pelo grupo gerador e, portanto, não estarão ligados aos UPSs. Nessa classificação estarão os equipamentos UPS, o subsistema de climatização da sala segura, o sistema de iluminação de emergência e o subsistema de detecção e combate a incêndio.

2.5.12 Requisitos para Subsistema de Detecção e Combate a Incêndios

Deverá ser implantado subsistema de detecção precoce e combate a incêndio com, no mínimo, as seguintes especificações técnicas:

- prover, no mínimo, quatro pontos de detecção precoce de incêndio na sala segura, dois na sala de telecomunicações e um na sala de *nobreaks*/UPS, com posicionamento adequado a ser definido pelo projeto executivo do *datacenter*;
- prover sistema de monitoração ativa da atmosfera capaz de coletar amostras do ar por aspiração para detecção de produtos de combustão. Os detectores deverão possuir ajuste automático de sensibilidade para acompanhar as variações entre dias de operação e noites ou dias de inatividade;
- possuir detectores de alta sensibilidade a *laser* e análise estatística por *software*, interligados ao sistema de supervisão e alarmes via TCP/IP;
- possuir monitoração ativa dos aerossóis presentes no ar, interligado ao controle de incêndio;
- utilizar tecnologia a *laser* de contagem de partículas no ar, aliada a *software* de análise em tempo real, capaz de detectar moléculas orgânicas liberadas pelo aquecimento de material elétrico antes da liberação de fumaça. Tal *software* deverá trabalhar com base de dados adquirida para o ambiente onde opera, e deverá permitir que sejam levantados e gravados históricos do nível de qualidade do ar, data/hora e configuração de alarmes predefinida;
- ser constituído por rede de tubos capazes de aspirar amostras de ar através de pequenos orifícios. O ar aspirado deverá ser levado até uma unidade de análise equipada com ventilador, bateria, sistema a *laser*, processador e painel com indicadores visuais e sonoros;
- possuir níveis de análise pré-definidos capazes de ativar alarmes, tais como: alerta, princípio de incêndio e incêndio. A programação deverá ser simples com auxílio de microcomputador. Deverá, ainda, possibilitar a observação do nível de contaminação do processo em tempo real;
- ser integrado via TCP/IP ao Subsistema de Monitoramento Ambiental e Vigilância - CFTV;

- possuir recursos de acionamento automático do sistema de combate a incêndio por laço de detectores de fumaça conectados a um painel central e acionado em caso de confirmação do sistema de monitoração a *laser*. Além da descarga automática, deverá haver acionamento manual e dispositivo que permita o bloqueio do processo de contagem (temporização) em curso para liberação do gás;
- possuir sinalização audiovisual de funcionamento dentro e fora da sala segura e em toda área de abrangência do *datacenter*.
- obedecer às normas legais, técnicas e do Corpo de Bombeiros aplicáveis à situação de cada ambiente do *datacenter*;
- prover painel central de sinalização e comando, capazes de supervisionar e alimentar detectores, ativar alarmes visuais e sonoros de incêndio, bem como efetuar comandos de equipamentos auxiliares;
- especificamente dentro da sala segura e sala de telecomunicações, prover sistema automático de supressão de combustão por inundação completa por agente limpo, a exemplo do FM-200, Inergen ou similares, com as seguintes características:
    - ser composto por cilindros fabricados em aço, com cabeçote de comando elétrico instalado na válvula do cilindro-mestre;
    - ser dimensionado para atender à sala segura através de tubulação, derivações e difusores apropriados, dimensionados conforme devidos cálculos hidráulicos. As tubulações, derivações e difusores devem atender à Norma ASTM-A106;
    - atuar por inundação completa de gás para o ambiente;
    - atender a Norma americana NFPA 2001 ou equivalente.
- Nas demais áreas do data center, prover solução específica para combate a incêndio em equipamentos elétricos, eletrônicos e áreas povoadas, por meio de extintores manuais e portáteis, de acordo com a sua aplicação, atendendo aos requisitos do Corpo de Bombeiros e normas aplicáveis.

2.5.13 Requisitos para subsistema de Controle de Acesso Biométrico

Deverá ser implantado subsistema de controle de acesso biométrico com, no mínimo, as seguintes especificações técnicas:

- prover, no mínimo, quatro pontos de acesso, sendo assim distribuídos:
    - um na porta de entrada da sala do NOC;
    - um na porta da sala de telecomunicações;
    - um na porta de entrada para a sala segura;
    - um na porta da sala de *nobreaks*/UPS.
- possuir tecnologia biométrica digital combinada com uso de senha. Será obrigação da **contratada** realizar sua integração com o mecanismo de travamento das portas fornecidas;
- acompanhar *software* de gerenciamento, sensores que identifiquem quando a porta está aberta, fechaduras eletromagnéticas, leitores de controle de acesso (teclado numérico) e leitores de biometria, em todos os pontos de acesso indicados, com, no mínimo as seguintes características:
    - possuir interface gráfica;
    - possuir funcionalidade de cadastramento de colaboradores com, pelo menos, os campos nome, sobrenome, foto, matrícula, função, área, ramal e perfil de acesso;
    - permitir configuração de perfis de acesso para trânsito de servidores, operadores, administradores, visitantes e terceirizados nos diversos pontos indicados, incluindo definição de tabelas com horários para restrição e permissão de acesso;
    - permitir registro e envio de informações de entrada e saída de colaboradores por meio do protocolo SNMP (*Simple Network Management Protocol*) para *software* de gerenciamento, incluindo eventos e alarmes;
    - permitir geração de relatórios acerca de registro de entrada e saída de colaboradores, incluindo data, hora, nome do usuário e perfil de acesso associado;
    - implementar mecanismos de restrição de acesso ao *software* de gerenciamento por meio de senha;
    - possuir integração com a plataforma Windows, capaz de visualizar foto

e dados de colaboradores quando da ocorrência de eventos e alarmes;

- permitir o envio de comandos às unidades remotas para atuação nos dispositivos de controle, tais como fechaduras;
- permitir armazenamento e preservação de *logs* de todos os eventos de acesso ocorridos nas diversas portas controladas;
- possuir integração com o Subsistema de Monitoramento Ambiental e Vigilância - CFTV.

2.5.14 Requisitos para Subsistema de Climatização de Precisão

Deverá ser fornecido e instalado no ambiente da sala segura do *datacenter* sistema de climatização de precisão com alta vazão, controle de umidade e filtragem eficiente, em conformidade com a NBR 16401 e com, no mínimo, as seguintes especificações técnicas:

- apresentar características de modularidade e ser capaz de operar em modo redundante e contingente, seja por falha de operação ou por manutenção (preventiva ou corretiva), de modo que as unidades restantes possam suportar a carga prevista, em casos de indisponibilidade de alguma. Em casos de interrupção de energia, tais equipamentos devem ser capazes de restabelecer os serviços quando da detecção automática de restauração da alimentação, sem intervenção humana;
- ser capaz de prevenir a entrada de gases de contaminação ou subprodutos de incêndio (fumaça, gases corrosivos, calor) no ambiente da sala segura. Da mesma maneira, deverá conter dispositivo automático de alívio de pressão do gás de extinção de incêndio, sem uso de energia elétrica e com as mesmas características de estanqueidade dos materiais utilizados na sala segura, de modo que possam ser testados em conjunto;
- ser integrado ao subsistema de provimento ininterrupto de energia elétrica, inclusive ao subsistema de provimento de energia elétrica de emergência. A conexão entre esses deverá utilizar recursos de segurança capazes de impedir tentativas de sabotagem e ataques de indisponibilidade;
- as unidades deverão insuflar o ar de modo a atender, de maneira eficiente, os

requisitos de temperatura, umidade e demais características descritas neste documento. A **contratada** apresentará, durante o projeto executivo, sua proposta de arquitetura de resfriamento, que será analisada pelo órgão antes da implantação;

- os equipamentos de ar-condicionado da sala segura deverão possuir, ainda, dispositivos lógicos de acionamento, interligados em rede, capazes de manter as unidades programadas em funcionamento em períodos de rotatividade. Caso haja alguma avaria não reconhecida pelo sistema, deverá ser acionado o equipamento que estiver em *stand by*;
- os equipamentos deverão ser do tipo eletrônico, microprocessado, interligado ao Subsistema de Monitoramento Ambiental e Vigilância - CFTV e apresentar as seguintes funções:
    - monitorar e informar em visor a temperatura da sala;
    - ligar e desligar os condicionadores;
    - promover rodízio dos condicionadores operantes;
    - acionar o condicionador reserva em caso de falha do operante;
    - alarmar a falha dos condicionadores;
    - alarmar temperaturas acima de 25ºC;
    - os parâmetros de alarme devem ser configuráveis pelo usuário.;
- promover o desligamento do ar condicionado quando houver acionamento da detecção de incêndio;
- os equipamentos condensadores deverão ser instalados nas áreas externas seguras, em local a ser definido e dimensionado no projeto executivo do *datacenter.* Áreas externas poderão ser visitadas durante o prazo de vistoria da licitação. Essas unidades deverão ser montadas sobre plataformas metálicas, com mecanismos de alta absorção vibratória. Ademais, deverão ser instaladas em conjunto com recursos de segurança, em especial a conexão entre estes e os equipamentos de evaporação, capazes de prevenir contra tentativas de sabotagem e ataques de indisponibilidade;
- a conexão entre as unidades evaporadoras e condensadoras deverá ser executada em tubulação apropriada e isolada termicamente e contra intempéries;
- todas as tubulações deverão ser apoiadas sobre suportes apropriados, de

modo a evitar a transmissão de vibrações e prover devida sustentação;

- cada elemento de duto deverá ser suspenso ou suportado, de maneira independente e diretamente à estrutura mais próxima, sem conexão com os outros elementos já sustentados. Deverão, ainda, manter espaçamento adequado entre si e não manter contato com paredes. Onde houver passagem de dutos através de paredes, estes deverão estar isolados através de vedação por um elastômero ou produto similar;
- o sistema de passagem e condução da infraestrutura de ar-condicionado na entrada da sala segura deverá prover o mesmo tipo de proteção em termos de estanqueidade do material utilizado em sua confecção;
- deverão ser previstas conexões para teste e leitura de pressão localizadas próximas a descarga dos condicionadores e em todos os locais necessários para se fazer balanceamento adequado de vazões de ar;
- todos os materiais utilizados deverão ser livres de CFC, bem como ser recicláveis;
- os quadros de alimentação e comando para o subsistema de climatização de precisão deverão atender às exigências estabelecidas nas Normas NBR 6808 e IEC 60.439-1, normas similares ou superiores. Neste caso, deverão ser fornecidos, em cada quadro elétrico, diagramas de alimentação, diagramas de comando, diagramas das borneiras e listas com especificação de todos os equipamentos internos. Tais diagramas deverão ser fornecidos em, no mínimo duas cópias, sendo uma instalada internamente ao painel, em suporte específico.

2.5.15 Requisitos para Subsistema de Climatização de Conforto

Deverá ser fornecido sistema de climatização de conforto para a Sala de Telecomunicações, Centro de Monitoramento de Redes (NOC) e Sala de *Nobreaks*, o qual atenda necessidades humanas de climatização, fluxo de ar, retirada e escoamento de calor dos equipamentos instalados no ambiente, tudo em conformidade com a NBR 16401, similar ou superior. O subsistema de climatização de conforto deverá ter, no mínimo, as seguintes

especificações técnicas:

- possuir condensadora remota;
- a conexão entre as unidades evaporadoras e condensadoras deverá ser executada em tubulação apropriada e isolada termicamente e contra intempéries;
- todas as tubulações deverão ser apoiadas sobre suportes apropriados, de modo a evitar a transmissão de vibrações e prover devida sustentação;
- ser modular, com, no mínimo, duas unidades, sendo um efetivo e um reserva, contando com sistema de revezamento automático;
- o sistema deverá contar com um painel de controle que efetuará revezamento, acionamento da unidade em *stand by* em caso de defeito da unidade principal, além de informar ao sistema de monitoração o defeito em uma das unidades;
- os controles e alarmes das unidades de ar condicionado deverão ser eletrônicos, com as seguintes funções:
    - monitorar e informar em visor a temperatura da sala;
    - ligar e desligar os condicionadores;
    - alarmar falhas dos condicionadores;
    - alarmar temperaturas acima de um valor configurável;
    - os parâmetros de alarme devem ser configuráveis pelo usuário;

Além das especificações acima, as salas de *nobreaks* e de telecomunicação deverão contar com as especificações abaixo.

- As salas de *nobreaks* e de telecomunicação deverão contar com, no mínimo, duas unidades em cada sala, sendo um efetivo e um reserva, contando com sistema de revezamento automático.
- Painel de controle que efetuará revezamento, acionamento da unidade em *stand by* em caso de defeito da unidade principal, além de informar ao sistema de monitoração o defeito em uma das unidades.
- Permitir *bypass* para trabalho das máquinas em manual.

2.5.16 Requisitos para Subsistema de Monitoramento Ambiental e de Vigilância (CFTV)

Agregando informações operacionais sobre monitoramento ambiental e de vigilância, assim como outros subsistemas da solução, esse sistema será utilizado como ponto central de monitoramento de toda a solução, a saber.

- Deverá permitir o monitoramento, de forma integrada, dos outros subsistemas que compõem a solução.
- Deverá permitir a geração de relatórios de acompanhamento das condições ambientais para apoiar a tomada de decisão.
- As condições ambientais devem incluir, sem se limitar a esta lista, informações sobre temperatura, umidade, alarmes, eventos e dados de acesso aos ambientes controlados.
- Deverá monitorar e detectar condições ambientais que possam afetar de forma negativa o funcionamento dos equipamentos instalados na sala segura, sala de telecomunicações e sala de *nobreaks*/UPS, e alertar os administradores do sistema quando tais condições ocorrerem.
- Deverá permitir que os operadores no Centro de Monitoramento de Redes possam ser avisados se algum alarme ocorrer e tomar ciência do tipo de alarme ou origem em tempo real.
  - O sistema, composto por *hardware* e *software* deverá permitir o monitoramento dos ambientes à distância, com o uso de câmeras e sensores apropriados.
  - Deverá funcionar ininterruptamente 24 horas por dia, durante 7 dias por semana.
  - Naquilo que for aplicável, o subsistema deve ser construído em conformidade com as Normas NBR 5410, NBR 5474, NBR 5471 e NBR 14565.
  - O subsistema deverá permitir a transmissão dos alarmes via rede, através dos protocolos TCP/IP.
  - Deverá ser fornecido, junto do sistema, *software* para o monitoramento das imagens geradas pelas câmeras, assim como para o gerenciamento de todo o subsistema.
  - O sistema deverá possibilitar comunicação pela rede *ethernet* através do protocolo HTTP para seu gerenciamento e monitoramento (acesso via interface web).
  - A atualização de versões de *software*, *firmware* e suporte técnico deverá ocorrer durante todo o período de vigência do contrato.

- O suporte técnico deverá ser constituído de manutenção preventiva e corretiva.
- A manutenção preventiva deverá contemplar regulagens de foco, manutenção das lentes, substituição de câmeras e quaisquer outras manutenções destinadas a manter a qualidade de captura, gravação, exportação e reprodução das imagens.
- A manutenção deve incluir ainda a troca de quaisquer outros componentes da solução como sensores, cabos e outros.
- O sistema deverá ter seu horário sincronizado via protocolo NTP e permitir a indicação dos servidores NTP que serão utilizados.
- A sincronização do horário via NTP deve ser configurável, pelo menos, no sistema de monitoramento ambiental, no sistema de vigilância (CFTV) e no sistema de gravação de vídeo (DVR).
- A solução deverá incluir equipamentos e softwares necessários para o seu pleno funcionamento, inclusive servidores dedicados, de modo a possibilitar o registro e monitoração de todas as informações descritas nos itens anteriores.
- Possibilitar monitoração e alarme de parâmetros de temperatura, tensão, umidade relativa do ar, estado das portas de acesso, presença de líquido, detecção de incêndio, falha nos equipamentos de climatização, falha de alimentação de energia, sensor de presença, ativação de geradores, ativação dos equipamentos nobreaks/UPS e demais sensores inerentes à solução de data center a ser fornecida.
- O Centro de Monitoramento de Redes será o local onde os responsáveis pelo monitoramento desempenharão suas atividades. A solução de monitoramento deve disponibilizar, para este centro, visão geral dos diversos parâmetros monitorados, principalmente dos sensores da sala segura, da sala de telecomunicações e da sala de nobreaks/UPS.
- O subsistema deverá possuir Circuito Fechado de TV (CFTV) contemplando câmeras de vídeo em quantidade capaz de cobrir todos os pontos da sala segura, da sala de telecomunicações e da sala de UPS. Deverá possuir, ainda, sistema para gravação digital, reprodução e exportação das imagens

capturadas.

- As câmeras de vídeo devem ser posicionadas de forma a cobrir toda a área necessária ao monitoramento, sendo vedada a existência de pontos não cobertos pelas imagens (pontos “cegos”).
- Os sinais de vídeo gerados pelas câmeras convergirão para um equipamento de processamento digital de imagens, que deverá estar ligado ao no-break/UPS do subsistema de provimento ininterrupto de energia e iluminação, e que será instalado em um rack na sala segura.
- O sistema deve executar gravação ininterrupta, diuturnamente, com capacidade de armazenamento de imagens para, no mínimo, 30 (trinta) dias corridos.
- Deverá permitir acesso a imagens já gravadas, exportação e backup (inclusive para mídia removível), sem interrupção da monitoração.
- A solução deve prover controle de acesso lógico às imagens, de forma que apenas usuários cadastrados tenham acesso às mesmas, com níveis de acesso diferenciados por perfil.

2.5.17 Requisitos para Sala de Telecomunicações

Caso seja prevista uma sala de telecomunicações, área destinada a equipamentos de telecomunicações com piso, paredes e teto idênticos aos da sala segura, deverá ter, no mínimo, os seguintes requisitos:

- possuir área interna mínima de 18 m²;
- possuir paredes, porta, piso e teto idênticos aos especificados para a sala segura, incluindo porta de acesso com fechadura e controle de acesso biométrico;
- deverá possuir paredes, piso e teto capazes de prover proteção contra fogo por, no mínimo, 90 minutos, comprovada por certificação obtida a partir de ensaios normatizados, conforme Norma ABNT NBR 10636 (classe CF90), similar ou superior, emitida por Organismo Certificador de Produto (OCP) acreditado pelo INMETRO no escopo adequado. A resistência ao fogo deverá englobar os testes de isolamento térmico, estanqueidade (chamas e gases quentes) e estabilidade (choques mecânicos), nos termos da referida norma;

- caso seja apresentada certificação em norma estrangeira similar ou superior, a certificação deverá ser emitida por Organismo Certificador de Produto do país em questão, desde que o OCP seja devidamente acreditado no escopo adequado por órgão local equivalente ao INMETRO, dotado de acreditação internacional pelo IAF (*International Accreditation Forum*);
- a porta deverá possuir dimensões suficientes para movimentação de equipamentos de TI, com largura entre 1,20 m e 1,30 m, e altura mínima de 2,10 m;
- a porta deverá ser dotada de fechadura com travamento eletromecânico e acionamento automático por leitura biométrica de entrada, conforme Subsistema de Controle de Acesso Biométrico;
- a porta deverá ser capaz de prover proteção contra fogo por, no mínimo, 90 minutos, comprovada por certificação obtida a partir de ensaios normatizados, conforme Norma ABNT NBR 6479, similar ou superior, emitida por Organismo Certificador de Produto (OCP) acreditado pelo INMETRO no escopo adequado. A resistência ao fogo deverá englobar os testes de isolamento térmico, estanqueidade (chamas e gases quentes) e estabilidade (choques mecânicos), nos termos da referida norma;
- para a comprovação da proteção descrita no item anterior, será permitida certificação na Norma ABNT NBR 10636, desde que a porta seja integrada ao corpo de prova, conforme prevê o item 5.3.1 da referida norma, e desde que as verificações de estabilidade, estanqueidade e isolamento térmico na porta sejam feitas de acordo com os métodos específicos descritos na Norma ABNT NBR 6479, conforme prevê o item 5.5.4.2 da Norma ABNT NBR 10636;
- deverá possuir ar-condicionado de conforto suficiente para manter sob controle a temperatura do ambiente em torno de 21ºC, em regime de funcionamento 24x7;
- possuir recursos para passagem de cabos, calhas, canaletas, distribuição, fusão e certificação do sistema de cabeamento estruturado;
- possuir luminárias adequadas ao local de instalação de equipamentos de telecomunicação, dimensionadas de forma a atingir nível adequado de iluminação ao ambiente, nos termos da norma TIA 942, norma similar ou superior;
- possuir luz de emergência e circuito autônomo;

- deverá possuir ponto de telefone integrado à central telefônica do prédio com aparelho fornecido pela **contratada**.

2.5.18 Requisitos para Sala de *Nobreaks*/UPS

A sala deverá ser destinada à instalação dos equipamentos de provimento ininterrupto de energia elétrica UPS (*Uninterruptible Power Systems*), com, no mínimo, as seguintes características:

- possuir área interna mínima de 9 m2;
- possuir porta de acesso com fechadura e controle de acesso biométrico;
- possuir ar-condicionado de conforto para funcionamento 24x7, suficiente para manter sob controle a temperatura do ambiente em torno de 21ºC.

2.5.19 Requisitos para Centro de Monitoramento de Redes (NOC)

A **contratada** deverá possuir sala para o funcionamento de Centro de Monitoramento de Redes (NOC), com, no mínimo, as seguintes especificações:

- possuir área interna mínima de 18 m2;
- ser delimitada por porta de acesso com fechadura e controle biométrico de acesso;
- a porta deverá possuir dimensões suficientes para movimentação de equipamentos de TI, com largura entre 1,20 m e 1,30 m, e altura mínima de 2,10 m;
- possuir ar-condicionado de conforto suficiente para manter sob controle a temperatura do ambiente em torno de 21ºC;
- possuir luminárias adequadas ao local de instalação de equipamentos de telecomunicações, dimensionadas de forma a atingir nível adequado de iluminação, conforme NBR5413, norma similar ou superior;
- possuir luz de emergência e circuito autônomo;
- possuir forro em fibra mineral (Armstrong, Kombimental, Radar ou de características similares ou equivalentes), com modulação 625x625mm, com propriedade termo acústica e resistência a fogo;

- o forro deverá apresentar característica fogo retardante e auto-extinguível com Ip<=25 ,segundo a Norma ABNT NBR 9442; Dm < 450, segundo a Norma ASTM E662; ou apresentar característica de incombustibilidade nos termos da Norma ISO 1182. A comprovação dos parâmetros acima far-se-á por laudo técnico emitido por laboratório acreditado pelo INMETRO no escopo adequado, atestando de forma inequívoca que as características preconizadas na referida norma são atendidas pelo material ofertado. Será aceita ainda comprovação por laboratório estrangeiro, desde que acreditado por órgão do país em questão equivalente ao INMETRO, dotado de acreditação internacional pelo ILAC (*International Laboratory Accreditation Cooperation*).

2.5.20 Requisitos para Suporte Técnico e Manutenção

É recomendado descrever algumas características e obrigações a serem seguidas por ambas as partes do contrato no que diz respeito a Central de Atendimento 24 Horas, suporte técnico e manutenção de infraestrutura.

A descrição dos itens com manutenção observada e cumprida não é obrigatória por ser ampla e já fazer parte da manutenção da infraestrutura compartilhada da empresa **contratada**, porém é possível listar os requisitos de manutenção mínimos, como por exemplo:

- manter as salas-cofre;
- manter as características do piso elevado;
- limpeza e organização;
- manter os sistemas *nobreak*, substituição de baterias e outros componentes perecíveis, conforme recomendação do fabricante;
- manter os sistemas de climatização, de precisão e de conforto de acordo com orientação dos fabricantes;
- manter os sistemas de detecção e combate a incêndio;
- manter os sistemas de controle biométrico de acesso, de monitoramento ambiental e vigilância;
- manter o sistema de cabeamento estruturado;
- manter os sistemas de monitoramento ambiental e vigilância de acordo com orientação dos fabricantes;

- manter os equipamentos integrantes do NOC (*Network Operation Center*) de acordo com orientação dos fabricantes;
- treinamento e aperfeiçoamento profissional dos funcionários diretamente envolvidos;
- manter auditoria física constante.

Abaixo, alguns outros exemplos do que pode ser levado em conta ao tratar sobre o assunto.

- Fornecer e substituir componentes que apresentarem defeitos ou desgastes, identificados dentro das condições normais de operação ou que necessitarem reposição em virtude da evolução de outros componentes da solução.
- A substituição de componente deverá ser efetuada por outro de configuração idêntica ou superior, original, novo e de primeiro uso, sem ônus adicional para a **contratante**.
- Manutenção do piso, incluindo substituição de partes defeituosas ou que sofreram danos pelo uso regular.
- Fornecer e instalar, para o sistema de climatização, gás, correias, filtros, lubrificantes e quaisquer outros materiais necessários à realização dos serviços de manutenção.
- Instalar e remover cabos na sala-cofre sempre que a **contratante** tiver necessidade de instalar novos equipamentos ou executar serviços que demandem inserção ou remoção de cabos. Nesses casos, caberá à **contratada** manter a estanqueidade e as condições de resistência a fogo da sala-cofre e sala de telecomunicações.
- A **contratada** deverá fazer a manutenção do gerador adquirido, dos UPS (*Uninterruptible Power Supply*) e dos quadros de energia elétrica fornecidos como parte da solução.
- Os chamados de manutenção e suporte técnico on-site deverão ser abertos por meio de central de abertura de chamados, em regime 24X7 (vinte quatro horas ao dia, todos os dias da semana, inclusive sábados, domingos e feriados). No momento da abertura do chamado, deverá ser fornecido à **contratante** um

número único de identificação do chamado.

- Os dados dos chamados, bem como das providências tomadas, devem ser armazenados em sistema para controle de chamados. Esse sistema deverá estar disponível ao acesso da **contratante** e ter capacidade de apresentar número do chamado, data e hora de abertura, nome da pessoa que abriu e do técnico alocado, descrição dos problemas, bem como dados das atividades executadas, data e hora de fechamento do chamado e solução aplicada.
- Com exceção de paradas programadas e acordadas previamente, nenhuma manutenção deverá acarretar parada das atividades do d*atacenter*.
- Os chamados somente poderão ser fechados após autorização da **contratante**.
- A **contratada** deverá encaminhar relatório mensal com todos os chamados de manutenção e suporte técnico, abertos e fechados, contendo os detalhes de abertura e fechamento do chamado e da solução aplicada.
- Os chamados poderão ser abertos segundo os níveis de severidade e de serviços (SLA) a seguir indicados, a saber.
    - a) A classificação da severidade do evento será determinada a critério da **contratante**, pela sua necessidade, respeitando-se o descrito na Tabela 2.5.1.
    - b) Todos os tempos especificados na Tabela 2.5.2 são contados a partir da abertura do respectivo chamado técnico.
    - Foi estipulado, conforme Tabelas 2.5.1 e 2.5.2, prazos máximos para reestabelecimento do sistema, com base na severidade da solicitação, contado a partir do momento em que for realizada a solicitação de atendimento técnico pela **contratante**.

Entende-se como atendimento a instalação, configuração, reinstalação ou o restabelecimento à normalidade, através de intervenção local, dos recursos computacionais que motivaram os usuários a abertura de um chamado no Central de Atendimento 24 Horas ou *Help Desk*.

Entende-se pelo início do atendimento técnico presencial o momento de chegada do técnico ao local onde está instalado o equipamento.

- A cada atendimento técnico presencial, a **contratada** deverá apresentar "Relatório de Visita", contendo hora de chamada, início e término do atendimento, identificação do problema, providências adotadas e outras informações que sejam pertinentes, a ser assinada pela **contratante** e pelo responsável pela manutenção.
- O atendimento de um chamado técnico só será considerado solucionado após atesto da **contratante**.
- Será estipulado um prazo máximo para substituição de peças, caso estas apresentem problemas, ainda que a peça não cause problema aparente no funcionamento do equipamento, com base na severidade da solicitação, contado a partir do momento em que for realizada a solicitação de atendimento técnico pela **contratante**.
- Caso algum equipamento apresente problema e fique indisponível, e a **contratada** não consiga recolocá-lo em funcionamento em até 36 (trinta e seis) horas contados da abertura do chamado, o equipamento poderá ser substituído pela **contratada**, a critério e sem custo adicional para a **contratante**.
- Entende-se por término de reparo a disponibilidade do equipamento para uso em perfeitas condições de funcionamento, no local onde estiver instalado, atestado pela **contratante**.

CLASSIFICAÇÃO DE EVENTOS	
(A) EMERGENCIAL	São consideradas como "Emergência" todas as falhas cujas consequências tenham impactos sobre o serviço, o tráfego de dados e sincronismo e/ou recursos de manutenção (Ex.: sistema de gerência) que exigem ação corretiva imediata (independente da hora do dia ou do dia da semana). **Ex.: Perda de tráfego, paralização ou intermitência de serviços, gerência ou replicação de dados.**
(B) ALTA PRIORIDADE	Situações que podem configurar uma severidade emergencial. São situações potenciais e exigem atenção imediata. São situações potenciais que precedem, em sua maioria, uma situação que pode ser classificada num segundo momento como severidade emergencial. **Ex.: Perda de redundância ou situação de funcionamento parcial que pode levar a interrupção de serviços.**

(C) MÉDIA PRIORIDADE	Problemas que não prejudicam significativamente o funcionamento dos sistemas / serviços. São problemas graves ou perturbações que afetam uma área específica de determinada funcionalidade. Exemplos: degradação de desempenho, perda de funcionalidades. **Ex.: Sistema de gerência com funcionalidade limitada**
(D) BAIXA PRIORIDADE E CONSULTA	Consulta geral e problemas secundários que têm um efeito pequeno na funcionalidade do produto. **Ex.: Falhas de documentação, falhas no projeto e questionamentos operacionais.**

Tabela 2.5.1 - Lista de classificação de eventos

NÍVEL	SEVERIDADE	TEMPO PARA RESTABELECIMENTO DO SISTEMA APÓS ABERTURA DO CHAMADO	TEMPO PARA SOLUÇÃO DEFINITIVA DO PROBLEMA
A	**EMERGENCIAL**	Até 01 hora	Até 04 dias corridos
B	**ALTA PRIORIDADE**	Até 02 horas	Até 07 dias corridos
C	**MEDIA PRIORIDADE**	Até 04 horas	Até 10 dias corridos
D	**BAIXA PRIORIDADE E CONSULTA**	1 dia	

Tabela 2.5.2 - Lista de classificação de eventos

2.6 Acordos de Níveis de Serviço

O principal instrumento para verificação da adequação dos serviços é o Acordo de Nível de Serviço (ANS ou SLA, do inglês *Service Level Agreement*), estabelecido entre as partes envolvidas. Durante a execução do contrato, a **contratante**, sempre que julgar conveniente e oportuno, revisará os padrões mínimos de qualidade, com o objetivo de adequá-lo à realidade da execução contratual.

Este item estabelece critérios quantitativos e qualitativos para a prestação de serviços técnicos e poderá ser adaptado ao longo da execução do contrato, de forma a corrigir falhas conceituais, legais e operacionais verificadas na execução prática dos serviços prestados,

desde que não onere esta prestação em execução e sem prejudicar a segurança institucional.

Um acordo de nível de serviços é um documento que declara as partes envolvidas; as condições do acordo, que serviços de suporte e aplicações estão incluídos; penalidades para o não cumprimento do acordo; pagamentos de honorários; políticas adotadas; termos de modificações; relatórios (frequência de geração do relatório e o nível de detalhe da informação); e responsabilidades de ambas as partes [31].

Os principais benefícios de um SLA são os seguintes [32].

- Estabelecer uma via de responsabilidade de mão dupla.
- Criar níveis de serviço negociados e padronizados.
- Documentar níveis de serviço.
- Definir claramente critérios para a avaliação do serviço.
- Fornecer uma base para melhoria de níveis de serviço.
- Padronizar métodos para comunicar as expectativas de serviço.

A definição de critérios e indicadores objetivos, claramente mensuráveis e com apuração rápida é uma das questões mais importantes num SLA, minimizando a subjetividade na avaliação da **contratante** e da **contratada** sobre o serviço prestado.

O conteúdo básico de um SLA é o mesmo de um contrato padrão de fornecimento de serviços [33], acrescido de cláusulas específicas [34], por exemplo, como os itens a seguir.

- Definição e escopo detalhado do serviço/ produto (o que se inclui e o que se exclui).
- Horário de atendimento e prestação de serviços.
- Contatos e procedimentos para requisição de serviços.
- Pré-requisitos do cliente; metas mensuráveis.
- Disponibilidade.
- Metas de desempenho/ capacidade do serviço (tempo de resposta, volume) incluindo prazos limite para determinados dias.
- Continuidade.
- Segurança.
- Padrões e procedimentos.
- Definições e situações de emergência.

- Reclamações e procedimentos de escalação.
- Procedimentos de mudança.
- Relatórios que devem ser produzidos.
- Frequência das reuniões de revisão.
- Contabilidade de custos e cobrança (se aplicável).
- Regulamento de bônus / multas.

Para os Acordos de Nível de Serviço pode-se, também, levar em consideração os seguintes aspectos.

- Aplicação: os ANS serão aplicados tanto aos serviços essenciais de infraestrutura como às solicitações ou incidentes registrados que dizem respeito à **contratada**.
- Melhoria: objetivando a qualidade, a **contratada** deverá estabelecer procedimentos e condições que permitam a melhoria contínua dos serviços prestados.
- Relatórios: foram definidas três periodicidades de medição dos indicadores de nível de serviço:
    - mensal: a **contratada** entregará, até o terceiro dia útil do mês subsequente ao mês que será medido, o relatório referente à medição do ANS desse período para a **contratante** em um formato acordado entre as duas partes;
    - trimestral: a **contratada** entregará, até o terceiro dia útil do mês subsequente ao período de três meses que será medido, o relatório referente à medição do ANS desse período para a **contratante** em um formato acordado entre as duas partes;
    - anual: a **contratada** entregará, até o terceiro dia útil do mês subsequente ao período de um ano que será medido, o relatório referente à medição do ANS desse período para a **contratante** em um formato acordado entre as duas partes.
- Penalidades: o não cumprimento de um ou vários indicadores do ANS ocasionará a aplicação de multas por parte da **contratada**, conforme penalidades especificadas no contrato.

Um ANS pode ser criado e conter descrições específicas para diversas áreas, como, por exemplo, as que serão descritas a seguir.

- Acompanhamento e registro de disponibilidade de energia elétrica em 100% em 24x7 (Vinte quatro horas ao dia, todos os dias da semana, inclusive sábados, domingos e feriados).
- Acompanhamento e registro de disponibilidade do serviço de climatização controlando temperatura e umidade.
- Acompanhamento e registro de processos de segurança: CFTV, catracas eletrônicas, controle de entradas, etc.
- Acompanhamento e registro de processos de gestão: relatório de incidentes, problemas e mudanças relacionadas a infraestrutura elétrica e de climatização.
- Especificações sobre procedimentos de recuperação.
- Especificações sobre manutenções e testes.
- Especificações sobre sanções e penalidades.
    - Por meio de IQS - Índice de Qualidade de Serviço, apurado mensalmente.
    - Por eventos de indisponibilidade.
- Garantia de qualidade do serviço e penalidades: o ANS demonstra o comprometimento da **contratada** no fornecimento do mais alto nível de desempenho. Caso não atinja os parâmetros de ANS contratados, poderão ser descritas sanções administrativas ou financeiras.
- Especificações para disponibilidade de infraestrutura (definida pela manutenção do fornecimento de energia e pela manutenção dos sistemas de climatização dentro de limites pré-definidos.
- Especificações para conectividade IP, latência e perda de pacote.

2.6.1 Exemplos de acordo de Nível de Serviço

2.6.1.1 Energia elétrica

A **contratada** deve garantir um alto grau de disponibilidade do fornecimento de energia elétrica além de possuir contratos de manutenção com fornecedores dos ativos necessários para garantir a redundância da infraestrutura que suporta esse serviço, bem como realizar manutenções preventivas e testes de ativação de redundância. Logo abaixo, nas Tabelas 2.6.1 a 2.6.4, podem ser observados os indicadores de nível desse serviço.

Indicador	Apresentação de contrato de fornecedor para reparo e manutenção de equipamentos de sistema elétrico.
Serviço	Energia elétrica
Processo	Gerenciamento de fornecedores
Tipo	Apresentação de documentação e auditoria
Periodicidade	Anual
Definição	Apresentar documentação que comprove contrato vigente, junto a empresa responsável pela manutenção preventiva e corretiva dos equipamentos que compões o sistema elétrico.
Unidade de Medida	Percentual (%)
Objetivo	Cumprimento 100%
Observação	A apresentação dessa documentação deverá ser feita até o terceiro dia útil após a data de início do contrato, e a cada 12 (doze) meses contados a partir desse início.
Considerações Gerais	Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.1 - Apresentação de contrato de fornecedor para reparo e manutenção de equipamentos de sistema elétrico

Indicador	Disponibilidade de fornecimento de alimentação elétrica do CPD
Serviço	Energia elétrica
Processo	Gerenciamento de disponibilidade
Tipo	Disponibilidade de serviços
Periodicidade	Mensal

Definição	Disponibilidade total do fornecimento de energia elétrica
Fórmula de cálculo	ANS = 100 * [(T_{total} – T_{indisp}) / T_{total}]
Detalhamento	T_{total} = Tempo total no período em minutos. T_{indisp} = Tempo total de indisponibilidade no período em minutos.
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 99,8%
Considerações Gerais	O cálculo do T_{indisp} deverá ser feito através de sistema de monitoramento dos circuitos elétricos entregues, por exemplo, através de quadros de distribuição gerenciais, permitindo a exportação de relatórios para auditoria e comprovação do ANS apresentado. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.2 - Disponibilidade de fornecimento de alimentação elétrica do CPD

Indicador	Disponibilidade de fornecimento de alimentação elétrica para áreas de pessoal
Serviço	Energia elétrica
Processo	Gerenciamento de disponibilidade
Tipo	Disponibilidade de serviços
Periodicidade	Mensal
Definição	Disponibilidade total do fornecimento de energia elétrica para as áreas de pessoal, a fim de garantir as atividades laborais.
Fórmula de cálculo	ANS = 100 * [(T_{total} – T_{indisp}) / T_{total}]

Detalhamento	T_{total} = Tempo total no período em minutos. T_{indisp} = Tempo total de indisponibilidade no período em minutos, desconsiderando-se os 5 minutos iniciais para ativação do Grupo Gerador.
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 99,5%
Considerações Gerais	O fornecimento de energia elétrica deve ser garantido através de geradores, porém sem a necessidade de utilização de UPS, portanto tolerando pequenos períodos para ativação a contingência. O cálculo do T_{indisp} será feito através de análise de chamados manualmente para cada incidente específico. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS.

Tabela 2.6.3 - Disponibilidade de fornecimento de alimentação elétrica das demais áreas (Todas exceto o CPD)

Indicador	Manutenção preventiva periódica de equipamentos do sistema elétrico
Serviço	Energia elétrica
Processo	Gerenciamento de disponibilidade
Tipo	Manutenções periódicas
Periodicidade	Mensal
Definição	Manutenção preventiva periódica dos equipamentos que compõe o sistema elétrico
Fórmula de cálculo	ANS = 100 * [(Q_{total} – Q_{indisp}) / Q_{total}]

Detalhamento	Q_{total} = Quantidade total de manutenções previstas no período. Q_{indisp} = Quantidade de manutenções programadas não realizadas no período.
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 80,0%
Considerações Gerais	Até o terceiro dia útil após o início do contrato, a **contratada** deverá apresentar seu plano de manutenção preventiva com calendário e datas a serem cumpridas. Esse planejamento deverá ser apresentado ao **contratante** e aprovado pelo mesmo. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.4 - Manutenção preventiva periódica de equipamentos do sistema elétrico

2.6.1.2 Climatização

A **contratada** deve possuir contrato de manutenção com fornecedores dos ativos necessários para garantir a climatização constante do ambiente, bem como realizar todas as manutenções preventivas e testes de ativação de redundância necessários.

Deve também acompanhar e registrar apenas a disponibilidade do serviço de climatização controlando temperatura e umidade. Não será admitida parada total do sistema de refrigeração. A temperatura deverá oscilar entre 22°C ± 1,2°C (>20,8°C<23,3°C) e o percentual de umidade deve ser de 50% ± percentual de 10% (>45% <55%).

Nas tabelas 2.6.5 a 2.6.9 abaixo, são mostrados alguns exemplos do acordo.

Indicador	Apresentação de contrato de fornecedor para reparo e manutenção de equipamentos de sistema de climatização.
Serviço	Climatização
Processo	Gerenciamento de fornecedores

Tipo	Apresentação de documentação e auditoria
Periodicidade	Anual
Definição	Apresentar documentação que comprove contrato vigente, junto à empresa responsável pela manutenção preventiva e corretiva dos equipamentos que compões o sistema de climatização.
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 100%
Observação	A apresentação dessa documentação deverá ser feita até o terceiro dia útil após a data de início do contrato, e a cada 12 (doze) meses contados a partir desse início.
Considerações Gerais	Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.5 - Apresentação de contrato de fornecedor para reparo e manutenção de equipamentos de sistema de climatização.

Indicador	Controle de temperatura no ambiente do CPD
Serviço	Climatização
Processo	Gerenciamento de fornecedores
Tipo	Disponibilidade de serviços
Periodicidade	Mensal
Definição	Controle de temperatura do ambiente de equipamentos do CPD, garantindo que o mesmo esteja sempre dentro de uma faixa de operação considerada normal.
Fórmula de cálculo	ANS = 100 * [($Temp_{total}$ – $Temp_{anormal}$) / $Temp_{total}$]
Detalhamento	$Temp_{total}$ = Total de aferições de temperatura no período $Temp_{anormal}$ = Total de aferições fora da faixa de normalidade no período
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 99,5% Faixa de Normalidade 18ºC ≤ ANS ≤ 24ºC

Considerações Gerais	As aferições devem ser realizadas através de um sistema por sensores, com possibilidade de exportação dos dados para geração do relatório, possibilitando auditoria. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.6 - Controle de temperatura no ambiente do CPD

Indicador	Controle de temperatura no ambiente de todas as áreas (exceto o CPD)
Serviço	Climatização
Processo	Gerenciamento de fornecedores
Tipo	Disponibilidade de serviços
Periodicidade	Mensal
Definição	Controle de temperatura do ambiente em todas as áreas internas, exceto na área do CPD, garantindo que a mesma esteja sempre dentro de uma faixa de operação considerada normal.
Fórmula de cálculo	ANS = 100 * [($Temp_{total}$ – $Temp_{anormal}$) / $Temp_{total}$]
Detalhamento	$Temp_{total}$ = Total de aferições de temperatura no período $Temp_{anormal}$ = Total de aferições fora da faixa de normalidade no período
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 99,5% Faixa de Normalidade 20ºC ≤ ANS ≤ 26ºC
Considerações Gerais	As aferições devem ser realizadas através de um sistema por sensores, com possibilidade de exportação dos dados para geração do relatório, possibilitando auditoria. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.7 - Controle de temperatura no ambiente de todas as áreas (exceto o CPD)

Indicador	Controle de umidade no ambiente do CPD

Serviço	Climatização
Processo	Gerenciamento de fornecedores
Tipo	Disponibilidade de serviços
Periodicidade	Mensal
Definição	Controle de umidade do ambiente de equipamentos do CPD, garantindo que a mesma esteja sempre dentro de uma faixa de operação considerada normal.
Fórmula de cálculo	ANS = 100 * [($Umid_{total}$ – $Umid_{anormal}$) / $Umid_{total}$]
Detalhamento	$Umid_{total}$ = Total de aferições de umidade no período $Umid_{anormal}$ = Total de aferições fora da faixa de normalidade no período
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 99,5% Faixa de Normalidade 45% ≤ ANS ≤ 55%
Considerações Gerais	As aferições devem ser realizadas através de um sistema por sensores, com possibilidade de exportação dos dados para geração do relatório, possibilitando auditoria. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.8 - Controle de umidade no ambiente do CPD

Indicador	Manutenção preventiva e periódica de aparelhos de climatização
Serviço	Climatização
Processo	Gerenciamento de fornecedores
Tipo	Disponibilidade de serviços
Periodicidade	Trimestral
Definição	Manutenção preventiva e periódica de equipamentos que compõem o sistema de climatização.
Fórmula de cálculo	ANS = 100 * [(Q_{total} – $Q_{anormal}$) / Q_{total}]
Detalhamento	Q_{total} = Quantidade total de manutenções previstas no período $Q_{anormal}$ = Quantidade de manutenções programadas não realizadas no período

Unidade de medida	Percentual (%)
Objetivo	Cumprimento 80%
Considerações Gerais	Até o terceiro dia útil após o início do contrato, a **contratada** deverá apresentar seu plano de manutenção preventiva com calendário e datas a serem cumpridas. Esse planejamento deverá ser apresentado ao **contratante** e aprovado pelo mesmo. O calendário deve incluir pelo menos 01 (uma) manutenção a cada trimestre. Se houver a penalidade, esta será aplicada na fatura relativa ao último mês do trimestre em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.9 - Manutenção preventiva e periódica de aparelhos de climatização

2.6.1.3 Conectividade

A **contratada** deve possuir equipe própria ou contratos de manutenção com fornecedores que garantam a manutenção e reparo dos enlaces de fibra óptica imediatamente no caso de incidentes (ver tabelas 2.6.10 a 2.6.11).

Indicador	Disponibilidade da conectividade por fibra óptica
Serviço	Conectividade
Processo	Gerenciamento de disponibilidade
Tipo	Disponibilidade de serviços
Periodicidade	Mensal
Definição	Disponibilidade total da conectividade por fibra óptica da **contratante**, onde pelo menos 01 (um) dos enlaces deve estar operando, para garantir a conectividade aos ativos.
Fórmula de cálculo	ANS = 100 * [(T_{total} – $T_{anormal}$) / T_{total}]
Detalhamento	T_{total} = Tempo total no período em minutos $T_{anormal}$ = Tempo total de indisponibilidade no período em minutos
Unidade de medida	Percentual (%)

Objetivo	Cumprimento 99,5%
Considerações Gerais	A **contratada** deve fazer o monitoramento dos enlaces através de um sistema, o qual permita contabilizar o nível de disponibilidade dos mesmos para confecção dos índices mensais. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte. No caso das fibras que serão entregues "apagadas", o **contratante** fornecerá as informações de indisponibilidade.

Tabela 2.6.10 - Disponibilidade da conectividade por fibra óptica

Indicador	Reparo de enlace de redundância de fibra óptica de comunicação
Serviço	Conectividade
Processo	Gerenciamento de disponibilidade
Tipo	Disponibilidade de serviços
Periodicidade	Mensal
Definição	Reparo ou recuperação de enlaces de fibra óptica, que estejam operando em contingência, sem sua redundância, porém sem causar indisponibilidade no serviço.
Fórmula de cálculo	$ANS = 100 * [(T_{total} - T_{anormal}) / T_{total}]$
Detalhamento	T_{total} = Tempo total no período em minutos $T_{anormal}$ = Tempo total de reparo do equipamento, no período em minutos
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 98%
Considerações Gerais	A **contratada** deve fazer o monitoramento dos enlaces através de um sistema, o qual permita contabilizar o nível de disponibilidade dos mesmos para confecção dos índices mensais. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.11 - Reparo de enlace de redundância de fibra óptica de comunicação

2.6.1.4 Controle de Incêndio

A **contratada** deve possuir contratos de manutenção com fornecedores dos ativos necessários para garantir a proteção constante do ambiente do CPD, bem como das demais áreas, realizando todas as manutenções preventivas e respectivos reparos, quando necessário (ver tabelas 2.6.12 a 2.6.16).

Indicador	Apresentação de contrato de fornecedor para reparo e manutenção de Sistema de Controle de Incêndio
Serviço	Controle de incêndio
Processo	Gerenciamento de fornecedores
Tipo	Apresentação de documentação e auditoria
Periodicidade	Anual
Definição	Apresentar documentação, a qual comprove contrato vigente junto à empresa responsável pela manutenção preventiva e corretiva dos equipamentos de detecção e combate a incêndio, inclusive do sistema de combate por gás.
Fórmula de cálculo	ANS = 100 * [(T_{total} – $T_{anormal}$) / T_{total}]
Detalhamento	T_{total} = Tempo total no período em minutos $T_{anormal}$ = Tempo total de reparo do equipamento, no período em minutos
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 100%
Observação	A apresentação dessa documentação deverá ser feita até o terceiro dia útil após a data de início do contrato e a cada 12 (doze) meses contados a partir desse início.
Considerações Gerais	Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.12 - Apresentação de contrato de fornecedor para reparo e manutenção de

Indicador	Apresentação de certificados de capacitação da brigada anti-incêndio
Serviço	Controle de incêndio
Processo	Gerenciamento de fornecedores
Tipo	Apresentação de documentação e auditoria
Periodicidade	Anual
Definição	Apresentar documentação, a qual comprove a capacitação de brigadistas da equipe da **contratada**, de acordo com a quantidade de funcionários da instalação. A quantidade de brigadistas deve considerar, inclusive, os recursos da **contratante**, que estarão alocados no ambiente.
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 100%
Observação	A apresentação dessa documentação deverá ser feita até o terceiro dia útil após a data de início do contrato, e a cada 12 (doze) meses contados a partir desse início.
Considerações Gerais	Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.13 - Apresentação de certificados de capacitação da brigada anti-incêndio

Indicador	Manutenção periódica preventiva de sistema de controle de incêndio
Serviço	Controle de incêndio
Processo	Gerenciamento de fornecedores
Tipo	Manutenções periódicas
Periodicidade	Semestral
Definição	Apresentar documentação, a qual comprove contrato vigente junto à empresa responsável pela manutenção preventiva e

	corretiva dos equipamentos de detecção e combate a incêndio, inclusive do sistema de combate por gás.
Fórmula de cálculo	ANS = 100 * [(Q_{total} – $Q_{anormal}$) / Q_{total}]
Detalhamento	Q_{total} = Quantidade total de manutenções previstas no período $Q_{anormal}$ = Quantidade de manutenções programadas não realizadas no período
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 80%
Considerações Gerais	No início da operação do contrato, a **contratada** deverá apresentar seu plano de manutenção preventiva com calendário e datas a serem cumpridas. O calendário deve incluir pelo menos 01 (uma) manutenção a cada semestre para cada um dos itens definidos acima. Se houver penalidade, esta será aplicada na fatura relativa ao último mês do semestre em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.14 - Manutenção periódica preventiva de sistema de controle de incêndio

Indicador	Testes periódicos de detecção e disparo de sistema de controle de incêndio
Serviço	Controle de incêndio
Processo	Gerenciamento de fornecedores
Tipo	Validações periódicas
Periodicidade	Anual
Definição	Todos os itens do sistema de controle de incêndio devem ser testados, a fim de garantir seu correto funcionamento no caso de incidentes.
Fórmula de cálculo	ANS = 100 * [(Q_{total} – $Q_{anormal}$) / Q_{total}]
Detalhamento	Q_{total} = Quantidade total de manutenções previstas no período $Q_{anormal}$ = Quantidade de manutenções programadas não realizadas no período
Unidade de medida	Percentual (%)

Objetivo	Cumprimento 80%
Considerações Gerais	No início da operação do contrato, a **contratada** deverá apresentar seu plano de testes com calendário e datas a serem cumpridas. O calendário deve incluir pelo menos 01 (um) teste anual para cada item definido acima. Se houver penalidade, esta será aplicada na fatura relativa ao último mês do ano em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.15 - Testes periódicos de detecção e disparo de sistema de controle de incêndio

Indicador	Simulação de evacuação para brigada de incêndio
Serviço	Controle de incêndio
Processo	Gerenciamento de fornecedores
Tipo	Validações periódicas
Periodicidade	Anual
Definição	Devem ser realizados testes periódicos de evacuação e simulação de incêndio nas dependências da **contratada**, a fim de garantir a segurança das pessoas e a continuidade do negócio.
Fórmula de cálculo	ANS = 100 * [(Q_{total} – $Q_{anormal}$) / Q_{total}]
Detalhamento	Q_{total} = Quantidade total de manutenções previstas no período $Q_{anormal}$ = Quantidade de manutenções programadas não realizadas no período
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 80%
Considerações Gerais	No início da operação do contrato, a **contratada** deverá apresentar seu plano de testes com calendário e datas a serem cumpridas. O calendário deve incluir pelo menos 01 (uma) simulação anual. Se houver penalidade, esta será aplicada na fatura relativa ao último mês do ano em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.16 - Simulação de evacuação para brigada de incêndio

2.6.1.5 Segurança

A **contratada** deve manter os mais altos níveis de segurança física e lógica, controlando o acesso às áreas exclusivas da **contratante** e possibilitando auditoria de todos os seus sistemas (ver tabelas 2.6.17 a 2.6.19).

Indicador	Apresentação de contrato de fornecedor segurança patrimonial armada
Serviço	Segurança
Processo	Gerenciamento de fornecedores
Tipo	Apresentação de documentação e auditoria
Periodicidade	Anual
Definição	Apresentar documentação, a qual comprove contrato vigente, junto a empresa de segurança patrimonial armada para as instalações da **contratada**.
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 100%
Observação	A apresentação dessa documentação deverá ser feita até o terceiro dia útil após a data de início do contrato, e a cada 12 (doze) meses contados a partir desse início.
Considerações Gerais	Se houver penalidade, esta será aplicada na fatura relativa ao último mês do ano em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.17 - Apresentação de contrato de fornecedor segurança patrimonial armada

Indicador	Apresentação de relatório para auditoria dos sistemas de controle de acesso
Serviço	Segurança
Processo	Gerenciamento de Segurança

Tipo	Apresentação de documentação e auditoria
Periodicidade	Mensal
Definição	Apresentar relatório para auditoria com os seguintes itens. • Relação de permissão de usuários do sistema de controle de acesso. • Relatório de entrada e saída de pessoas de áreas restritas a **contratante**.
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 100%
Considerações Gerais	Mensalmente os relatórios definidos acima devem ser apresentados, para que o **contratante** possa auditar os acessos realizados. A alteração de permissões de pessoas no sistema de controle de acesso deverá ser realizada sempre mediante abertura e chamado, os quais podem ser solicitados pela **contratante** para ajudar na análise da auditoria do sistema. Se penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.18 - Apresentação de relatório para auditoria dos sistemas de controle de acesso

Indicador	Apresentação de relatório de eventos dos sistemas de câmeras e gravação
Serviço	Segurança
Processo	Gerenciamento de Segurança
Tipo	Apresentação de documentação e auditoria
Periodicidade	Mensal
Definição	Apresentar relatório para auditoria com os *logs* de eventos do sistema de câmeras e gravação.
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 100%

Considerações Gerais	Mensalmente o relatório do sistema de câmeras e gravação deve ser apresentado para que a **contratante** possa auditar os acessos realizados. Qualquer alteração no sistema de controle de câmeras e gravação deverá ser realizada sempre mediante abertura e chamado, os quais podem ser solicitados pela **contratante** para ajudar na análise da auditoria do sistema. Uma amostragem de imagens pode ser solicitada pela **contratante**, a fim de garantir a retenção mínima das mesmas. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.19 - Apresentação de relatório de eventos dos sistemas de câmeras e gravação

2.6.1.6 Central de Suporte

Atendimento a chamados de incidentes.

Indicador	Atendimento de chamados de incidentes
Serviço	Central de Suporte
Processo	Gerenciamento de incidentes
Tipo	Atendimento ao usuário
Periodicidade	Mensal
Definição	Apresentar relatório de atendimentos solicitados no período para solução de incidentes. Os incidentes serão classificados de acordo com critério já estipulados em contrato.
Fórmula de cálculo	ANS = 100 * [(Q_{total} – Q_{fp}) / Q_{total}]
Detalhamento	Q_{total} = Quantidade total de manutenções previstas no período Q_{fp} = Quantidade de manutenções programadas não realizadas no período
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 90%. Prazos estipulados em contato.
Considerações	Os incidentes tratados nesse item são todos aqueles que não

Gerais	foram relacionados, até então, neste anexo. O ANS para chamados deverá ser extraído do próprio sistema de atendimentos e apresentado na sua forma original, bem como na forma de relatório gerencial, para facilitar sua análise. O modelo do relatório pode ser definido em conjunto entre a **contratada** e **contratante** no início da prestação de serviço. Pequenas alterações podem ser solicitadas, desde que não incorram em aumento de mão de obra para geração das mesmas. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.20 - Atendimento de chamados de incidentes.

Indicador	Atendimento de chamados de requisição de solicitações
Serviço	Central de Suporte
Processo	Gerenciamento de incidentes
Tipo	Atendimento ao usuário
Periodicidade	Mensal
Definição	Apresentar relatório de atendimentos solicitados no período para solução de incidentes. As solicitações serão classificadas de acordo com critério já estipulados em contrato.
Fórmula de cálculo	ANS = 100 * [(Q_{total} – Q_{fp}) / Q_{total}]
Detalhamento	Q_{total} = Quantidade total de manutenções previstas no período Q_{fp} = Quantidade de manutenções programadas não realizadas no período
Unidade de medida	Percentual (%)
Objetivo	Cumprimento 90%. Prazos estipulados em contato.
Considerações Gerais	O ANS para chamados deverá ser extraído do próprio sistema de atendimentos e apresentado na sua forma original, bem como na forma de relatório gerencial, para facilitar sua análise. O modelo do relatório pode ser definido em conjunto entre a **contratada** e **contratante** no início da prestação de serviço.

	Pequenas alterações podem ser solicitadas, desde que não incorram em aumento de mão de obra para geração das mesmas. Se houver penalidade, esta será aplicada na fatura relativa ao mês em que ocorreu o descumprimento do ANS ou na fatura seguinte.

Tabela 2.6.20 - Atendimento de chamados de requisição de solicitações.

2.6.1.7 Penalidades

O sistema de penalidade fica estabelecido da seguinte forma.

- Cada indicador tem um Nível de Serviço associado ou ANS e seu não cumprimento será objeto de uma penalidade, segundo especificado a seguir e conforme os valores indicados no item “Cálculos” que serão descritos adiante.
- O **contratante** deverá analisar as causas do não cumprimento e identificar as ações requeridas para corrigir as anomalias. Em caso de que o resultado de um indicador não for informado, será considerado não cumprido e lhe será aplicada a penalidade correspondente, salvo se razoavelmente justificado.
- O valor das penalizações será um percentual sobre o valor total da fatura de serviço do mês corrente, emitida pela **contratada** para a **contratante**, sendo esta multa recolhida na fatura emitida no mês subsequente. As penalidades indicadas abaixo, somente serão aplicáveis no caso das causas de origem, serem de responsabilidade da **contratada** ou de seus subcontratados.

2.6.1.8 Cálculos

A Tabela de Penalidades para os ANS será estabelecida considerando os seguintes princípios (Tabelas 2.6.21 e 2.6.22).

- Para cada indicador, serão definidas três faixas: Faixa 1, Faixa 2 e Faixa 3.
- Para cada um deles serão determinados pontos de penalização, em percentual, da seguinte forma:
    - a penalização correspondente à Faixa 1 será de 5% sobre o valor da

fatura mensal;

- a penalização correspondente à Faixa 2 será 10% sobre o valor da fatura mensal;
- a penalização correspondente à Faixa 3 será 15% sobre o valor da fatura mensal.

Item	**Definição**
X	Valor do ANS calculado pela fórmula de cada indicador
L_{min}	Limite mínimo do ANS a ser cumprido em percentual
Faixa 1	Primeira faixa de cumprimento do ANS
Faixa 1	Segunda faixa de cumprimento do ANS
Faixa 3	Terceira faixa de cumprimento do ANS

Tabela 2.6.21 – Definições

L_{min}	**Faixa 1**	**Faixa 2**	**Faixa 3**
100	100% > x ≥ 99,5%	99,5% > x ≥ 99,00%	99,00% > x
99,9	99,90% > x ≥ 99,40%	99,40% > x ≥ 98,90%	98,90% > x
99,8	99,80% > x ≥ 99,30%	99,30% > x ≥ 98,80%	98,80% > x
99,7	99,70% > x ≥ 99,20%	99,20% > x ≥ 98,70%	98,70% > x
99,6	99,60% > x ≥ 99,10%	99,10% > x ≥ 98,60%	98,60% > x
99,5	99,5% > x ≥ 99,25%	99,25% > x ≥ 99,00%	99,00% > x
99,0	99,00% > x ≥ 98,50%	98,50% > x ≥ 98,00%	98,00% > x
98,0	98,00% > x ≥ 97,00%	97,00% > x ≥ 96,00%	96,00% > x
97,0	97,00% > x ≥ 96,00%	96,00% > x ≥ 94,00%	94,00% > x
96,0	96,00% > x ≥ 94,00%	94,00% > x ≥ 92,00%	92,00% > x
95,0	95,00% > x ≥ 92,50%	92,50% > x ≥ 90,00%	90,00% > x
92,0	92,00% > x ≥ 88,00%	88,00% > x ≥ 84,00%	84,00% > x
90,0	90,00% > x ≥ 85,00%	85,00% > x ≥ 80,00%	80,00% > x
80,0	80,00% > x ≥ 70,00%	70,00% > x ≥ 60,00%	60,00% > x

Tabela 2.6.22 - Tabela de faixas de ANS e penalidades

2.6.1.9 Índice de Qualidade do Serviço

Uma sanção ou penalidade pode ser calculada também, por meio do IQS - Índice de Qualidade de Serviço e para o(s) evento(s) de falha nas categorias Energia Elétrica e Climatização.

O IQS pode ser apurado mensalmente e representa o valor obtido pela seguinte fórmula:

$$IQS = \sum NOTAS \div \sum PESOS$$

A Nota para cada indicador/métrica representa o produto entre Peso (conforme tabela 2.6.23 abaixo) e o Escore (valor atribuído conforme tabelas 2.6.24 a 2.6.28 abaixo). Os critérios de atribuição de nota estão na Tabela 2.6.29.

O Peso é um valor fixo que varia entre 1 a 10.

O Escore varia entre 1 e 3 e dependerá dos limites utilizados.

Atribuição de Pesos		
Categoria	**Métrica**	**Peso**
Energia Elétrica	Percentual de Disponibilidade	10
Climatização	Temperatura em °C	10
	Percentual de Umidade	7
Processos	Sistema CFTV	7
	Catracas Eletrônicas	5
	Incidentes e Problemas	5
	Mudanças	5
	Conservação	3

Tabela 2.6.23 - Atribuição de Pesos

Energia Elétrica	
Valor	**Escore**

100%	3
< 100%	1

Tabela 2.6.24 - Escore Energia Elétrica

Climatização			
Temperatura		**Umidade**	
Valor	**Escore**	**Valor**	**Escore**
> 20,8 °C < 23,3 °C	3	> 45% < 55%	3
< 20,8 °C ou > 23,3 °C	1	< 45% ou > 55%	1

Tabela 2.6.25 - Escore Climatização

Segurança			
Sistema CFTV		**Catracas Eletrônicas**	
Valor	**Escore**	**Valor**	**Escore**
100%	3	100%	3
< 100%	1	< 100%	1

Tabela 2.6.26 - Escore Segurança

Gestão			
Incidentes e Problemas		**Mudanças**	
Valor	**Escore**	**Valor**	**Escore**
100% Resolvidos	3	2	3
< 100% Resolvidos	1	> 2	1

Tabela 2.6.27 - Escore Gestão

Administração	
Conservação	
Valor	**Escore**
Bom	3
Regular	2

Ruim	1

Tabela 2.6.28 - Escore Administração

Índice de Qualidade do Serviço								
Critério de Atribuição de Nota								
Categoria	**Métrica**	**Peso**	**Escore**	**Nota Max.**	**Escore**	**Nota**	**Escore**	**Nota Mín.**
Energia Elétrica	Disponibilidade	10	3	30			1	10
Climatização	Temperatura	10	3	30			1	10
	Umidade	7	3	21			1	7
Processos		7	3	21			1	7
		5	3	15			1	5
		5	3	15			1	5
		5	3	15			1	5
		3	3	9	2	6	1	3
IQS Máximo		**3**						
IQS Mínimo		**1**						

Tabela 2.6.29 - Critério de Atribuição de Nota

A sanção por IQS terá percentual diferenciado, conforme a categoria, que determinará o valor a ser deduzido da fatura mensal. A Tabela 2.6.30 apresenta o valor de IQS e o percentual que determinará a cobrança.

A sanção por evento será cobrada apenas para categorias Energia Elétrica e Climatização. Possui um valor fixo cobrado a partir da primeira ocorrência para falhas de energia elétrica (fórmula do S1 abaixo) e um valor calculado em função do tempo de parada dos equipamentos por motivo de energia elétrica e/ou climatização (fórmula do S2 abaixo).

A sanção será medida pelas seguintes fórmulas:

S1 = 15% do Valor da Fatura Mensal

Onde, **S1** é a sanção calculada por evento de indisponibilidade de equipamento causada por falha de energia elétrica.

S2 = Tt x 0,40% do Valor da Fatura Mensal *

* (Limitado a 30% do valor total da Fatura)

Onde, **S2** é a sanção calculada por evento de indisponibilidade de equipamento causada por falha de energia elétrica e/ou climatização. E **Tt** é o tempo total de indisponibilidade em minutos do(s) equipamento(s) medida pelo incidente.

Categoria	**Indicadores**	**Métrica**	**Sanção por IQS**		**Sanção por Evento**	
			IQS	**Valor**	**Valor Fixo para Energia Elétrica**	**Valor**
Energia Elétrica	Disponibilidade	Percentual	<3	1,00%	S1	S2
Climatização	Disponibilidade	Temperatura	<3	0,50%		
		Umidade	<3	0,50%		
Processos	Segurança	CFTV	<3	0,25%		
		Catracas	<3	0,15%		
	Gestão	Incidentes	<3	0,10%		
		Mudanças	<3	0,10%		
	Administração	Conservação	<2,94	0,05%		

Tabela 2.6.30 - Critério de Sanção

2.7 Cenário de *Colocation* e *Cloud Computing*

De acordo com Kaufman [01], o conceito de computação em nuvem vem evoluindo

há mais de 40 anos. Na década de 1960, J.C.R. Licklider introduziu o termo "*intergalactic computer network*" na Agência de Projetos de Pesquisa Avançada. Este conceito serviu para introduzir o termo que o mundo hoje conhece como internet. A premissa subjacente era a interconexão global de programas de computador e dados.

O nome “computação em nuvem” foi inspirado no símbolo da nuvem que, muitas vezes, é usado para representar a internet em fluxogramas e diagramas. A migração para a nuvem vem ocorrendo nos últimos anos com os usuários finais.

A computação em nuvens vem crescendo cada vez mais com o passar dos anos. Segundo Machado [02], estima-se que até 2015 o crescimento seja de 74%. Esse índice pode se concretizar devido a compreensão por parte de empresários quanto a questão de segurança que envolve a tecnologia, segundo estudos da consultoria Frost & Sullivan [03].

Segundo Barros [04], argumentos econômicos também somam para que a computação em nuvem ganhe ampla aceitação. Provedores de computação em nuvem podem construir grandes *datacenters* a baixo custo, devido a grande experiência desses provedores na organização e provisionamento de recursos computacionais, as economias de escala podem aumentar a receita para os provedores de nuvem e ao mesmo tempo conseguir custos mais baixos para os usuários de nuvem.

Ainda segundo Barros [04], o modelo resultante de computação sob demanda permite aos provedores conseguirem uma melhor utilização dos recursos computacionais compartilhando infraestrutura de *datacenter*, recursos, ferramentas e processos de gerenciamento.

Esse mesmo modelo de consumo da computação permite aos pequenos usuários da nuvem evitar os custos de excesso no provisionamento de recursos, podendo aumentar ou reduzir dinamicamente sua infraestrutura ou aplicações conforme a necessidade.

Em uma definição simplificada, a computação em nuvem seria um conjunto de recursos como capacidade de processamento, armazenamento, conectividade, plataformas, aplicações, *hardwares* e serviços disponibilizados na internet, ou ainda, podemos pensar que seja como um *datacenter* disponível, completo, confiável e pronto para ser usado como um serviço, acessíveis por demanda e pago mensalmente (na maioria dos casos).

O *colocation*, neste contexto, seria um *datacenter* disponível, completo e confiável a espera dos equipamentos para funcionar.

Podemos listar a escalabilidade como caracteristica peculiar e comum aos dois serviços e o maior risco de comprometimento da privacidade de armazenamento como um ponto de desvantagem da computação em nuvem.

Pequenas empresas e aquelas iniciantes podem preferir um modelo de computação em nuvem para uso, pois não exige muito conhecimento em TI para se começar a operar.

As empresas maiores e aquelas com departamentos de TI costumam escolher pelo serviço de *colocation* para abrigar seus equipamentos, pois valorizam a flexibilidade para o crescimento e mudança. Os custos de se ter um *datacenter* são enormes e construir o seu próprio não faz mais sentido para muitas empresas que precisam de altos níveis de confiabilidade.

2.8 Vantagens de se contratar um *Datacenter* X Construir um *Datacenter* X Hospedagem na nuvem

Conforme as empresas crescem, suas necessidades de TI geralmente crescem com elas, e, consequentemente, isso acaba forçando a busca por maior capacidade, disponibilidade e segurança nos *datacenters*. Neste ponto, grandes dúvidas surgem: Onde hospedar minha solução tecnológica? Em um novo *datacenter*? Contratar um serviço de hospedagem? *Cloud Computing*?

Ainda que indicadores financeiros sejam muito importantes, outros fatores precisam ser levados em conta como, prazo de implantação, manutenção, segurança, nível de especialização, infraestrutura, disponibilidade, e outros fatores estratégicos.

Todos fatores desempenham um importante papel nas decisões, por isso este relatório tenta abordar os principais pontos.

Pequenas e até médias empresas, sem necessidades complexas em TI ou grandes soluções e processos, podem preferir a utilização dos serviços como hospedagem na nuvem, pois são geralmente de baixo custo, com configuração pré-estabelecida e na grande maioria dos casos, não exige a necessidade de um conhecimento aprofundado para funcionamento.

Pode-se até achar que manter dados na nuvem exige apenas um baixo custo, mas não é a opção mais barata para todas as soluções. A Forbes publicou um artigo [08] com muitos dados sobre o mercado de disco rígido na nuvem em 2012, escrito por Gene Marks, que aconselha os clientes em suas compras de TI. Ele ajudou 30 empresas de pequeno

porte a avaliar as soluções de computação em nuvem e todos recusaram com base apenas em custo.

Ao falarmos sobre grandes empresas, a escolha pelos serviços da nuvem pode e deve gerar perguntas como as seguintes.

- Como os dados são protegidos? (aplicação, arquitetura, física, pessoal)
- Os dados são criptografados em todos os pontos de transferência?
- Sob quais conformidades, padrões, auditorias de segurança ou certificados a *colocation center* é avaliada?
- Como o prestador de serviços detecta o comprometimento ou violação? Como o cliente é alertado?

De acordo com Vijay Gill, *Senior Manager of Production Network Engineering and Architecture* na Google, em sua comparação de 2010 [10], *colocation* é mais barato do que usar um serviço de nuvem se a empresa executar seus processos em servidores altamente utilizados. Os dados foram comparados utilizando os preços da *Amazon Web Services* como referência.

Em sua pesquisa, Gill criou uma planilha que define a análise, a qual mostra que para um mesmo trabalho/processo, custaria U$ 118.248 dólares na Amazon e U$ 70,079 dólares em uma instalação de *colocation*. Embora possamos considerar que os preços tenham caído um pouco, esta pesquisa ainda é válida.

Mas para médias e grandes empresas com projetos mais complexos ou mais críticos, a escolha tem sido o *colocation* por conta da flexibilidade, confiabilidade, facilidade de mudança, acordos de níveis de serviço e por um motivo muito importante: não precisar construir seu próprio *datacenter*.

A construção de um *datacenter* próprio ou a hospedagem de servidores dentro da própria empresa com infraestrutura equivalente a de um *datacenter*, demanda altos investimentos e está sendo cada vez mais deixado de lado, pois além dos altos custos, cria-se uma série de obrigações de manutenção de uma estrutura complexa, com requisitos de conformidade e certificações necessárias, que são caros e de difícil manutenção.

A parte **contratante** do serviço de hospedagem tem pouco ou nenhum trabalho extra para se manter em conformidade com padrões e normas nacionais e internacionais. Por isso é observável que a hospedagem permite reduzir o custo geral de TI, pois é uma

alternativa para construir o seu próprio *datacenter* de uma forma mais econômica.

Muitas vezes, a opção mais barata não é a melhor escolha. É preciso considerar cuidadosamente as opções de fornecedores, suas experiências, tempo de mercado, relacionamento, aderência as normas e padrões etc.

Naturalmente, o preço deve ser apenas um dos fatores ao avaliar fornecedores do serviço. Outros fatores podem ser mais difíceis de quantificar, mas são tão importantes, quiçá mais, do que considerações de preços.

Considerando, ainda, que as empresas responsáveis pelos *datacenters* possuem profissionais altamente capacitados para o suporte e manutenção necessários no dia-a-dia e em tempo integral, a organização **contratante** poderá focar seus esforços no crescimento e manutenção da sua solução tecnológica ou de seu produto hospedado.

Em relação a segurança e proteção dos dados, assim como o caso de proteção contra falhas, ao contratar o serviço de *datacenter*, a organização está compartilhando os custos de medidas de segurança para o *datacenter* com outros clientes, ou seja, têm-se medidas de segurança robustas, certificadas e com custo compartilhado.

Com as violações de dados aumentando consideravelmente a cada ano, regulamentações e certificações estão se tornando cada vez mais rigorosas e as penalidades e prejuízos para as empresas afetadas vão muito além do financeiro.

Levando em consideração este ponto de vista, os *datacenters* comerciais estão focando cada vez mais em segurança física, controle de acessos, sistemas contra incêndios e desastres naturais.

No que tange o suporte, as grandes empresas fornecedoras do serviço de hospedagem em *datacenters* terão equipes de especialistas em diversas tecnologias disponíveis para monitorar toda infraestrutura do *datacenter* e até mesmo, sala-cofres e equipamentos da empresa **contratante** dos seus serviços. Serão assim, capazes de responder a quaisquer problemas que possam surgir, e o melhor, com prioridade.

Isso implica no custo total da solução, já que alguns especialistas não vão precisar estar na folha de pagamento da empresa **contratante** e na tranquilidade de não precisar gerenciar aspectos rotineiros de um *datacenter*, focando apenas na solução tecnológica.

3 Recomendações de Segurança da Informação para Desenvolvimento de *Software*

O desenvolvimento de *softwares* responsáveis por suportar os processos de negócios tem crescido exponencialmente ao longo dos anos e esse fator fez crescer consideravelmente a busca por melhores práticas e padrões que gerem além de qualidade, agilidade, eficiência, eficácia e segurança. A preocupação no desenvolvimento de *softwares* seguros já se tornou parte dos processos de negócio, visando garantir a proteção dos ativos e das informações das empresas.

Neste sentido, a segurança da informação passa a ter um conceito mais amplo, não apenas relacionada com a esfera da tecnologia e das ferramentas necessárias para proteger a informação, mas também como um dos pilares de suporte à estratégia de negócio para o tomador de decisão de uma corporação [40] [50].

Os requisitos de segurança da informação são tão importantes no desenvolvimento dos projetos quanto os requisitos de sistema. Uma avaliação dos riscos de segurança da informação pode ser insumo para criação dos requisitos de segurança. Gastos com os controles de segurança precisam ser balanceados de acordo com os danos causados aos negócios gerados pelas falhas potenciais na segurança da informação. Os resultados da avaliação de riscos ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos da segurança da informação [41] [50].

A segurança de *software* é um campo relativamente novo, os primeiros livros e disciplinas acadêmicas surgiram no ano de 2001, a partir da necessidade de desenvolvedores, arquitetos e cientistas da computação de lidar com a construção de *software* mais seguro [42].

De forma prática, o *software* resistente a invasão é o que reduz a probabilidade de um ataque bem-sucedido e mitiga a extensão do dano se o ataque ocorrer. Para que o *software* seja seguro e resistente a invasão, ele deve levar em conta conceitos de segurança de *software* [43]. Outra visão é: o *software* seguro é aquele que não pode ser intencionalmente subvertido ou forçado a falhar. Ou seja, ele se mantém correto e previsível mesmo após o esforço intencional e comprometer seu funcionamento [44].

O *software* seguro é desenhado, implementado, configurado e suportado de forma que é possível estabelecer que ele continue operando corretamente na presença dos prin-

cipais ataques, resistindo à exploração de falhas ou outras fraquezas no *software* pelo atacante, ou ainda tolerando os erros e falhas que podem resultar desta exploração, bem como isole, contenha e limite o dano resultante de falhas causadas por qualquer defeito acionado por ataques que o *software* não consiga resistir ou tolerar e se recupere o mais rápido possível destas falhas [44].

As seguintes propriedades caracterizam a segurança do *software* [44].

- Falhas exploráveis e outras fraquezas são evitadas por desenvolvedores bem-intencionados.
- A probabilidade de que desenvolvedores mal-intencionados implantem falhas exploráveis ou lógicas maliciosas no *software* é baixa ou nula.
- O *software* será resistente, tolerante ou resiliente a ataques. Para desenvolver *software* seguro, é importante incorporar conceitos de segurança nas fases de requisito, projeto, codificação, liberação e descarte do ciclo de vida do *software*.
- Incorporar conceitos de segurança é uma necessidade básica que precisa ser abordada e que não pode ser ignorada na construção das aplicações [42].

Os investimentos em segurança de *software* giram em torno de US$400.000 anuais, em média, e o custo para remediar as vulnerabilidades não encontradas antes da implantação, que são 20% do total de vulnerabilidades encontradas, é de US$ 300.000, [45] [47]. Apesar do investimento sobrepor o custo, é notório que somente 1 de cada 5 vulnerabilidades é capaz de colocar toda a iniciativa de segurança em risco, e por isso se faz necessário que seja incluído um processo de construção de *software* seguro na cultural organizacional [47].

Construir um *software* seguro é responsabilidade de todos os intervenientes envolvidos com o ciclo de desenvolvimento de *software*. Enquanto a segurança do *software* pode ser atribuída às tecnologias escolhidas ou aos processos seguidos, uma eventual responsabilidade é atribuída para os desenvolvedores. Tecnologias são intrinsecamente seguras e limitadas, a probabilidade de que elas sejam implementadas de forma segura é isolada. Muitas vezes, os processos que servem para auxiliar na segurança do *software* podem ser contornados, por exemplo, vítimas do cronograma e orçamento.

A obtenção de *software* seguro é uma atividade altamente complexa que envolve

vários fatores a serem considerados e práticas a serem executadas [46]. Essa diversidade se apresenta como um fator de impedimento para as organizações interessadas no assunto, fato que induziu ao desenvolvimento de alguns processos como, por exemplo o *Software Development Lifecycle* (SDL) da Microsoft [60]; além de modelos para profissionalizar um programa de segurança como, por exemplo, OpenSAMM (SAMM da *Open Web Application Security Project* (OWASP) e o BSIMM da Cigital [47].

Qualquer uma das partes interessadas no *software* é responsável pela construção com o objetivo de garantir que o *software* construído não é suscetível a falhas de segurança. Nenhum *software* é 100% seguro. No entanto*, softwares* podem ser projetados, desenvolvidos e implantados tendo o assunto segurança sempre em mente, desenvolvendo controles de segurança necessários para minimizar a probabilidade de exposição e do impacto, se explorado [56].

O (ISC)² - *International Information Systems Security Certification Consortium*, instituto de referência mundial em Segurança da Informação, lista as dez melhores práticas para construção de um *software* seguro [56], a saber.

1. Proteger a marca e a confiança dos seus clientes.
2. Conhecer o negócio e dar suporte de TI com soluções seguras.
3. Compreender a tecnologia do *software*.
4. Certificar-se de *compliance* para governança, regulamentos e privacidade.
5. Conhecer os princípios básicos da segurança de *software*.
6. Assegurar a proteção de informações sensíveis.
7. Projetar o *software* com recursos de segurança.
8. Desenvolver o *software* com recursos seguros.
9. Implantar o *software* com recursos de segurança.
10. Educar-se e educar aos outros sobre como construir *softwares* seguros.

3.1 Safety Software

A disciplina de *safety software* está preocupada em garantir a confiança dos sistemas computacionais a partir de um julgamento quantitativo das suas propriedades. Este conceito está ligado a dependabilidade, que é a propriedade que define a capacidade dos sistemas computacionais de prestar um serviço que se pode justificadamente confiar [48]

[49].

A noção de dependabilidade pode ser quebrada em seis propriedades fundamentais, relacionada aos sistemas computacionais, a seguir [48] [49].

- Confiança: manterá o funcionamento correto quando estiver em uso.
- Disponibilidade: estará operacional quando necessário.
- *Safety*: sua operação não trará perigo ao usuário ou operador.
- Confidencialidade: não haverá revelação não autorizada da informação.
- Integridade: não haverá modificação não autorizada da informação.
- Manutenibilidade: facilidade de modificação do *software* com objetivo de corrigir defeitos, se adequar a novos requisitos ou se ajustar a um ambiente novo.

É importante observar os requisitos de segurança não estão explicitamente incluídos nesta lista, porém eles estão cobertos pelas propriedades disponibilidade, confidencialidade e integridade [48] [49].

3.2 Contexto Atual

A falta de segurança em projetos de *software* é uma das principais preocupações das organizações. É por meio das vulnerabilidades presentes em projetos de *software* que ocorre a quebra de sigilo e roubo de informações. Devido a esse fator, as organizações estão buscando adotar medidas cada vez mais rigorosas de proteção alinhadas a normas e metodologias de segurança [51] [52].

As ameaças à segurança das informações dos negócios, de propriedade intelectual e a privacidade das informações pessoais estão aumentando. Assim, a necessidade de conter tais ameaças, presentes a cada dia, faz com que o gerenciamento da segurança de informações ganhe mais importância nas empresas. De acordo com um estudo realizado por McAfee [51] [53], o roubo de dados e violações de crimes cibernéticos pode ter custado para as empresas, em 2008 mais que U$ 1 trilhão em razão da perda de propriedade intelectual e dos gastos com a reparação dos prejuízos. Esses dados são assustadores e se pudessem ser previstos certamente poderiam ter sido evitados através da implementação de alguns modelos de segurança como: ISO 27001, ISO 27002, SSE-CMM, entre outros. [51] [54].

O CERT do *Software Engineering Institute* (SEI) é um centro de peritos em Segurança na Internet. Suas estatísticas mostram que o número de vulnerabilidades nas aplicações relatadas aumentou de 171 em 1995 para 6058 em 2008 [46]. Uma fonte de problemas de segurança é a não consideração de requisitos de segurança no completo desenvolvimento do sistema [51].

Um estudo divulgado pela Symantec [78] revela que o uso de *toolkits* se tornou mais amplo devido a sua acessibilidade e a relativa facilidade de se usar. Isso atraiu criminosos tradicionais que, de outra forma, não teriam os conhecimentos técnicos necessários para o *cyber* crime e tem alimentado uma economia global cada vez mais organizada e rentável.

Os *toolkits* para ataque são programas de *software* que podem ser usados por novatos e também por especialistas para facilitar o lançamento de ataques generalizados a computadores em rede. Estes *kits* permitem que o invasor lance facilmente numerosas ameaças contra sistemas de computador criadas previamente. Também possibilitam personalizar essas ameaças a fim de escapar de ferramentas de detecção, além de automatizar o processo de ataque [78].

A velocidade com que novas vulnerabilidades e maneiras de explorá-las se espalham pelo mundo aumentou devido às inovações que os desenvolvedores de *kits* para ataque integraram aos seus produtos. Esses *kits* são agora muito fáceis de atualizar, o que permite adicionar rapidamente código para explorar as novas vulnerabilidades.

Com o intuito de diminuir a incidência de ataques e exploração de vulnerabilidades, é necessário que a organização almeje a busca por conformidade, isto é, esteja apoiada em um modelo de processo organizacional eficiente. Este modelo pode incluir normas, padrões e outros aspectos legais, bem como um modelo de qualidade, não para um produto específico, mas para qualificação da empresa como um todo.

A busca da qualidade no desenvolvimento de *software* é um processo sistemático que deve focalizar todas as etapas e artefatos produzidos com o objetivo de garantir a conformidade de processos e produtos, prevenindo e eliminando defeitos. No desenvolvimento de *software*, a qualidade do produto está diretamente relacionada à qualidade do processo de desenvolvimento. Desta forma, é comum que a busca por um *software* de maior qualidade passe necessariamente por uma melhoria no processo de desenvolvimento.

3.3 Vulnerabilidades

A melhor maneira de desenvolver *software* seguro é incorporar a segurança desde o início do desenvolvimento de *software*. Além disso, o desenvolvedor deve conhecer as vulnerabilidades em diferentes artefatos do ciclo de vida do desenvolvimento do *software* para que estes possam ser removidos assim que possível. Caso contrário, a remoção as vulnerabilidades, numa fase posterior irá aumentar o custo significativamente [55].

Vulnerabilidades em *software* nos afetam quase diariamente, nos forçaram a mudar a forma como usamos os computadores e a internet, além de ser o centro de algumas das mais espetaculares e caras falhas. Por exemplo, o custo total do vírus "*Code Red*" foi estimado em 2,6 bilhões de dólares, e o vírus "Nachi" afetou operações da companhia aérea do Canadá e da CSX ferrovias. Os dois exploraram "*buffer overflows*", uma classe de vulnerabilidades que é conhecida desde 1988. Esforços estão começando a reduzir as vulnerabilidades em *software*, mas a indústria certamente ainda tem um longo caminho a percorrer [51].

As vulnerabilidades podem ser causadas por erros originados em diversas fases do desenvolvimento da aplicação. *Bugs* são a consequência de fatores humanos na tarefa de programar e produzem resultado incorreto ou inesperado. São classificados de acordo com o estágio em que o *bug* ou falha foi detectado, dentre eles: *Bugs* de Projeto, definidos como falhas que surgem ainda na etapa de concepção do *software*, como a escassez de requisitos exigidos; *Bugs* de Implementação, caracterizados por uma interpretação equivocada dos requisitos funcionais que resulta em falhas, principalmente na fase de código, como estouro da pilha; e *Bugs* de Configuração, causados por má configuração e ajuste dos parâmetros do *software*.

Outra questão importante, considerando *bugs* de segurança, é o foco em problemas de alto risco. É sobre isto que a lista OWASP Top 10 trata, ela identifica os *bugs* de segurança mais críticos e comuns para aplicações *Web* [79]. Esta lista ajuda a entender onde estão as vulnerabilidades e onde focar as revisões e testes. Auxilia também na percepção de mudança do cenário de ameaças que serve de base para a construção de *softwares* mais seguros.

Os riscos detectados em 2013 foram os seguintes [79].

1. Injeção de código.
2. Quebra de autenticação e Gerenciamento de Sessão.
3. *Cross-Site Scripting* (XSS).

4. Referência Insegura e Direta a Objetos.
5. Configuração Incorreta de Segurança.
6. Exposição de Dados Sensíveis.
7. Falta de Função para Controle do Nível de Acesso.
8. *Cross-Site Request Forgery* (CSRF).
9. Utilização de Componentes Vulneráveis Conhecidos.
10. Redirecionamento e Encaminhamento Inválidos.

3.4 Ciclo de vida de Desenvolvimento de *Software*

Um modelo de ciclo de vida organiza as atividades de desenvolvimento de *software* e provê um *framework* para monitorar e controlar o seu projeto de construção e operação. Sem a adoção de um modelo, é difícil endereçar em que momento o desenvolvimento e a validação do projeto se encontram e até mesmo como e em que situações os pontos de controle devem ser aplicados [48] [57] [58].

Com a adoção de padrões de construção de *software* seguro dentro do seu ciclo de vida é possível, a partir de atividades, garantir identificação, avaliação, tratamento, aplicação e validação de controles de segurança da informação. Assim, espera-se o aumento da qualidade e diminuição máxima das possibilidades de ataque dentro das aplicações. O levantamento e o desenvolvimento de *checklists* com os controles a serem aplicados podem auxiliar a incorporação de práticas de codificação defensiva ao longo da construção das aplicações.

O tratamento dos aspectos relacionados à segurança do *software* não necessariamente representa aumento do custo no seu ciclo de vida de desenvolvimento, tendo em vista que corrigir problemas e falhas desta natureza custam mais depois da aplicação pronta e em produção [58].

3.4.1 *Software Development Life Cycle* (SDLC)

O Ciclo de Vida do Desenvolvimento de Sistemas (SDLC – *Systems Development Life Cycle*), conhecido também com o “ciclo de vida do *software*” refere-se aos estágios de concepção, projeto, criação e implementação de um sistema. Um desdobramento possível

para SDLC é mostrado na Figura 4.1 a seguir [59]:

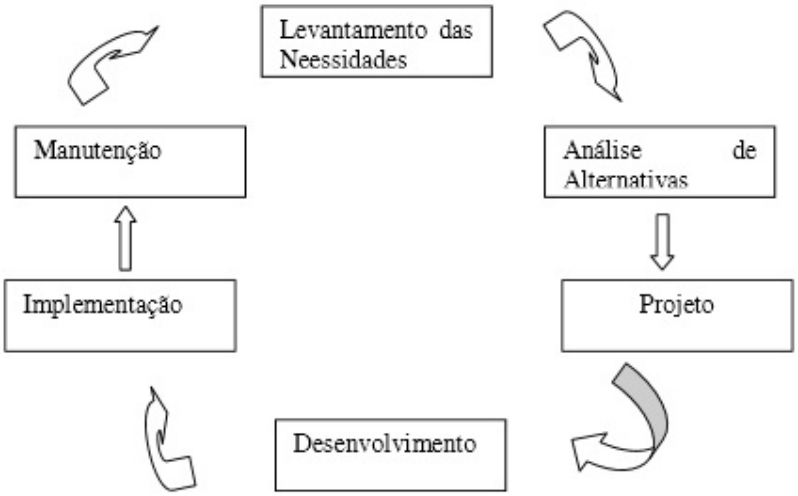

Figura 4.1 SDLC – *Systems Development Life Cycle* [59]

O levantamento das necessidades, também chamado de análise de requisitos, identifica as necessidades de informações da organização. A análise de alternativas consiste na identificação e avaliação de sistemas alternativos. O Projeto trata da construção das especificações detalhadas para o projeto selecionado. Essas especificações incluem o projeto das interfaces, banco de dados, características físicas do sistema, tais como número, tipos e localizações das estações de trabalho, *hardware* de processamento, o cabeamento e os dispositivos de rede. Deve especificar os procedimentos para testar o sistema completo antes da instalação [59].

A etapa do desenvolvimento inclui o desenvolvimento ou aquisição do *software*, a provável aquisição do *hardware* e o teste do novo sistema. A Implementação ocorre após o sistema ter passado satisfatoriamente por testes de aceitação. O sistema é transferido do ambiente de desenvolvimento para o ambiente de produção. O sistema antigo (se existir) deve migrar para o novo. A Manutenção refere-se a todas as atividades relacionadas a um sistema depois que ele é implementado. Deve incluir atividades, tais como, a correção de *software* que não funcione corretamente, a adição de novos recursos aos sistemas em resposta às novas demandas dos usuários [59].

Não há modelo de SDLC uniformemente aceito. Alguns modelos combinam desenvolvimento e implementação em uma única etapa. Outros combinam o levantamento e a

análise das necessidades também em uma única etapa. Alguns modelos dividem o projeto em projeto lógico e projeto físico [59].

O SDLC pode parecer sugerir que os novos sistemas sempre progridem de modo regular e sequencial de um estágio para o seguinte. Na prática, os sistemas nem sempre seguem esta progressão. Os administradores e os profissionais de informática podem mover-se através do SDLC usando o modelo em cascata, a abordagem em espiral, a prototipagem ou a programação ágil [59].

O modelo em cascata segue o SDLC em sequência. Como a água que flui numa cascata, o desenvolvimento movimenta-se somente num sentido, de modo que as etapas não podem ser repetidas. A abordagem em espiral implementa os sistemas, baseada no conceito de maior necessidade. Ela entrega o sistema em versões. Cada versão passa por todas as etapas do SDLC, exceto a implementação que pode ser adotada por algumas versões, e a manutenção que se aplica somente a última versão. A prototipagem descreve uma abordagem que tenta satisfazer as necessidades do usuário focalizando a interface do usuário. Os estágios do projeto e de desenvolvimento, no que concerne à interface de usuários, repetem-se até que o usuário esteja satisfeito [59].

Programação ágil é um nome dados às diversas metodologias que se concentram na reação rápida às mudanças nos requisitos do usuário e que visam a pequenos grupos de desenvolvimento e projetos que requeiram um mínimo de documentação. Um exemplo de programação ágil que recentemente tornou-se popular é a programação extrema (*XP – Extreme Programming*), uma metodologia que junta dois programadores com um dos clientes para o qual o *software* está sendo desenvolvido. Apesar de contradizer antigas crenças sobre o desenvolvimento de *software,* a experiência mostra que a XP pode reduzir o tempo de desenvolvimento e os defeitos de *software*, ao mesmo tempo que aumenta a satisfação entre desenvolvedores e usuários [59].

A melhor abordagem para um determinado projeto depende, em grande parte, da natureza do projeto e da natureza da organização.

3.4.2 *Security Development Lifecycle* – SDL na Microsoft

Os objetivos do SDL (*Security Development Lifecycle* - Ciclo de vida do desenvolvimento da segurança), adotado pela Microsoft, são dois: reduzir o número de defeitos de

codificação e de *design* relacionados à segurança e reduzir a gravidade de todos os demais defeitos. Isso segue o lema frequentemente citado: "Seguro por *design*, seguro por padrão, seguro em implantação e comunicação" (também conhecido em inglês como SD3+C) [60].

O SDL se concentra principalmente nos dois primeiros elementos desse lema. Seguro por *design* significa que o *design* e o código serão seguros desde o início e Seguro por padrão é o reconhecimento de que isso jamais ocorrerá. O SDL não reconhece o processo no que se refere ao desenvolvimento do *software*, pois realmente tanto faz usar um modelo em cascata, um modelo em espiral ou um modelo ágil. O SDL envolve a modificação dos processos de uma organização de desenvolvimento de *software* através da integração de medidas que levam a uma segurança de *software* aprimorada. O SDL aprimora a qualidade do *software*, reduzindo os defeitos de segurança [60].

O SDL é muito bem-sucedido na Microsoft e a resposta é muito simples: suporte executivo, treinamento e reconhecimento. Os principais executivos da empresa se comprometeram com o SDL, mas uma força de trabalho de engenharia capacitada é igualmente fundamental. Para liderança, é preciso designar uma ou mais pessoas como os responsáveis pela segurança. Suas tarefas incluem ficar à frente de questões de segurança, promover práticas de segurança na organização de desenvolvimento e ser a voz da razão quando for necessário tomar decisões difíceis em relação à segurança [60].

Se os engenheiros responsáveis não conhecem nada sobre filosofias básicas de segurança, sobre os tipos de defeitos de segurança comuns, sobre o *design* seguro básico ou sobre os testes de segurança, não há realmente chance de produzirem um *software* seguro. Em média, os engenheiros de *software* não prestam muita atenção à segurança. Eles podem saber muito sobre recursos de segurança, mas precisam ter um melhor conhecimento sobre o que é necessário para criar e fornecer recursos seguros.

Segundo Michael Howard (Gerente de programas sênior na Microsoft), o verdadeiro problema é que a maioria das escolas, universidades e cursos técnicos ensina recursos de segurança, e não como criar *softwares* seguros. Isso significa que há muitos engenheiros de *software* sendo formados por essas escolas ano após ano que acreditam que sabem criar *softwares* seguros apenas porque sabem como um *firewall* funciona. Resumindo, você só pode contar que a pessoa **contratada** saberá criar defesas de segurança para o seu *software* se perguntar a ela especificamente qual sua experiência e seu conhecimento do assunto.

Ainda segundo Howard, um esforço de segurança é o foco de toda a equipe em atualizações do modelo de segurança, na revisão do código, nos testes e nas minúcias da documentação. O esforço não é simplesmente uma correção rápida para um processo que não possui disciplina de segurança; ele é, na verdade, uma tentativa centralizada de confirmar a validade das informações da arquitetura de segurança, de descobrir alterações que possam ter ocorrido durante o processo de desenvolvimento e de identificar e corrigir quaisquer vulnerabilidades de segurança ainda existentes que você possa descobrir. Não é possível criar segurança em um *software* apenas com um esforço de segurança.

Não há maneira fácil de determinar quanto tempo é necessário para um esforço de segurança; a duração do esforço no fim é determinada pela quantidade de código que precisa ser revisado quanto à segurança, visto que todos os esforços até hoje foram embarreirados pela quantidade de código. As equipes são altamente incentivadas a tentar conduzir as revisões de código de segurança em todo o processo de desenvolvimento, desde que o código esteja razoavelmente estável, pois a qualidade das revisões de código será comprometida ao se tentar condensar um excesso de revisões de código em um período de tempo muito curto [60].

Ao aproximar-se do final do projeto, uma pergunta muito importante deverá ser respondida: do ponto de vista de segurança, o *software* está pronto para o lançamento? A Revisão Final de Segurança (FSR) responde a essa pergunta. Ela é executada pela equipe de segurança central com ajuda da equipe de produto, mas não apenas pela equipe de produto. O princípio básico é determinar o código principal, usando a heurística tal como exposição à Internet, manipulação de informações sigilosas ou identificáveis pessoalmente, etc. e marcá-lo como código de prioridade um. Esse código deve ser revisto durante o esforço, o qual só pode ser concluído quando o código é revisado [60].

O SDL funciona. O uso das técnicas do Ciclo de vida do desenvolvimento da segurança resulta em *softwares* mais seguros. Na Microsoft, foi constatada a redução dos defeitos de segurança em aproximadamente 50 a 60 por cento quando acompanhamos o SDL. O fato é que todo produto tocado pelo SDL possui menos defeitos de segurança. E isso, certamente, já basta para que ele seja adquirido.

3.4.3 *Secure Software Development Process* (SSDP)

Requisitos de segurança são geralmente mantidos em separado e não são interligados com os requisitos funcionais e design do *software*. Isto leva a inconsistências e ambiguidades, uma vez que é essencial que o *software* seja desenvolvido de forma segura desde o início. Por isso, é preciso ter um Processo repetível e Seguro de Desenvolvimento de *Software* (SSPD), que aborda aspectos da segurança durante cada fase de desenvolvimento do *software* [66].

O SSDP tem como proposta a divisão em quatro fases: Engenharia de Requisitos, *Design*, Implementação e Garantia. Cada uma dessas fases está dividida em atividades que devem ser seguidas, além do relacionamento entre as mesmas. Essa divisão permite uma maior transparência a respeito dos objetivos de segurança e performance, além de facilitar a comunicação com clientes, desenvolvedores e gerentes.

A fase de Engenharia de Requisitos deve receber uma atenção especial, já que pode evitar o custo de correção de erros em fases posteriores de desenvolvimento [66]. É composta pelas atividades de:

- especificação dos requisitos funcionais;
- inspeção nas especificações para identificar erros de *software* sempre necessário;
- modelagem de ameaças com base em informações de ataques e tentativas de ataques;
- análise de risco de ameaças;
- especificação de requisitos de alto nível de segurança, como confidencialidade, integridade e disponibilidade;
- seleção e verificação de mecanismos de segurança capazes de cumprir os requisitos de segurança;
- priorização de requisitos de alto nível de segurança por meio de uma análise custo/benefício;
- inspeções realizadas a fim de identificar erros de segurança em software e requisitos de segurança de baixo nível;
- definição de um limite de segurança aceitável;
- inclusão de requisitos de baixo nível de segurança, caso o limite de segurança calculado seja inferior ao inicial;

- requisitos de segurança, que são priorizados com base em análise de custo/benefício.

A fase de *Design* representa as decisões tomadas para cumprir os requisitos de segurança. O *design* define os aspectos de estrutura estática e comportamento dinâmico do *software*. As atividades dessa fase seguem, basicamente, a mesma configuração da Engenharia de Requisitos com:

- definição detalhada dos requisitos de *design*;
- inspeção regular do projeto para identificação de possíveis erros;
- reforço e correção do modelo de ameaças, repetidas vezes, através da atividade anterior;
- realização de análise de ameaças a fim de obter dados de sua proveniência e prevenir futuras ameaças;
- remoção de ameaças relacionadas a requisitos de segurança;
- decisões de *design* seguro para remoção de ameaças são priorizadas com base numa análise custo/benefício;
- identificação de decisões de *design* seguro e erros de *software* previamente especificadas;
- definição de um nível inicial de segurança;
- se o índice de segurança calculado é inferior ao inicial, então as decisões de *design* seguro para remover os erros devem ser especificadas.

Na fase de Implementação ocorre a interpretação do *design* em código. Pode-se considerar que todos os requisitos de segurança e o *design* especificado serão implementados de maneira correta, através da utilização de linguagem de programação segura e da utilização de padrões, guias e normas de codificação. Por fim, na fase de Garantia, o *software* passa por diversos testes, como inspeção de código e verificação de cumprimento de requisitos, para assegurar que ao final de sua implementação o *software* possua um alto nível de segurança.

A vantagem é que, quando os níveis descritos acima são aplicados de forma conjunta, com sincronismo entre as partes, o produto resultante apresenta conformidade com

as regras de segurança estabelecidas sem a necessidade de *patches* ou correções finais.

3.4.4 Atividades no Ciclo de Vida do *Software*

Com o intuito de melhorar a segurança, uma série de boas práticas de segurança de *software* precisa ser aplicada dentro das fases de ciclo de vida do *software* e não apenas na fase de requisitos, como sugere a Norma IEC 62306:2006. A execução dessas atividades em conjunto com as fases do ciclo de vida é proposta por McGraw [58] e pode ser visualizada na Figura 4.2.

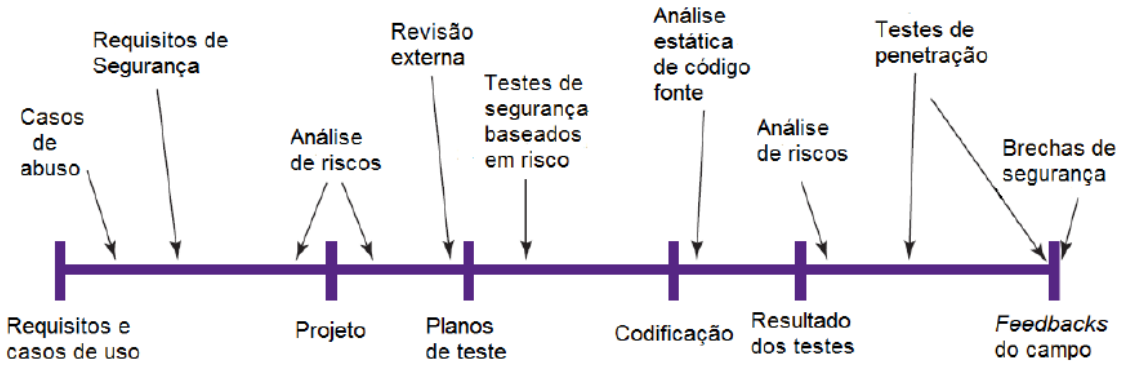

Figura 4.2 Atividades de segurança no ciclo de vida do *software* [58].

A construção de casos de abuso é necessária para relacionar problemas e análises de risco. Deve-se observar neste momento se algum padrão de ataque se encaixa no sistema ou nos requisitos do *software* [48]. Nesta atividade também se concentra o desenvolvimento de cenários que contenham vulnerabilidades a serem exploradas em revisões de código ou testes de penetração.

Os requisitos de segurança abrangem os requisitos funcionais de segurança e casos de abusos baseados em padrões de ataque. Esta atividade requer que todas as camadas de segurança sejam mapeadas afim de garantir a sua correta implementação.

A análise de risco arquitetural auxilia na tomada de decisões bem como no levantamento de riscos, os quais podem estar presentes na arquitetura do *software* a ser desenvolvido. Funciona como uma pequena fase inicial no gerenciamento de riscos, necessário para garantir a aderência à Norma IEC 62304:2006.

Os testes de segurança, em geral, devem cobrir pelo menos dois tópicos principais:

os testes baseados em requisitos de segurança e funcionais; e os testes baseados em riscos.

Após a fase de codificação e antes da fase de testes, a análise de código fonte é uma boa atividade para garantir que os requisitos de segurança foram bem implementados e que as vulnerabilidades listadas na análise de casos de abuso não estão presentes no *software*. A revisão de código pode ser automática e manual, tendo cada estratégia prós e contras [48].

Os chamados testes de penetração são utilizados para testar, de forma dinâmica, um *software* contra vulnerabilidades e falhas de projeto. Este conjunto de técnicas e ferramentas deve garantir que a aplicação não possui nenhum problema potencial ou brecha de segurança que possa ser usado para alterar o comportamento da mesma.

Cabe ressaltar que as atividades de segurança descritas podem ser aplicadas a qualquer tipo de ciclo de vida de *software*, bem como independem do modelo de desenvolvimento de *software* adotado pelos desenvolvedores. Estas atividades não têm nenhuma ligação direta com o modelo de desenvolvimento de *software*, apesar da sua eficácia na melhoria da qualidade das aplicações [48].

3.5 Normas e Modelos de Segurança

Normas e modelos de segurança apresentam práticas fundamentais para que organizações possam estar de acordo com um nível esperado de segurança [12]. Elas contribuem para quantificar um nível aceitável de risco e implementar medidas apropriadas de segurança que garantam a confidencialidade, integridade e disponibilidade das informações.

Nessa seção são descritas normas e modelos que foram considerados no desenvolvimento deste Termo Técnico. Estas foram escolhidas por serem atualmente as principais normas presentes na literatura que tratam de segurança de sistemas.

3.5.1 Norma ISO/IEC 21827 (SSE-CMM)

O modelo SSE-CMM (*System Security Engineering Capability Maturity Model*), atualmente conhecido como a Norma ISO/IEC 21827, fornece um conjunto de boas práticas

de segurança que podem ser adotadas pelas organizações para aumentar a segurança do *software*. O modelo é indicado para o desenvolvimento seguro de *software* e para a elaboração de processos de gestão de segurança. Os padrões de segurança fornecem soluções já consolidadas para problemas recorrentes e servem de referência para as organizações que buscam satisfazer requisitos de segurança. Sendo assim, padrões podem ser associados às práticas do SSE-CMM, identificando como essas podem ser implementadas em um processo de *software*. A incorporação dos padrões ao processo de *software* ocorre no momento da adaptação do processo para atender às necessidades específicas de um projeto [64].

A ISO/IEC 21827 foi desenvolvida pelo ISSEA (*International Systems Security Engineering Association*) em 1999 e descreve as características essenciais que um processo de engenharia da segurança da informação deve possuir para assegurar a boa segurança [61].

A Norma ISO/IEC 21827 não prescreve uma sequência ou um processo particular, mas captura as práticas que são geralmente observadas na indústria. Esta norma é designada para todos os tipos de organizações, sendo usada para a melhoria e avaliação da capacidade de maturidade dos processos de segurança. A estrutura de desenvolvimento da Norma ISO/IEC 21827 é dada por 22 PAs (*Process Areas*), divididas em dois grupos, Práticas Base de Segurança e Práticas Base Organizacionais e do Projeto. A estrutura de distribuição das PAs, em seus grupos correspondentes, pode ser vista na Tabela 5.1 abaixo [61]:

Categorias	**PAs (*Process Areas*)**
Práticas Base de Segurança	PA01 - Administrar controles de segurança PA02 - Avaliar impacto PA03 - Avaliar riscos de segurança PA04 - Avaliar ameaças PA05 - Avaliar vulnerabilidades PA06 - Construir argumentos de segurança PA07 - Coordenar a segurança PA08 - Monitorar a postura da segurança PA09 - Estabelecer a entrada de segurança

	PA10 - Especificar necessidades de segurança PA11 - Verificar e validar a segurança
Práticas Base Organizacionais e do Projeto	PA12 - Assegurar qualidade PA13 - Gerenciar a configuração PA14 - Gerenciar riscos do projeto PA15 - Monitorar e controlar esforço técnico PA16 - Planejar esforço técnico PA17 - Definir processos de engenharia de sistemas da organização PA18 - Melhorar processos de engenharia de sistemas da organização PA19 - Gerenciar evolução da linha do produto PA20 - Gerenciar ambiente de suporte a engenharia de sistemas PA21 - Promover habilidade e conhecimento progressivo PA22 - Coordenar com fornecedores

Tabela 5.1 - Estrutura de distribuição da PAs da Norma ISO/IEC 21827.

A Norma ISO/IEC 21827 também define níveis de maturidade dos processos de segurança da organização que são ampliados após o estabelecimento e cumprimento das práticas da segurança [65]. O processo mais "maduro" define uma organização cujos processos são melhores definidos e conduzidos. São seis níveis de maturidade definidos, onde cada um desses níveis consiste de um número de Práticas Genéricas - GP (*Generic Practices*) que suportam o desempenho das PAs. Os níveis de maturidade atribuídos pela norma ISO/IEC21827 são os seguintes [61].

- Nível 0 - Práticas base não são realizadas.
- Nível 1 - Práticas base são realizadas informalmente.
- Nível 2 - Práticas base são planejadas e monitoradas.
- Nível 3 - Práticas base estão bem definidas.
- Nível 4 - Práticas base são controladas quantitativamente.
- Nível 5 - Práticas base estão em contínua melhoria.

O processo de melhoria e maturidade organizacional da Norma ISO/IEC 21827 é realizado por meio do modelo IDEAL que foi desenvolvido pelo SEI – *Software Engineering*

Institute. Este modelo é usado para definir ações que capacitem as organizações a melhorarem seus processos. O modelo IDEAL serve como um guia para iniciar, planejar e implementar ações de melhoria. A palavra IDEAL é um acrônimo do inglês para Iniciar (*initiating*), Diagnosticar *(diagnosing*), Estabelecer (*establishing*), Agir (*acting*) e Aprender *(learning*). O modelo IDEAL forma uma infraestrutura de cinco fases para guiar organizações no planejamento e na implementação de um efetivo programa de melhoria de processos [61].

3.5.2 Normas ISO/IEC 17799 e ISO/IEC 27001

A Norma ISO/IEC 27001:2006 foi construída baseada na Norma britânica BS7799 e na ISO/IEC 17799 (ABNT NBR ISO/IEC 27001,2006). Seu objetivo é proporcionar um modelo para o estabelecimento, implementação, funcionamento, acompanhamento, revisão, manutenção e melhoria de um sistema documentado dentro do contexto dos riscos de negócio globais da organização [61] [62]. Ela pode ser aplicada em todos os tipos de organizações como por exemplo, empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos, etc. [61]

Esta norma é adotada para o estabelecimento de estratégias de segurança pela organização e pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas (ABNT NBR ISO/IEC 27001, 2006). Um sistema projetado pela norma assegura a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas. Todos os controles de segurança recomendados pela Norma ISO/IEC 27001:2006 são encontrados na Norma ISO/IEC 17799:2005. A Norma ISO/IEC 17799:2005 está contida na ISO/IEC 27001:2006, ou seja, a Norma ISO/IEC 27001:2006 fornece um processo definido de implantação dos controles à ISO/IEC 17799:2005. A Norma ISO/IEC 27001:2006 aplica um sistema de processos dentro de uma organização, junto com a identificação e interações destes processos. Essa abordagem de processos enfatiza a importância dos seguintes aspectos [61].

- Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação.
- 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.
- Monitoração e análise crítica do desempenho e eficácia do sistema.

- Melhoria contínua baseada em medições objetivas.

A Norma ISO/IEC 27001:2006 incorpora o ciclo Plan-Do-Check-Act (PDCA), que é adotado em toda a estrutura dos processos do SGSI. O ciclo PDCA baseia-se no ciclo de melhoria contínua que consiste em planejar (*Plan* – P), fazer (*Do* – D), checar (*Check* – C) e agir (*Act* – A). O ciclo PDCA é uma ferramenta importante para a análise e melhoria dos processos organizacionais contribuindo para a tomada de decisões gerenciais e para o alcance das metas e dos objetivos da organização [61] [63].

Tanto a Norma ISO/IEC 27001:2006 como a Norma ISO/IEC 21827 podem ser adotadas por qualquer tipo de organização, seja ela de pequeno ou grande porte. Isso indica que não há restrições quanto ao uso das normas e a escolha de aderir a uma ou a outra norma de segurança deve ser direcionada ao atendimento dos objetivos de segurança organizacionais [61].

3.5.3 IEC 62304:2006

A Norma IEC 62304:2006 foi baseada na ISO/IEC 12207 e define os requisitos de ciclo de vida de *softwares* para dispositivos médicos. O conjunto de processos, atividades e tarefas descritas nesta norma estabelecem um *framework* comum para processos de ciclo de vida de *software* em dispositivos médicos.

Tem o seu foco em processos de desenvolvimento e manutenção de dispositivos na área médica, porém não especifica a metodologia, artefatos, estrutura organizacional, conteúdo da documentação ou modelos de ciclo de vida [36]. Pode ser aplicada com qualquer um dos modelos existentes, ficando a critério dos desenvolvedores.

Sua filosofia se baseia em três componentes: Engenharia de *Software*, Gerenciamento de Qualidade e Gerenciamento de Risco, sendo o gerenciamento de risco o ponto principal. Após passar pelas fases de desenvolvimento de planejamento e requisitos gerais; análise de requisitos; planejamento arquitetural; detalhamento do *design*; verificação da unidade e testes do sistema; as vulnerabilidades do sistema são detectadas e avaliadas quantos aos riscos gerados. Os riscos são classificados em três níveis de acordo com o grau de severidade, a saber [36].

- Classe A: nenhum ferimento ou danos à saúde é possível.
- Classe B: nenhum ferimento grave é possível.

- Classe C: morte ou ferimento grave é possível.

Esta norma caracteriza-se pelo seu caráter flexível, que admite a sua aplicação e execução em diversas formas de modelos de ciclo de vida, documentação etc.

3.5.4 ISO/IEC 13335

Formalmente denominada de *Guidelines for the Management of IT Security* (GMITS), a Norma ISO/IEC TR 13335:1998 é composta por 5 partes envolvendo a área de TI [68], a saber.

A Parte 1 – *Concepts and Models for IT Security* – publicada em 1996, fornece uma visão geral dos conceitos e modelos fundamentais usados na gestão de segurança de TI.

A Parte 2 – *Managing and Planning IT Security* – publicada em 1997, trata do relacionamento da área de segurança da informação com as demais áreas da organização, principalmente a área de segurança corporativa. De maneira semelhante ao padrão BS7799, a Parte 2 sugere a criação de um comitê interdisciplinar que envolva as diversas áreas da empresa principalmente os responsáveis pelos ativos e pelas informações. Este comitê deve reunir-se periodicamente para definir os níveis aceitáveis de risco, cobrar e acompanhar resultados e reavaliar o projeto de segurança da informação quando necessário. A cláusula 7 da Parte 2 especifica um fluxo de planejamento e gerenciamento do projeto de segurança da informação, além de definir uma série de responsabilidades, com a orientação das atribuições dos atores do processo.

Parte 3 – *Techniques for the Management of IT Security* – publicada em 1998, descreve técnicas de gestão de segurança para a área de TI baseada nas diretrizes das duas primeiras partes. Ela pode ser utilizada em conjunto com a Norma BS7799-2, a qual sugere quais os processos (e não apenas as técnicas, como na ISO 13335-3) devem ser implantados na condução da gestão de segurança [69]. Vale observar ainda que a Parte 3 trata a gestão de risco em praticamente todas as cláusulas, através de técnicas de análise de risco e políticas de segurança corporativa.

A Parte 4 – *Selection of Safeguards* – foi publicada em 2000 e fornece um catálogo de contramedidas e um guia para a seleção destas.

A Parte 5 – *Management Guidance on Network Security* – complementa a parte 4 da

norma, acrescentando fatores relevantes para a conexão de sistemas em redes, tendo sido publicada no ano de 2001.

Os padrões ISO/IEC TR 13.335-3:1998 e ISO/IEC TR 13.335-4:2000 foram revisados e transformaram-se no padrão internacional ISO/IEC 27.005:2008, que foi traduzido para a língua portuguesa e publicado pela ABNT como a norma técnica ABNT NBR ISO/IEC 27.005:2008: Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

3.5.5 ISO/IEC 15.408 - *Common Criteria for Information Technology Security Evaluation*

O *Commom Criteria for Information Technology Security Evaluation* (CC) surgiu como um esforço coletivo de vários países que desenvolveram um padrão para inserção e avaliação de segurança em tecnologia da informação.

A Norma ISO/IEC 15.408, que por questões históricas ficou mais conhecida como CC, propõe um conjunto de exigências e um processo de avaliação para produtos e serviços em seus aspectos de confiabilidade, integridade e disponibilidade. Esta Norma é referência para o desenvolvimento e comercialização de produtos ou serviços e garantias de cumprimento dos requisitos de segurança, necessários para o ambiente do usuário [67].

Os trabalhos foram iniciados com a elaboração do "*Orange Book*" (TSEC – *Trusted Computer Security Evaluation Criteria*) nos Estados Unidos, seguidos pela publicação do ITSEC (*Information Technology Security Evaluation Criteria*) pela Comissão Europeia. Foi sucedido, no Canadá, pelo CTPEC (*Canadian Trusted Computer Product Evaluation Criteria*) e pela publicação americana FC (*Federal Criteria for Information Technology Security*) [67]. Todas essas publicações serviram de base para o Projeto CC, que gerou um documento único contendo critérios de segurança para que fossem adotados por todos.

O produto ou sistema que está sujeito a avaliação é chamado de TOE (*Target of Evaluation* – Alvo de Avaliação). A avaliação feita deve verificar as características de segurança do alvo e é feita com base nos seguintes documentos:

PP (*Protection Profile* – Perfil de Proteção) é o documento criado a fim de identificar os requisitos de segurança para uma classe de segurança relevante com uma finalidade específica para o usuário.

ST (*Security Target* – Alvo de Segurança) é o documento que identifica as propriedades de segurança do TOE. O TOE é avaliado de acordo com os seus requisitos funcionais de segurança (SFRs), podendo referir-se a um ou mais PPs. Dessa forma, permite adequar a avaliação para que corresponda com precisão às capacidades do sistema ou produto. Normalmente, é publicado para que os clientes possam determinar as características específicas de segurança que tenham sido certificadas pela avaliação.

SFR (*Security Functional Requirements* – Requisitos Funcionais de Segurança) determina o nível de segurança individual das funções que podem ser oferecidas por um produto. A lista de SFRs pode variar de uma avaliação para a outra, mesmo se dois objetivos são do mesmo produto. Embora o *Common Criteria* não prescreva qualquer SFRs a ser incluída em um ST, pode identificar dependências onde o correto funcionamento de uma função (como a capacidade de limitar o acesso de acordo com papéis) é dependente de outro (como a habilidade de identificar os vários papéis) [67].

A Norma ISO/IEC 15.408 também avalia de acordo com a garantia de qualidade de processos. EAL (*Evaluation Assurance Level* – Nível de Garantia de Avaliação) é uma classificação numérica que determina a profundidade e rigor de uma avaliação. Cada EAL corresponde a um pacote de requisitos de garantia de segurança que abrange o desenvolvimento completo de um produto, com um determinado nível de rigor [67]. O CC define sete níveis, sendo EAL 1 o mais básico e barato de se implementar e EAL 7 o mais rigoroso e mais caro. EALs superiores não implicam necessariamente uma “melhor segurança”, significa apenas que a garantia da segurança alegou que TOE tem sido mais extensivamente validado [67].

Seu objetivo é ser usado como base para avaliação de propriedades de segurança de produtos e sistemas de TI, permitindo a comparação entre os resultados de avaliações independentes de segurança, por meio de um conjunto de requisitos padronizados a serem atingidos. O processo de avaliação estabelece níveis de confiabilidade de que as funções avaliadas atinjam os requisitos estabelecidos, ajudando os usuários a determinar se tais sistemas ou produtos possuem os níveis desejados de segurança e se os riscos advindos de seu uso são toleráveis. Seu público alvo são os desenvolvedores, avaliadores e usuários de sistemas e produtos de TI que requerem segurança.

3.5.6 SQUARE (*Security Quality Requirements Engineering*)

O modelo SQUARE (*Security Quality Requirement Engineering* – Engenharia de Requisitos, Segurança e Qualidade) foi desenvolvido pela Carnegie Mellon University (CMU) e define nove passos para cumprir o processo de desenvolvimento de *software* [75]. O foco do SQUARE é um modelo para construir conceitos de segurança e qualidade em um estágio mais cedo no ciclo de desenvolvimento. Pode ser utilizado para analisar os aspectos de documentação e qualidade de um projeto. Para a utilização do SQUARE, os nove passos a serem seguidos são:

- concordar com definições;
- identificar os objetivos de segurança;
- desenvolver artefatos para apoiar a definição de requisitos de segurança;
- avaliar os riscos;
- selecionar a técnica de levantamento;
- extrair os requisitos de segurança;
- categorizar os requisitos;
- priorizar os requisitos;
- inspecionar os requisitos.

Como a execução do SQUARE normalmente leva muito tempo para ser concluída, a CMU desenvolveu uma versão mais curta, conhecida como SQUARE-Lite que possui cinco passos, são eles:

- concordar com definições;
- identificar os objetivos de segurança;
- avaliar os riscos;
- extrair os requisitos de segurança;
- priorizar os requisitos.

O SQUARE-Lite se adequa bem para as empresas que já possuem um processo de engenharia de requisitos e querem se adequar às exigências de qualidade e de segurança para ele, ou até também para as empresas que ainda não definiram a implementação do modelo completo [75].

3.5.7 Requisitos de Segurança de *Software*

Os requisitos de segurança são definidos como as necessidades do *software* que atendem as políticas regulatórias da organização, fornecendo informações sobre a real necessidade da aplicação de forma a alcançar seus objetivos de negócios. Para a especificação dos requisitos de segurança, deve-se reconhecer as ameaças pelas quais o *software* está submetido, considerando políticas de alto nível para a determinação da pertinência de cada uma das ameaças levantadas [50]. O reconhecimento das ameaças é possível por meio da execução de análises *top-down* ou *bottom-up* de prováveis falhas de segurança.

De acordo com a Norma ISO/IEC 27001, segurança da informação implica na preservação da confiabilidade, da integridade e da disponibilidade da informação, além de outras propriedades, como autenticidade, responsabilidade e não repúdio podem também estar envolvidas [50]. A mesma norma identifica três principais fontes de requisitos de segurança da informação.

Uma fonte é obtida a partir da avaliação de riscos para a organização, com base nos objetivos e estratégias da organização. Utilizando-se da análise de riscos, é possível determinar as ameaças aos ativos e as vulnerabilidades destes, e realizar uma estimativa da probabilidade de ocorrência das ameaças e o impacto sofrido pelo negócio.

A segunda fonte é a regulamentação, estatutos, cláusulas contratuais e legislação vigente que ditam como um provedor de serviços, parceiro comercial ou contratado deve proceder.

Outra fonte é o conjunto de metas, princípios, requisitos e objetivos da organização para o processamento de informação no desenvolvimento de suas atividades.

Os resultados da análise/avaliação de riscos ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos da segurança da informação, bem como a implementação dos controles selecionados para a proteção contra estes riscos [50]. Esta análise/avaliação deve ser repetida periodicamente para contemplar quaisquer mudanças.

Medidas de segurança são essenciais ao cumprimento de requisitos da segurança da informação. São definidas como procedimentos e mecanismos usados para a proteção da informação e seus ativos, de forma que controlem as ameaças e impeçam a exploração de vulnerabilidades. São as seguintes.

- Preventiva: evita que incidentes venham a ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança da instituição.
- Detectáveis: tem como objetivo identificar condições ou indivíduos causadores de ameaças para evitar que as mesmas explorem vulnerabilidades.
- Corretivas: são medidas de segurança que visam corrigir uma estrutura a fim de que a mesma se adapte às condições de segurança previstas.

Além de todos esses conceitos que devem ser levados em conta no momento da definição de requisitos de segurança do sistema, também é necessário que o usuário esteja consciente da importância da segurança no sistema para que ele possa auxiliar na implementação da política da segurança da informação tomando medidas preventivas e evitando maus hábitos em relação à segurança.

3.5.8 Padrões de Segurança

Os padrões de segurança fornecem a solução para um problema. Basicamente, são um conjunto de boas práticas aplicadas pela indústria para limitar ataques. Os padrões capturam a experiência de indivíduos especialistas em segurança e apresentam soluções para problemas relacionados com a segurança, que podem ser aplicados por indivíduos não especialistas [50].

Como os padrões de segurança fornecem meios de proteção a confidencialidade, integridade e disponibilidade, pode-se admitir que também funcionam como guia de desenvolvimento seguro de um *software*, satisfazendo os requisitos funcionais. Assim, os padrões de segurança podem ser úteis para satisfazer os requisitos de segurança.

Padrões geralmente são divididos do seguinte modo.

- Objetivo: descreve o padrão, sua lógica e propósito.
- Contexto: descreve o contexto do problema.
- Problemas: descreve qual problema este padrão soluciona.
- Descrição: um cenário que ilustra o problema de *design*.
- Solução: indica como resolver o problema.
- Consequências: descreve os resultados da utilização do padrão.
- Conhecimentos utilizados: exemplos de padrões encontrados em sistemas reais.

- Padrões relacionados: lista de outros padrões relacionados que utilizam este padrão como referência.

Shumacher [70] cita as vantagens da criação de um padrão, dentre elas destacam-se: a padronização de conhecimentos de segurança em um caminho estruturado e compreensível; a documentação de mecanismos simples e eficazes; o fornecimento de um vocabulário e taxonomia comuns para desenvolvedores; a combinação de padrões para as soluções descritas agilizarem o processo; e a utilização de uma abordagem padrão em todos os níveis de arquitetura, ajudando na integração de altos e baixos níveis.

Padrões de segurança representam uma forma de sintetizar o conhecimento acumulado sobre o *design* de sistemas de segurança. Os padrões de segurança também são destinados a serem utilizados e compreendidos por desenvolvedores que não são profissionais de segurança [71]. Como exemplo de padrões de segurança, propostos por Schumaher [70], pode-se citar o *Threat Assesment, Controlled Process Creator, Access Control Requirements, Role Rights Definition, Role-Based Access Control, Risk Determination, Vulnerability Assessmen*t.

O autor Rosado [71] é relevante para este contexto, pois é considerado um dos principais autores de padrões de segurança, tais como: *Authorization Pattern, RBAC, Multilevel Pattern, Reference Monitor Pattern, Virtual Address Space, Access Control, Execution Domain Pattern, SAP Pattern, Check Point Pattern*.

Romanoski [72] define que os padrões de segurança podem ser explicados por meio da motivação, do problema, das forças, da solução, de consequências, de conhecimentos utilizados e de padrões relacionados. Alguns dos padrões definidos por Romanosky são: *Authoritative Source of Data, Risk Assessment and Management, Enterprise Partner Communication, The Security Provider*.

Segundo Trowbridge [73], as melhores soluções são aquelas compostas por uma série de mecanismo pequenos e simples que resolvem o problema de maneira segura e eficaz. Este autor divide os padrões de segurança em: padrões para a *Web*, padrões para sistemas distribuídos, padrões de desenvolvimento e padrões de organização.

Padrões de segurança também são desenvolvidos no sentido de serem utilizados e entendidos por desenvolvedores que não são profissionais de segurança. Enquanto sua ênfase está na segurança, estes padrões capturam os pontos fortes e deficiências de cada

abordagem diferente, com o intuito de permitir que desenvolvedores tomem decisões a respeito da segurança e outras metas a serem atingidas [74]. Os padrões desenvolvidos por Kienzle [74] apresentam, basicamente, a mesma forma dos autores mostrados anteriormente.

3.6 Modelos de Maturidade para Segurança de *Software*

Modelos de maturidade, em geral, ajudam organizações a entender que há uma progressão de capacidades e competências, na medida em que as organizações se tornam mais proficientes em uma certa área de atuação, como é o caso da Gestão da Segurança da Informação, em que se inclui com destaque a Segurança de *Software* mais atualmente. Eles contêm os elementos essenciais para a construção de processos efetivos para uma ou mais disciplinas e descreve um caminho de melhoria evolucionária que vai desde processos *ad-hoc*, seguindo por processos imaturos, disciplinados e finalizando nos processos maduros com qualidade e efetividade melhorada [76].

Os modelos de maturidade visam o melhoramento de processos de uma organização, e para isso, proveem orientação para ser utilizada no desenvolvimento de processos efetivos, porém, não são processos ou descrições de processos [48].

Destacam-se como modelos de maturidade de segurança de *software* os *frameworks* OpenSAMM e BSIMM. Apesar de ambos modelos serem pautados na melhoria da maturidade da organização, a natureza deles é distinta, uma vez que o primeiro se coloca como um modelo prescritivo, ou seja, ele enumera ações que, na opinião de alguns especialistas, devem ser empreendidas para uma organização produzir *software* seguro [47]. O segundo se propõe a ser um modelo descritivo, ou seja, nele encontram-se consolidadas observações realizadas em campo. Essa diferenciação confere ao modelo BSIMM um caráter científico ausente no OpenSAMM [47].

3.6.1 OpenSAMM (*Open Software Assurance Maturity Model*)

O SAMM [77] é um *framework* aberto para ajudar as organizações a formular e implementar uma estratégia para a segurança de *software*. Foi originalmente desenvolvido por Pravir Chandra, um consultor independente de segurança de *software*. Após o seu lançamento, foi integrado a OWASP (*Open Web Application Security Project*) que ficou conhecido como OpenSAMM.

O OpenSAMM foi projetado para ser bem flexível, podendo assim ser utilizado em pequenas, médias e grandes empresas e utilizando qualquer estilo de desenvolvimento, podendo ser aplicado para projetos individuais ou para toda uma organização. Os recursos oferecidos pelo OpenSAMM ajudarão em [48]:

- avaliar as práticas de segurança de *software* existentes na organização;
- construir e equilibrar o programa de garantia de segurança de *software* em interações bem definidas;
- demonstrar melhoramentos concretos no programa de garantia de segurança;
- definir e mensurar atividades relacionadas à segurança por toda organização.

O OpenSAMM especifica quatro funções de negócios críticos, cada uma com três atividades práticas de segurança, são elas [77]:

Funções de Negócios	**Práticas de Segurança**
Governança	**Estratégia e Métricas:** definição da estratégia que será utilizada para a garantia de *software*. Criar definições de metas de segurança e estudar os riscos da empresa.
	Políticas e Conformidade: entender as diretrizes/políticas e regulamentá-las nos padrões de segurança. Fazer auditorias para descobrir quando algum projeto não atingir as expectativas.
	Orientação e Educação: orientar o pessoal envolvido no desenvolvimento do *software* como implementar um *software* seguro. Uma técnica para melhorar o desempenho é a definição de objetivos para cada funcionário.
	Modelagem de Ameaças: identificar e entender os níveis de risco na

Construção	funcionalidade do *software* no ambiente em que ele será executado. Com base nos detalhes obtidos torna-se mais fácil tomar decisões.
	Requisitos de Segurança: definir o comportamento esperado a respeito da segurança do *software*, definindo cada processo por níveis. Fazer auditorias para garantir que todas as especificações de segurança estão sendo utilizadas.
	Arquitetura de Segurança: projetar *softwares* seguros por padrões reutilizando os componentes, reduzindo assim os riscos de segurança do *software*.
Verificação	**Revisão de Arquitetura:** avaliar a segurança da arquitetura do *software*, permitindo assim detectar problemas logo no início.
	Revisão de Código: inspecionar os códigos fontes a fim de encontrar potenciais falhas no *software* que ocorreram no desenvolvimento.
	Testes de Segurança: testar o *software* a procura de vulnerabilidades, garantindo que os resultados serão os esperados quando estiver em execução.
Implantação	**Gerenciamento de Vulnerabilidades:** gerenciar os relatórios de vulnerabilidades e incidentes operacionais ganhando assim uma base de dados dos problemas ocorridos.
	Proteção de Ambiente: garantir que o *software* será executado corretamente no ambiente de produção, reforçar a segurança da infraestrutura e implementar atualizações de segurança.
	Capacitação Operacional: procurar todo tipo de informação que possa afetar a segurança do *software* e comunicar aos desenvolvedores, assim detalhando os impactos que possam ocorrer para os usuários e operadores.

Tabela 6.1: Definição das funções de negócio do OpenSAMM.

3.6.2 BSIMM (*Building Security In Maturity Model*)

BSIMM (*Building Security In Maturity Model*) é definido como um estudo de iniciativas de segurança em *softwares* existentes. Quantificando as práticas de várias organizações

distintas, pode-se descrever o ponto comum, compartilhado por muitas, e também as variações que fazem cada uma única [35]. O principal objetivo é ajudar o plano comunitário de *software* seguro a realizar e medir suas próprias iniciativas. O BSIMM não é um guia de como fazer, ele é um reflexo do estado da arte do *software* seguro aplicado as organizações [35].

O BSIMM é um modelo de maturidade que considera preocupações do interesse de um programa de segurança de *software*. Essas preocupações estão representadas em 109 atividades, distribuídas em 12 práticas, classificadas nos quatro domínios sendo eles: Governança, Inteligência, SSDL *Touchpoints* e Implantação [47].

- Governança: são práticas que envolvem planejamento, atribuição de papéis e responsabilidades. Identifica os objetivos do programa além do custo a ser gasto durante todo o programa e a identificação dos alvos do programa.
- Inteligência: o domínio visa identificar recursos utilizados no programa de segurança de *software* da organização.
- SSDL (*Software Security Development Lifecycle) Touchpoints*: práticas associadas com o desenvolvimento da aplicação na fase de desenvolvimento.
- Implantação: o domínio de implantação envolve práticas de verificação da aplicação em relação à segurança e verificação dos ativos que o programa entregou.

O BSIMM é resultado de pesquisa que observou vários programas de segurança de *software* com o intuito de reconhecer e consolidar atividades comuns executadas por diversas organizações. As atividades reconhecidas são categorizadas em três níveis, conforme a sua ocorrência nas organizações, ou seja, se uma atividade foi mais observada nas organizações participantes, ela é pautada como uma atividade básica, ou nível 1, à medida que a quantidade de organizações executa alguma atividade, ela vai recebendo um nível maior [47].

Essa grande quantidade de práticas (109 atividades em 12 práticas) não significa que para ter um *software* seguro é necessário a adoção de todas as práticas em todos os níveis, deve ser feito uma adaptação de acordo com o(s) objetivo(s) proposto(s) pela organização e quais práticas poderão auxiliar a alcançá-lo(s) [47].

O BSIMM pode ser usado por alguém responsável por criar e executar iniciativas de segurança de *software* e traz a confiança do conhecimento das melhores práticas sobre

software seguro para estabelecer um *framework* de segurança de *software* [35].

3.7 Atividades de acordo com Modelo de Maturidade BSIMM

O modelo de maturidade BSIMM apresenta uma série de atividades associadas a cada uma das doze práticas. Cada um dos quatro domínios no *Framework* de Segurança de *Software* (SSF) possui suas próprias metas, baseando-se na identificação de metas para cada nível de uma prática, que podem ser detalhadamente divididas em objetivos para a prática/nível e estão desta forma associadas às atividades [35].

As atividades deste *Framework* serão listadas abaixo de uma forma mais objetiva, deste modo, é necessário, para maiores esclarecimentos, que as atividades sejam consultadas diretamente no modelo de maturidade BSIMM e é importante que sejam aplicadas, sempre que possível, no Ciclo de Desenvolvimento de *Software* Seguro.

Escolher quais atividades do BSIMM adotar e em qual ordem pode ser um desafio. Nós sugerimos a criação de uma estratégia e um plano de segurança de *software*, focando nas metas e objetivos em primeiro lugar e deixe as atividades se selecionarem por conta própria. Criando um cronograma para a implementação é sempre muito útil [35].

3.7.1 Governança - Estratégia e Métricas (SM): os objetivos gerais são transparência das expectativas e responsabilização pelos resultados.

3.7.1.1 SM Nível 1 - Alcançar um entendimento comum de direção e de estratégia: os gerentes devem garantir que todos os envolvidos na criação, implantação, operação e manutenção de *software* compreendam os objetivos formalizados de segurança de software da organização.

3.7.1.1.1 Publique o processo (papéis, reponsabilidades, plano), o evolua quando necessário.

3.7.1.1.1.1 Crie o papel de evangelistas e faça propaganda interna.

3.7.1.1.1.2 Eduque os executivos. Os executivos aprendem sobre as consequências da segurança de *software* inadequada e o impacto negativo para o negócio que pode ter uma segurança pobre.

3.7.1.1.1.3 Identifique pontos de barreiras, reúna os artefatos necessários. O processo de segurança de *software* envolverá barreiras para liberação em um ou mais pontos no Ciclo de Vida de Desenvolvimento de *Software* Seguro (SDLC), ou do mais provável, dos SLDCs.

3.7.1.1.1.4 Exija a autorização da segurança. A organização tem um processo amplo de iniciativa para aceitação de riscos de segurança e documentar responsabilização.

3.7.1.2 SM Nível 2 - Alinhe comportamento e estratégia e verifique a aderência. Os gestores devem identificar explicitamente os indivíduos responsáveis pela gestão de risco de segurança de *software*.

3.7.1.2.1 Publique dados sobre segurança de *software* internamente.

3.7.1.2.2 Imponha barreiras com avaliação e rastreie as exceções.

3.7.1.2.3 Crie ou aumente os satélites. O satélite começa como um conjunto de pessoas pela organização que demonstram um nível de interesse ou habilidade em segurança acima da média.

3.7.1.2.4 Identifique métricas e use-as para orientar os orçamentos.

3.7.1.3 SM Nível 3 - Pratique gestão de portfólio baseada em risco: os responsáveis pelas aplicações e o SSG devem informar aos gestores sobre o risco associado a cada aplicação no portfólio.

3.7.1.3.1 Use rastreamento interno de aplicações com visão do portfólio.

3.7.1.3.2 Execute um programa de *marketing* externo. O SSG promove a iniciativa de segurança de *software* fora da empresa para construir apoio externo.

3.7.2 Governança - Conformidade e Política (CP): os objetivos gerais são a orientação normativa para todos os *stakeholders* e auditabilidade da atividades do SSDL.

3.7.2.1 CP Nível 1 - Documente e unifique os direcionadores de conformidade estatutária,

regulatória e contratual.

3.7.2.1.1 Unifique as pressões regulatórias. Se o negócio está sujeito a guias de regulação ou conformidade, o SSG atua como um ponto focal para a compreensão das restrições que tais guias impõem ao *software*.

3.7.2.1.2 Identifique as obrigações PII (Dados de identificação pessoal). A maneira como o software manipula informações de identificação pessoal pode ser expressamente regulada, mas mesmo que não seja a privacidade é muito relevante.

3.7.2.1.3 Crie uma política.

3.7.2.2 CP Nível 2 - Alinhe as práticas internas à regulação de conformidade e política, apoiada pelos executivos.

3.7.2.2.1 Identifique o inventário dos dados PII.

3.7.2.2.2 Exija a autorização da segurança para os riscos de conformidade.

3.7.2.2.3 Implemente e monitore os controles de conformidade.

3.7.2.2.4 Formalize todos os contratos de fornecedores com SLAs de segurança de *software*.

3.7.2.2.5 Promova conscientização dos executivos sobre as obrigações de conformidade e privacidade.

3.7.2.3 CP Nível 3 - Dados de ameaças, ataques, defeitos e questões operacionais direcionam a evolução das políticas e a demanda aos fornecedores.

3.7.2.3.1 Crie um atrativo regulatório.

3.7.2.3.2 Imponha a política a fornecedores.

3.7.2.3.3 Conduza o *feedback* de dados do SSDL de volta à política.

3.7.3 Governança - Treinamento (T): os objetivos gerais são a criação de uma força de trabalho bem informada e a correção de erros no processo.

3.7.3.1 T Nível 1- Disponibilize os treinamentos personalizados, por papel, sob demanda.

3.7.3.1.1 Forneça treinamento de conscientização.

3.7.3.1.2 Distribua um currículo avançado especifico por papéis (ferramentas, listas de tecnologias, mostra de *bugs*).

3.7.3.1.3 Crie e use material específico para a história da companhia.

3.7.3.1.4 Distribua treinamento individual sob demanda.

3.7.3.2 T Nível 2 - Crie o satélite de segurança de *software*. O SSG deve crescer e fortificar os satélites através de atividades sociais, incluindo treinamento e eventos relacionados.

3.7.3.2.1 Fortaleça os satélites através de treinamentos e eventos.

3.7.3.2.2 Traga pessoal de segurança a bordo. O processo para trazer novos contratados para a engenharia da organização requer um módulo para segurança de *software*.

3.7.3.2.3 Identifique satélites através do treinamento.

3.7.3.3 T Nível 3 - Promova o reconhecimento para habilidades e um plano de carreira.

3.7.3.3.1 Recompense o avanço na grade curricular (certificação e RH).

3.7.3.3.2 Forneça treinamento para fornecedores e profissionais terceirizados.

3.7.3.3.3 Hospede eventos externos de segurança.

3.7.3.3.4 Exija reciclagem anual.

3.7.3.3.5 Estabeleça um horário de trabalho para o SSG.

3.7.4 Inteligência - Modelos de Ataque (AM): o objetivo geral é a criação de conhecimento adaptado aos ataques relevantes para a organização. O conhecimento adaptado deve orientar decisões tanto sobre código, como controles.

3.7.4.1 AM Nível 1 - Crie uma base de conhecimento sobre ataques e dados de ativos.

3.7.4.1.1 Elabore e mantenha uma lista de ataques top N.

3.7.4.1.2 Crie um esquema de classificação e inventário de dados.

3.7.4.1.3 Identifique potenciais atacantes.

3.7.4.1.4 Colecione e publique histórias de ataques.

3.7.4.1.5 Reúna inteligência sobre ataques

3.7.4.1.6 Crie um fórum interno para discutir ataques.

3.7.4.2 AM Nível 2 - Forneça divulgação sobre atacantes e ataques relevantes.

3.7.4.2.1 Construa padrões de ataque e casos de abuso amarrados aos potenciais atacantes.

3.7.4.2.2 Crie padrões de ataque específicos por tecnologia.

3.7.4.3 AM Nível 3 - Pesquise e mitigue novos padrões de ataque.

3.7.4.3.1 Mantenha um time de pesquisa que desenvolve novos métodos de ataque.

3.7.4.3.2 Crie e use automação para fazer o que os atacantes farão.

3.7.5 Inteligência - Funcionalidades e Projeto de Segurança (SFD): o objetivo geral é a criação de conhecimento adaptado sobre funcionalidades, *frameworks* e padrões de segurança.

3.7.5.1 SFD Nível 1- Publique os elementos e arquitetura de segurança.

3.7.5.1.1 Construa e publique funcionalidades de segurança.

3.7.5.1.2 Envolva o SSG com a arquitetura.

3.7.5.2 SFD Nível 2 - Construa e identifique soluções de segurança.

3.7.5.2.1 Construa *frameworks*, *middleware* e bibliotecas seguras desde a concepção.

3.7.5.2.2 Crie capacidade no SSG para resolver problemas de projeto complexos.

3.7.5.3 SFD Nível 3 - Reuse ativamente os funcionalidades de segurança aprovadas e *frameworks* seguros desde a concepção.

3.7.5.3.1 Estabeleça um grupo de revisão ou comitê central para aprovar e manter padrões de projeto seguros.

3.7.5.3.2 Exija o uso de funcionalidades e *frameworks* de segurança aprovados.

3.7.5.3.3 Encontre e publique padrões de projetos maduros da organização.

3.7.6 Inteligência - Padrões e Requisitos (SR): o objetivo geral é criar uma orientação normativa para todos os *stakeholders*.

3.7.6.1 SR Nível 1- Forneça padrões e requisitos de segurança acessíveis.

3.7.6.1.1 Crie padrões de segurança.

3.7.6.1.2 Crie um portal de segurança.

3.7.6.1.3 Traduza restrições de conformidade para requisitos.

3.7.6.1.4 Use padrões de código seguro.

3.7.6.2 SR Nível 2 - Comunique padrões formalmente aprovados internamente e para os fornecedores.

3.7.6.2.1 Crie um grupo de revisão de padrões.

3.7.6.2.2 Crie padrões específicos por setores de tecnologia.

3.7.6.2.3 Identifique código aberto.

3.7.6.2.4 Crie um SLA padronizado.

3.7.6.3 SR Nível 3 - Exija decisões de gestão de risco para uso de código aberto.

3.7.6.3.1 Controle o risco de código aberto.

3.7.6.3.2 Comunique padrões aos fornecedores.

3.7.7 SSDL *Touc hpoints* - Análise Arquitetural (AA): o objetivo geral é o controle de qualidade.

3.7.7.1 AA Nível 1 - Realize revisão AA baseada em risco, conduzida pelo SSG.

3.7.7.1.1 Realize revisão de funcionalidades de segurança.

3.7.7.1.2 Realize revisão de projeto para aplicações de alto risco.

3.7.7.1.3 Estabeleça um esforço de revisão coordenado pelo SSG.

3.7.7.1.4 Use um questionário de risco para categorizar as aplicações.

3.7.7.2 AA Nível 2 - Difunda o uso do processo AA documentado.

3.7.7.2.1 Defina e use um processo AA.

3.7.7.2.2 Padronize a descrição de arquitetura (incluindo fluxo de dados).

3.7.7.2.3 Torne o SSG disponível como um recurso ou mentor de AA.

3.7.7.3 AA Nível 3 - Forme capacidade de revisão e remediação dentro do grupo de arquitetos.

3.7.7.3.1 Tenha arquitetos de *software* liderando esforços de revisão de projetos.

3.7.7.3.2 Canalize os resultados de análise para os padrões de arquitetura.

3.7.8 SSDL *Touc hpoints* - Revisão de Código (CR): o objetivo geral é o controle de qualidade.

3.7.8.1 CR Nível 1 - Utilize revisão de código manual ou automatizada com relatórios centralizados.

3.7.8.1.1 Crie uma lista de *bugs top* N (preferencialmente com dados reais).

3.7.8.1.2 Tenha o SSG realizando revisões *ad hoc*.

3.7.8.1.3 Use ferramentas automatizadas juntamente com revisão manual.

3.7.8.1.4 Torne a revisão de código obrigatória para todos os projetos.

3.7.8.1.5 Utilize relatórios centralizados para fechar o laço do conhecimento e orientar e treinamento.

3.7.8.2 CR Nível 2 - Imponha padrões a partir do processo de revisão de código.

3.7.8.2.1 Imponha padrões de código.

3.7.8.2.2 Atribua mentores de ferramentas.

3.7.8.2.3 Use ferramentas automatizadas com regras adaptadas.

3.7.8.3 CR Nível 3 - Construa uma fábrica de revisão de código fonte com regras personalizadas.

3.7.8.3.1 Construa uma fábrica.

3.7.8.3.2 Construa capacidade para erradicar *bugs* específicos de toda a base de código.

3.7.8.3.3 Automatize a detecção de código malicioso.

3.7.9 SSDL *Touc hpoints* - Testes de Segurança (ST): o objetivo geral é o controle de qualidade realizado durante o ciclo de desenvolvimento.

3.7.9.1 ST Nível 1 - Incremente a QA além da perspectiva funcional.

3.7.9.1.1 Garanta que o QA suporte teste de fronteira e de condição de valor limite. O time de QA extrapola o teste funcional para realizar testes antagonistas.

3.7.9.1.2 Oriente os testes com requisitos e funcionalidades de segurança.

3.7.9.2 ST Nível 2 - Integre a perspectiva do atacante aos planos de teste.

3.7.9.2.1 Integre ferramentas de caixa preta de segurança no processo do QA.

3.7.9.2.2 Compartilhe os resultados de segurança com o QA.

3.7.9.3 ST Nível 3 - Entregue teste de segurança baseado em riscos.

3.7.9.3.1 Inclua testes de segurança na automação de QA.

3.7.9.3.2 Realize testes *fuzz* personalizados para as APIs das aplicações.

3.7.9.3.3 Oriente os testes pelos resultados de análise de risco.

3.7.9.3.4 Alavanque análise de cobertura. Os testadores avaliam a cobertura de código de seus testes de segurança para identificar o código que esteja sendo exercitado.

3.7.9.3.5 Comece a construir e aplicar testes antagônicos de segurança (casos de abuso).

3.7.10 Implantação - Testes de Penetração (PT): o objetivo geral é o controle de qualidade do *software* que passou pelo desenvolvimento.

3.7.10.1 PT Nível1 - Corrija os achados do teste de penetração.

3.7.10.1.1 Use testadores externos para encontrar problemas

3.7.10.1.2 Forneça resultados para gestão e mitigação de defeitos do sistema.

3.7.10.1.3 Utilize ferramentas de teste de penetração internamente.

3.7.10.2 PT Nível 2 - Agende testes de penetração regulares com os testadores internos.

3.7.10.2.1 Forneça toda informação disponível aos testadores.

3.7.10.2.2 Agende testes de penetração para cobertura da aplicação.

3.7.10.3 PT Nível 3 - Realize testes profundos de penetração.

3.7.10.3.1 Use testadores externos para realizar testes profundos.

3.7.10.3.2 Faça com que o SSG personalize as ferramentas e *scripts* para testes de penetração.

3.7.11 Implantação - Ambiente de *Software* (SE): o objetivo geral é a gestão da mudança.

3.7.11.1 SE Nível 1 - Garanta que o ambiente da aplicação suporta segurança de *software*.

3.7.11.1.1 Use monitoramento de entradas da aplicação.

3.7.11.1.2 Garanta que o básico de segurança de *host* e de rede esteja no lugar.

3.7.11.2 SE Nível 2 - Utilize guias de instalação publicados e código assinado.

3.7.11.2.1 Publique guias de instalação.

3.7.11.2.2 Utilize código assinado.

3.7.11.3 SE Nível 3 - Proteja o código no lado do cliente e monitore ativamente o comportamento do *software*.

3.7.11.3.1 Use proteção de código contra engenharia reversa.

3.7.11.3.2 Utilize o monitoramento do comportamento e diagnóstico das aplicações.

3.7.12 Implantação - Gestão de Configuração e Gestão de Vulnerabilidade (CMVM): o objetivo geral é gerir mudança.

3.7.12.1 CMVM Nível 1 - Utilize dados da operação para orientar o comportamento do desenvolvedor.

3.7.12.1.1 Crie ou interaja com a resposta a incidentes.

3.7.12.1.2 Identifique os defeitos de *software* encontrados na operação e realimente o desenvolvimento com eles.

3.7.12.2 CMVM Nível 2 - Certifique-se que a resposta de emergência está disponível durante ataques a aplicações.

3.7.12.2.1 Estabeleça uma resposta de emergência à base de código.

3.7.12.2.2 Acompanhe o processo de correção das falhas encontradas na operação do *software*.

3.7.12.2.3 Desenvolva inventário de aplicações em operação.

3.7.12.3 CMVM Nível 3 - Crie um laço apertado entre a operação e o desenvolvimento.

3.7.12.3.1 Corrija todas as ocorrências de *bugs* de *software* em operação.

3.7.12.3.2 Melhore o SSDL para prevenir *bugs* de *software* encontrados na operação.

3.7.12.3.3 Simule uma crise de *software*.

3.7.12.3.4 Opere um programa de recompensas para *bugs*.

3.8 Requisitos Funcionais de Segurança

Os requisitos de segurança de *software* são o conjunto de necessidades de segurança que o *software* deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, e compreendendo aspectos funcionais que descrevem comportamentos, viabilizando a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários (administradores, usuários comuns), autenticação com o uso de credenciais (usuário e senha, certificados digitais, entre outros.), dentre outros.

Os requisitos de segurança devem ser definidos explicitamente e devem ser corresponder aos objetivos e metas de segurança da organização. Quando os requisitos são apropriadamente definidos e documentados é possível mensurar os objetivos e metas de segurança do projeto, facilitando a implementação e liberação do *software* [48].

Os requisitos de segurança aumentam capacidade da aplicação de estar menos vulnerável a possíveis tentativas de ataques e invasões por terceiros. Os requisitos de segurança estão ligados às propriedades de confiança, resiliência e capacidade de recuperação, no que diz respeito a qualidade de *software* [48].

Devido a sua importância, pois através deles é que são endereçadas as principais dificuldades de segurança que uma aplicação deve lidar, os requisitos de segurança precisam ser considerados durante todas as fases de construção e desenvolvimento de um *software* [48].

Nesta seção são apresentados alguns dos requisitos funcionais de segurança mais comuns quando o desenvolvimento de *software* é abordado [80].

3.8.1 Controle de Acesso

É um mecanismo usado para limitar as ações ou operações que um usuário legítimo de um sistema pode realizar, com base nas autorizações aplicáveis ao mesmo no momento do acesso. Uma autorização estabelece o que é permitido ou o que é proibido realizar, com a determinação dos direitos de acesso de um usuário a um objeto específico. Tem por objetivo prevenir que um sistema entre em um estado inseguro, de modo que ele continue a satisfazer uma política de segurança. É recomendável o Controle de Acesso pelos seguintes motivos [80].

3.8.1.1 Possuir funcionalidades de expiração de senha.

3.8.1.2 Possuir regras de composição e de tamanho mínimo de senhas (conceito de "senha forte").

3.8.1.3 Permitir suporte à autenticação de dois fatores (uso combinado de senha e *tokens* ou de senha e biometria, por exemplo).

3.8.1.4 Deve existir mecanismo de escolha da senha pelos novos usuários sem a interferência do pessoal de apoio.

3.8.1.5 Deve existir mecanismo de bloqueio de acesso após número definido de tentativas de *Login* com falha.

3.8.1.6 Controlar, no ambiente de desenvolvimento, o acesso de múltiplos usuários ao mesmo objeto (*check in/out*).

3.8.1.7 Possuir mecanismo de *time out* para *logoff* de usuários após determinado tempo de inatividade, a ser controlado por parametrização.

3.8.1.8 O controle de acesso deve ser uniforme em todo o sistema, utilizando-se uma única rotina de verificação.

3.8.1.9 O controle de acesso deve ser feito na camada mais próxima possível dos dados.

3.8.1.10 O *software* será implantado somente na intranet e o usuário autenticado deve fornecer novamente suas credenciais para acessar a aplicação, uma vez que esteja autenticado na rede.

3.8.1.11 O *software* deverá suportar SSO (*Single-Sign-On*) a terceiros e fornecedores que estão definidos na lista de interessados.

3.8.1.12 A política de autenticação garante a necessidade para dois – ou autenticação com múltiplos fatores para todo o *software* de processamento financeiro.

3.8.2 Autorização

3.8.2.1 O acesso a arquivos secretos de alta sensibilidade deve ser restrito somente a usuários com níveis de permissão secreto e supersecreto.

3.8.2.2 Os usuários não devem ser demandados a enviar suas credenciais sempre, uma vez que ele tenha se autenticado com sucesso.

3.8.2.3 Todos os usuários autenticados herdarão a permissão de leitura somente que são parte do papel do usuário convidado enquanto os usuários autenticados por padrão terão permissão de leitura e escrita como parte do papel de usuário regular.

3.8.2.4 Somente os usuários com acesso administrativo terão todos os direitos dos usuários regulares, adicionalmente a execução de operações.

3.8.3 Controles Criptográficos

Os sistemas desenvolvidos devem garantir Confidencialidade, Disponibilidade e Integridade das informações por eles processadas. Sempre que aplicável, os referidos sistemas deverão implementar controles criptográficos seguindo as Normas de Segurança da

contratante. As diretrizes são as seguintes [80].

3.8.3.1 Os controles criptográficos deverão tratar a informação observando sua classificação e criticidade.

3.8.3.2 O nível de proteção deve ser identificado com base em uma prévia análise/avaliação de riscos, levando em consideração o tipo, a força e a qualidade do algoritmo de criptografia requerido.

3.8.3.3 As diretrizes de criptografia também se aplicam aos sistemas desenvolvidos para uso em dispositivos móveis.

3.8.3.4 As ações de segurança no desenvolvimento de sistemas devem ser realizadas com base nas Normas ABNT NBR ISO/IEC 27001, 27002, 27005, ISO/IEC 11770 e ISO/IEC 15408, Nível 2.

3.8.3.5 Em caso de perda da chave pelo usuário final ou pela equipe de desenvolvimento, o sistema deve prever troca de chaves; neste caso, o responsável pelo gerenciamento das chaves deve ser comunicado para que a referida chave não mais seja utilizada.

3.8.3.6 Em caso de comprometimento ou dano causado às chaves, o aplicativo deve prever procedimento de recuperação. Além disso, o fato deve ser comunicado ao responsável pelo gerenciamento e o tratamento deve ser dado para que elas não mais sejam usadas.

3.8.3.7 Em caso de uso de certificação digital, os sistemas desenvolvidos deverão observar a validade do mesmo, de forma a não comprometer a continuidade de negócio; os aplicativos deverão gerar alertas quanto à expiração a partir de um prazo definido pelo gestor.

3.8.3.8 O uso de controles criptográficos deve observar a necessidade de desempenho e tempo de resposta requerida pelo sistema, de forma a não comprometer os referidos parâmetros.

3.8.3.9 Senha e outros campos de entrada de dados sensíveis necessitam ser mascarados.

3.8.3.10 Senhas não devem ser armazenadas às claras nos sistemas *backend*, e quando armazenadas devem passar por processo de *hash* com uma função pelo menos equivalente a SHA-256.

3.8.3.11 TLS (*Transport Layer Security*) como SSL (*Secure Socket Layer*) deve ser colocado em prática para proteger contra ameaças internas de *Man-in-the-Middle* (MITM) para todas as informações financeiras que sejam transmitidas.

3.8.3.12 O uso de protocolos reconhecidamente inseguros como, por exemplo, FTP (*File Transfer Protocol*) para transmitir credenciais de contas em texto claro a terceiros fora de sua organização deve ser proibido.

3.8.3.13 Arquivos de *log* não devem armazenar qualquer informação sensível como definido pelo negócio, de modo que seja compreensível por seres humanos.

3.8.4 Trilha de Auditoria e *Logging*

É relevante possuir recursos de trilha de auditoria, com dados sobre os eventos referentes à autenticação de usuários e suas ações, de forma a manter registros das operações de atualização e das consultas a informações sigilosas permitindo o rastreamento de transações efetuadas, considerando “quem”, “quando”, “onde”, “o quê” e tipo de alteração (inclusão, alteração, exclusão e consulta), e possibilitar o envio para servidores remotos, no padrão *syslog* e mediante protocolo de transporte orientado à conexão, dos registros de auditoria gerados, logo após a ocorrência dos eventos [80].

3.8.4.1 Todas as tentativas de autenticação devem ser registradas juntamente com o *timestamp* e o endereço de IP de origem da requisição.

3.8.4.2 Os valores anteriores e posteriores a uma mudança de preço modificado por um usuário, quando da atualização de um preço por um usuário, devem ser monitorados com os seguintes campos auditados: identidade, ação, objeto e *timestamp*.

3.8.4.3 Os *logs* de auditoria devem sempre ser adicionados de novos registros e nunca

sobrescritos.

3.8.4.4 Os *logs* de auditoria devem ser mantidos de forma segura por um período de 3 anos.

3.8.5 Integridade

3.8.5.1 Todos os formulários de entrada e *query strings* necessitam ser validadas frente a um conjunto de entradas aceitáveis, antes do *software* aceitá-los para processamento;

3.8.5.2 O *software* a ser publicado deve ser disponibilizado juntamente com o *checksum* e a função *hash* usada para computar o *checksum*, de modo que o interessado possa validar sua precisão e completude;

3.8.5.3 Todos os personagens não humanos, como usuários para sistemas ou processos *batch*, devem ser identificados, monitorados e possuir escopo limitado no âmbito de sua alteração de dados, a medida de sua utilização nos sistemas que eles executam a não ser que explicitamente autorizado para tal.

3.8.6 Disponibilidade

3.8.6.1 O *software* deve oferecer alta disponibilidade de oito (8) noves (9), como definido pelo SLA (*Service Level Agreement*).

3.8.6.2 O *software* deve estar preparado para atender capacidade máxima de 300 usuários simultâneos.

3.8.6.3 O *software* e seus dados devem ser replicados por todos os centros de dados para prover balanceamento de carga e redundância.

3.8.6.4 A funcionalidade de missão crítica no *software* deve ser restaurada a operação normal no prazo de 1 hora de descontinuidade; funcionalidade de missão essencial no *softwar*e deve ser restaurada a operação normal no prazo de 4 horas da

interrupção, e funcionalidade de missão suporte no *software* deve ser restaurada a operação normal no prazo de 24 horas.

3.8.7 Gerenciamento de Sessão

3.8.7.1 Cada atividade do usuário deverá ser rastreada de modo único.

3.8.7.2 O *software* não deve solicitar as credenciais de acesso do usuário, uma vez que ele esteja autenticado na aplicação.

3.8.7.3 As sessões devem ser explicitamente suspensas quando o usuário solicita o *logoff* ou fecha a janela do navegador.

3.8.7.4 Identificadores de sessão usados para identificar a sessão de usuários devem não ser passados em claro ou ser facilmente adivinhado.

3.8.8 Erros e Gerenciamento de Exceção

3.8.8.1 Todos os erros e exceções devem ser explicitamente manipulados a partir de blocos *try, catch* e *finally.*

3.8.8.2 Mensagens de erro, que são mostradas ao usuário, revelarão somente a informação necessária, sem vazamento de detalhes internos do sistema na mensagem de erro.

3.8.8.3 Detalhes de exceções de segurança devem ser auditados e monitorados periodicamente.

3.8.9 Parâmetros de Configuração

3.8.9.1 Os dados sensíveis do arquivo de configuração da aplicação *web*, como *strings* de conexão, devem ser criptografados.

3.8.9.2 Senhas e chaves de criptografia não devem ser registradas no código fonte do *softwar*e.

3.8.9.3 A inicialização e a liberação de variáveis globais necessitam ser monitoradas com muito cuidado.

3.8.9.4 Eventos de inicialização e interrupção de sessão devem incluir proteções na informação de configuração como uma salvaguarda contra ameaças de vazamento.

3.8.10 Termos de Compromisso e Sigilo

3.8.10.1 A **contratada** deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do **contratante** ou de terceiros de que tomar conhecimento em razão da execução do contrato, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes.

3.8.10.2 A **contratada** deverá manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, incluindo os coletores de dados e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos trabalhos de levantamento de requisitos, construção, implantação e execução dos serviços, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo contratante a tais documentos.

3.8.10.3 A **contratada** deverá assinar o termo de compromisso de manutenção de sigilo e cumprimento das normas de segurança da informação, declarando total obediência às normas de segurança vigente, ou que venham a ser implantada, a qualquer tempo, pelo **contratante**.

3.8.10.4 Os funcionários da **contratada** diretamente envolvidos na contratação

deverão assinar o Termo de Ciência da Declaração de Manutenção de Sigilo e das Normas de Segurança vigentes na entidade.

3.8.11 Propriedade Intelectual

3.8.11.1 O **contratante**, para todos os efeitos da aplicação da Lei n.º 9.609/98, que dispõe sobre a proteção da propriedade intelectual de programa de computador, e regulamentos correlatos, é o único proprietário dos produtos entregues pela prestadora de serviços.

3.8.11.2 O **contratante** terá o direito de propriedade intelectual do *software* e respectivos componentes, bem como de todos os artefatos gerados nas etapas de fabricação de forma permanente, permitindo ao **contratante**, a qualquer tempo, distribuir, alterar e utilizar o *software* sem limitações de quaisquer licenças restritivas.

3.9 Requisitos não Funcionais de Segurança

Os requisitos não funcionais de segurança são aqueles não ligados diretamente à codificação dos sistemas de informação, mas que agregam segurança ao processo de desenvolvimento de *software.* Requisitos não funcionais de segurança contemplam medidas administrativas diretamente relacionadas ao ambiente de desenvolvimento de *software* e aos procedimentos de geração dos sistemas. Requisitos não funcionais têm como objetivo minimizar o roubo de código, introdução de código malicioso, garantir o sigilo do código fonte, garantir a origem e autenticidade dos executáveis gerados, permitir o rastreamento de alterações nos códigos fontes e controlar o fluxo de informação. As recomendações de segurança estão divididas nas seções a seguir [80].

3.9.1 Gerência de Configuração

O objetivo de segurança da Gerência de Configuração é garantir a integridade dos

códigos-fonte e prevenir alterações, subtrações, extravios e edição não autorizada do sistema. A gerência de configuração deve proceder da seguinte maneira [80].

3.9.1.1 Detectar modificações não autorizadas ou acidentais no sistema ou em partes do sistema quando ocorrerem.

3.9.1.1.2 Prover, de maneira automatizada a garantia que somente modificações autorizadas sejam implementadas no sistema e em todos os itens de configuração.

3.9.1.1.3 Prover meios automatizados para averiguar as mudanças entre o sistema e sua versão predecessora. Se nenhuma versão prévia do sistema existir, o desenvolvedor precisa prover meio automatizado para averiguar as mudanças entre o sistema e uma versão futura.

3.9.1.1.4 Garantir a integridade do sistema desde os estágios de elaboração até os esforços de manutenção subsequentes.

3.9.1.1.5 Descrever todos os passos necessários para geração, instalação e inicialização segura do sistema.

3.9.1.1.6 Descrever todos os procedimentos necessários para manter a segurança ao distribuir versões do sistema para o ambiente usuário.

3.9.1.1.7 Identificar unicamente o sistema para garantir que não haja dúvidas quanto à versão que está sendo utilizada e para que todos os usuários envolvidos possam ter certeza de quais versões do sistema estão utilizando.

3.9.1.1.8 A referência deve ser única para cada versão do sistema.

3.9.1.1.9 Identificar unicamente os itens de configuração para melhorar a compreensão da composição do sistema, contribuindo para o avaliador determinar os itens de configuração passíveis de avaliação.

3.9.1.1.10 Incluir uma lista de configuração e descrever o método de identificação dos itens de configuração.

3.9.1.1.11 Identificar todos os itens de configuração inclusos no sistema.

3.9.1.1.12 Identificar unicamente todos os itens de configuração inclusos no sistema a cada versão.

3.9.1.1.13 Descrever os itens de configuração inclusos no sistema.

3.9.1.1.14 Prover controles a fim de garantir que modificações não autorizadas não sejam feitas no sistema, ajudando a manter sua integridade.

3.9.1.1.15 Implementar procedimentos de aceite para confirmar que qualquer criação ou modificação de itens de configuração tenha sido previamente autorizada.

3.9.1.1.16 Implementar as ferramentas automatizadas que precisam apoiar as numerosas mudanças que acontecem durante o desenvolvimento e assegurar que essas mudanças serão autorizadas.

3.9.1.1.17 Descrever as ferramentas automatizadas utilizadas no sistema de gerência de configuração.

3.9.1.1.18 Descrever como são utilizadas as ferramentas automatizadas do sistema de gerência de configuração.

3.9.1.1.19 Assegurar que todos os itens de configuração são controlados por meios automatizados.

3.9.1.1.19.2 Garantir que exista controle na distribuição do sistema e nos procedimentos de entrega do sistema, a fim de garantir que os clientes recebam a aplicação conforme ela foi criada, sem quaisquer modificações. Para se considerar uma entrega válida, os procedimentos usados para a distribuição do sistema devem endereçar as ameaças ou descrição funcional relacionadas à segurança do sistema durante a entrega. Esses procedimentos visam garantir que: o sistema recebido pelo usuário corresponda, precisamente, à cópia mestra do sistema; evitar ou detectar qualquer falsificação da versão atual do sistema; prevenir que versões adulteradas/fraudulentas do sistema sejam distribuídas; evitar divulgação não autorizada da distribuição do sistema; evitar ou detectar que o sistema seja interceptado durante entrega; evitar atrasos ou extravios de distribuição do sistema.

3.9.2 Gerência de Requisitos

São competências da Gerência de Requisitos [80], a saber.

3.9.2.1 Descrever os Requisitos Funcionais de Segurança e suas interfaces externas, ainda que de modo informal.

3.9.2.2 Descrever o propósito e método de utilização das interfaces externas de todos os Requisitos Funcionais de Segurança, fornecendo detalhes dos objetos, exceções e mensagens de erro.

3.9.2.3 Atender completamente aos Requisitos Funcionais de Segurança.

3.9.2.4 Descrever a estrutura das funções de segurança em subsistemas e as funcionalidades de segurança implementadas por cada função de segurança em subsistemas.

3.9.2.5 Identificar qualquer *hardware, firmware*, e/ou *softwares* (DLL´S, etc.) de camadas próximas solicitados pelas funções de segurança do sistema, com a condição de representar as funções de segurança implementadas por aquele determinado *hardware, firmware*, ou *software*.

3.9.3 Gerência de Documentação

O objetivo das recomendações da Gerência de Documentação é garantir que os requisitos de segurança estejam na documentação de orientação (manuais) de usuários e administradores. A Gerência de Documentação deve [80]:

3.9.3.1 Garantir que todo sistema tenha documentação com foco no Administrador descrevendo:

3.9.3.1.1 As funções administrativas e interfaces acessíveis aos administradores do sistema.

3.9.3.1.2 Como administrar o sistema de maneira segura.

3.9.3.1.3 Alertas e avisos sobre funções e privilégios que devem ser controlados em um ambiente operacional seguro.

3.9.3.1.4 Todas as suposições relativas ao comportamento de usuário que possam comprometer a segurança do sistema.

3.9.3.1.5 Todos os parâmetros de segurança sob o controle do administrador e seus valores apropriados.

3.9.3.1.6 Os eventos significativos de segurança e as ações necessárias a serem desempenhadas para garantir a operação segura do sistema, incluindo quaisquer mudanças de características na camada de apoio ou sistemas sob o controle da função de segurança.

3.9.3.1.7 Todos os requisitos de segurança para o ambiente de TI que sejam relevantes para o administrador.

3.9.3.2 Garantir que todo sistema tenha documentação com foco no Usuário descrevendo:

3.9.3.2.1 As funções e interfaces acessíveis a usuários do sistema.

3.9.3.2.2 O uso das funções de segurança acessíveis ao usuário fornecidas pelo sistema.

3.9.3.2.3 Alertas e avisos sobre funções e privilégios que devem ser controlados para uma operação segura.

3.9.3.2.4 Claramente ao usuário, suas responsabilidades referentes a operação segura do sistema, incluindo aquelas relacionadas as premissas de comportamento do usuário, descritas na declaração de segurança do sistema.

3.9.3.2.5 De uma forma consistente e coerente baseada na documentação provida para avaliação.

3.9.3.2.6 Todos os requisitos de segurança para o ambiente de TI, que apresentem relevâncias ao usuário.

3.9.4 Ciclo de Vida de *Software*

O ciclo de vida de um *software* abrange todas as etapas do desenvolvimento de um *software*, de sua concepção a sua extinção. Visa definir as premissas intermediárias que permitem a validação do desenvolvimento da aplicação e a verificação dos métodos aplicados. O Ciclo de Vida de *Software* deve [80]:

3.9.4.1 Especificar um modelo de ciclo de vida a ser adotado.

3.9.4.1.1 O documento de definição do ciclo de vida deve descrever o modelo usado no desenvolvimento e manutenção do sistema.

3.9.4.1.2 O modelo de ciclo de vida adotado deve dispor de controles apropriados para o desenvolvimento e manutenção do sistema.

3.9.4.2 Fazer recomendações de segurança no desenvolvimento, que englobe medidas de segurança física para o ambiente e procedimentos operacionais.

3.9.4.2.1 Fornecer procedimentos para tratamento de falhas aos desenvolvedores do sistema.

3.9.4.2.2 Estabelecer procedimentos para receber e agir sobre qualquer notificação de falhas de segurança e requisições para correções dessas falhas.

3.9.4.2.3 Fornecer orientação de tratamento de falhas dirigida aos usuários do sistema.

3.9.4.3 O tratamento de falhas exige procedimentos claros para receber ou reportar falhas de segurança no sistema, endereçá-las corretamente e tratá-las conforme sua criticidade, risco e tempo necessários para sua correção, distribuição e implantação.

3.9.4.3.1 Descrever os procedimentos para mapeamento e rastreamento das falhas de segurança reportadas ou descobertas em cada *release* ou versão do sistema.

3.9.4.3.2 Solicitar uma descrição da natureza e efeito que cada falha de segurança pode acarretar, assim como a correção apresentada para a falha.

3.9.4.3.3 Solicitar que ações corretivas sejam devidamente identificadas para cada falha de

segurança.

3.9.4.3.4 Descrever os procedimentos adotados em caso de falhas, desde sua percepção, correções e um guia de ações corretivas aos usuários.

3.9.4.3.5 Descrever os métodos usados para relatar falhas, correções e guiar ações corretivas aos usuários do sistema.

3.9.4.3.6 Descrever as maneiras e meios que o desenvolvedor receberá, dos usuários do sistema, as respostas e solicitações sobre suspeitas de falha de segurança no sistema.

3.9.4.3.7 Garantir que qualquer falha reportada será corrigida e a correção comunicada e dirigida aos usuários do sistema.

3.9.4.3.8 Garantir que correções não impliquem em novas falhas de segurança

3.9.4.3.9 Descrever uma maneira de como os usuários do sistema podem reportar uma suspeita de quebra de segurança.

3.9.4.4 Especificar as ferramentas e técnicas que são usadas para a elaboração do sistema.

3.9.4.4.1 Todas as ferramentas de desenvolvimento usadas para implementação devem ser bem definidas.

3.9.4.4.2 A documentação das ferramentas de desenvolvimento deve definir, de maneira clara e não ambígua, todas as opções e valores usados na implementação das ferramentas.

3.9.4.4.3 A documentação das ferramentas de desenvolvimento deve definir, de maneira clara, o propósito para cada opção definida na ferramenta de desenvolvimento.

3.9.5 Teste de *Software* e Análise de Vulnerabilidade

Esta etapa ajuda a estabelecer que a segurança esteja de acordo com os requisitos funcionais de segurança, embora não constate que o sistema não faz mais do que foi especificado e descrito. Os testes também podem ser dirigidos à estrutura interna da função de segurança, para provar que subsistemas ou módulos atendem às especificações. Avalia

também a existência de vulnerabilidades no sistema, uso indevido e configuração incorreta do sistema verificando a possibilidade de quebra de mecanismos probabilísticos (ex.: criptografia) ou permutacionais (ex.: senhas) e a possibilidade de exploração de vulnerabilidades introduzidas propositadamente no desenvolvimento ou operação do sistema. O Teste de *Software* deve atender as seguintes características [80].

3.9.5.1 Confirmar que a(s) função(ões) de segurança opera(m) de acordo com sua especificação. (Testes Funcionais dos Casos de Uso das Funções de Segurança).

3.9.5.2 Gerar evidências sobre a cobertura de testes contendo:

3.9.5.2.1 A correspondência entre os testes identificados na documentação de teste e a função de segurança como descrito na especificação funcional.

3.9.5.3 Contemplar teste de profundidade:

3.9.5.3.1 Demonstrando, na documentação de teste, que as funções de segurança operam de acordo com a descrição de alto nível.

3.9.5.4 Ser documentado contendo:

3.9.5.4.1 Planos de teste, descrições de procedimento de teste, resultados esperados do teste e resultados de teste atuais.

3.9.5.4.2 Os planos de teste identificam a função de segurança a ser testada e descreve os objetivos dos testes a serem executados.

3.9.5.4.3 A descrição dos procedimentos de testes identifica os testes a serem executados e descrevem os cenários para testar cada função de segurança. Esses cenários incluem quaisquer dependências nos resultados de outros testes.

3.9.5.4.4 O planejamento do teste deve mostrar, antecipadamente, o resultado esperado da execução do teste.

3.9.5.4.5 O resultado do teste do desenvolvedor deve demonstrar que cada função de segurança testada se comportou como especificada.

A Análise de Vulnerabilidade deve:

3.9.5.5 Detectar facilmente estados inseguros do sistema.

3.9.5.6 Fornecer uma documentação de ajuda que apresente identificação de todos os possíveis modos de operação da aplicação, inclusive de operações que possam conduzir a falhas, suas consequências e implicações para manutenção de uma operação segura.

3.9.5.6.1 Esta documentação identifica todos os possíveis modos de operação do sistema (Incluindo operação após falhas de sistema ou erro operacional), suas consequências e implicações para manter a operação segura.

3.9.5.6.2 A documentação de orientação deve ser Clara, Completa, Consistente e Racional.

3.9.5.6.3 A documentação de orientação deve listar todas as considerações a respeito do ambiente operacional pretendido.

3.9.5.6.4 A documentação de orientação deve listar todos os requisitos para medidas externas de segurança, incluindo procedimentos, segurança física e em pessoas.

3.9.5.7 Deve conter uma especificação de resistência ou força na função de segurança do sistema, a análise de resistência. Esta análise deve demonstrar:

3.9.5.7.1 Que atende ou excede a especificação mínima de força ou descrição funcional.

3.9.5.7.2 Que a função de segurança atende ou excede a especificação de força, resistência ou métrica ou descrição funcional.

3.9.5.8 Ser documentada descrevendo:

3.9.5.8.1 O tratamento dado as maneiras óbvias que um usuário teria de tentar violar as funções de segurança.

3.9.5.8.2 As vulnerabilidades óbvias de segurança e confirmar que não podem ser exploradas no ambiente da qual a aplicação será instalada.

4 Políticas e Recomendações Técnicas e Operacionais para Protocolo de Comunicação Segura

No contexto da segurança da informação e em consonância com os resultantes de um subconjunto das atividades previstas no termo de cooperação, o principal objetivo desta seção do relatório técnico é fornecer políticas e recomendações técnicas e operacionais em segurança da informação para o protocolo de comunicação segura da infraestrutura, comunicação e armazenamento do Sistema Nacional do Registro de Identificação Civil.

São objetivos desta seção: estabelecer mecanismos e controles para garantir a efetiva proteção dos dados e informações, bem como a redução de riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações.

4.1 Políticas Técnicas

A seguir será apresentado um conjunto de políticas, extraídas de legislação e normas internacionais afeitas ao tema estudado por este relatório. Este conjunto tem por objetivo orientar a equipe técnica do RIC na adoção segura de padrões e políticas técnicas em segurança da informação.

- Segundo art. 1° do Decreto nº 8.135 [92], de 4 de novembro de 2013, as comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.

- Segundo a Portaria SLTI/MP nº 92, de 24 de dezembro de 2014 [93], a qual institui a arquitetura ePING [94] (Padrões de Interoperabilidade de Governo Eletrônico), que define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de governo eletrônico, a adoção dos padrões e políticas contidos abaixo é obrigatória para os órgãos do governo federal.
- Os dados, informações e sistemas de informação do governo devem ser protegidos contra ameaças, de forma a reduzir riscos e garantir a integridade, confidencialidade, disponibilidade e autenticidade, observando-se as normas do governo federal referentes a Política de Segurança da Informação e Comunicações, favorecendo, assim, a interoperabilidade.
- Os dados e informações devem ser mantidos com o mesmo nível de proteção, independentemente do meio em que estejam sendo processados, armazenados ou trafegando.
- As informações classificadas e sensíveis que trafegam em redes inseguras, incluindo as sem fio, devem ser cifradas de modo adequado, conforme os componentes de segurança especificados neste documento, em normas oficiais e ferramentas ou técnicas adquiridas/implementadas para fins de proteção de informações, conforme recomendações de mercado consolidadas.
- Os requisitos de segurança da informação dos serviços e de infraestrutura devem ser identificados e tratados de acordo com a classificação da informação, níveis de serviço definidos e com o resultado da análise de riscos.
- A segurança deve ser tratada de forma preventiva. Para os sistemas que apoiam processos críticos, deverão ser elaborados planos de continuidade, nos quais serão tratados os riscos residuais, visando atender aos níveis mínimos de produção.
- A segurança é um processo que deve estar inserido em todas as etapas do ciclo de desenvolvimento de um sistema.
- Os sistemas devem possuir registros históricos (*logs*) para permitir auditorias e provas materiais, sendo imprescindível a adoção de um sistema de sincronismo de tempo centralizado, bem como a utilização de mecanismos que garantam a

autenticidade dos registros armazenados, se possível, com assinatura digital.

- Nas redes sem fio metropolitanas, recomenda-se a adoção de valores aleatórios nas associações de segurança, diferentes identificadores para cada serviço e a limitação do tempo de vida das chaves de autorização.
- O uso de criptografia e certificação digital para a proteção do tráfego, armazenamento de dados, controle de acesso, assinatura digital e assinatura de código deve estar em conformidade com as regras da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) [85].
- A documentação dos sistemas, dos controles de segurança e das topologias dos ambientes deve ser mantida atualizada e protegida, mantendo-se grau de sigilo compatível.
- Os usuários devem conhecer suas responsabilidades com relação à segurança e devem estar capacitados para a realização de suas tarefas e utilização correta dos meios de acesso.
- Os órgãos da Administração Pública Federal – APF, visando a melhoria da segurança, devem ter como referência: Decreto nº 3.505/2000; Decreto nº 7.845/2002; a Instrução Normativa nº 01/2008 – GSI/PR e suas Normas Complementares; a Instrução Normativa nº 02/2013 – GSI/PR; a Instrução Normativa nº 3/2013 – GSI/PR; e as Normas NBR ISO/IEC 27001:2006 – Sistemas de Gestão de Segurança da Informação; NBR ISO/IEC 27002:2005 – Código de Prática para a Gestão da Segurança da Informação; NBR ISO/IEC 27003:2011 – Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação; NBR ISO/IEC 27004:2010 – Medição; NBR ISO/IEC 27005:2008 – Gestão de Riscos de Segurança da Informação; NBR ISO/IEC 27011:2008 – Diretrizes para Gestão da Segurança da Informação para Organizações de Telecomunicações Baseadas na ABNT NBR ISO/IEC 27002; e NBR 15999-1:2007 e 15999-2:2008 – Gestão de Continuidade de Negócios.
- Para especificações sobre cartões inteligentes, *tokens* e outros dispositivos HSM (*Hardware Security Module*), deverão ser adotados os requisitos contidos nos normativos que tratam da homologação de equipamentos e sistemas no âmbito da ICP-Brasil. Estes requisitos, observados por produtos homologados na ICP-Brasil, tais como mídias que armazenam os certificados digitais e

respectivas leitoras, além dos sistemas e equipamentos necessários à realização da certificação digital, estabelecem padrões e especificações técnicas mínimas, a fim de garantir a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação por eles utilizados.

- Os protocolos FTP (*File Transfer Protocol*) e/ou HTTP (*HyperText Transfer Protocol*) devem ser utilizados para transferência de arquivos, observando suas funcionalidades para recuperação de interrupções e segurança. Para transferência de arquivos sensíveis e/ou cifrados, utilizar SSH FTP e/ou HTTPS.

4.2 Recomendações Técnicas

O presente conjunto de recomendações tem por objetivo orientar a equipe técnica do RIC na adoção adequada de processos de comunicação segura, assinatura digital, criptografia, segurança do meio eletrônico, etc.

Diversos padrões e procedimentos foram abordados de modo breve e objetivo, visando permitir a comunicação segura entre aplicações e servidores, além de preservar questões de segurança, sigilo e integridade.

As normas e recomendações utilizadas neste capítulo podem ser obtidas diretamente nas referências descritas no final do documento.

4.2.1 Assinatura Digital

Recomenda-se o uso do algoritmos criptográficos baseados em criptografia de curvas elípticas (ECDSA 512 bits, ECIES) homologados pelo Instituto Nacional de Tecnologia da Informação (ITI) [82] e pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) [85], conforme Instrução Normativa n° 1 de 04 de Junho de 2014 [83] [84] e Resolução n° 65 [91], de 09 de Junho de 2009, seguindo o padrão FIPS 186-4 [86] (*Federal Information Processing Standards Publication* 186-4) do *National Institute of Standards and Technology* (NIST) [87].

Recomenda-se também o uso do algoritmo criptográfico RSA, conforme definido no padrão PKCS #1 (*Public Key Cryptography Standard* #1) *Specifications Version* 2.1 - RSA

Encryption – RFC 3447 [81] e homologado pelo ITI conforme Resolução n° 68 [90] de 13 de outubro de 2009.

4.2.2 Algoritmos para *Hashing* em Assinatura Digitais

Recomenda-se o uso da função SHA 256 ou SHA 512, conforme definido nos padrões FIPS 180-4 (*Secure Hash Standard* (SHS)) [88] e RFC 6234 (*US Secure Hash Algorithms*) [89] e homologado pelo ITI/ICP-Brasil, conforme Resolução n° 65 [91], de 09 de Junho de 2009 e n° 68 [90] de 13 de outubro de 2009.

4.2.3 Criptografia Simétrica

Recomenda-se o uso dos algoritmos simétricos AES, conforme definido no padrão FIPS 197 (*Advanced Encryption Standard* - AES) [95] e 3DES, de acordo com padrão FIPS 46-3 (*Data Encryption Standard* - DES) [96].

4.2.4 Codificação de Dados para Transmissão

Recomenda-se uso do padrão BASE64 para transmissão de dados binários, conforme definido no padrão RFC 2045 Item 6.8 (*Base64 Content-Transfer-Encoding*) [97].

4.2.5 Certificados Digitais

Em conformidade com a legislação brasileira em vigor, é necessário uso de certificados padrão X.509 v.3 (RPF 2459 - *Internet X.509 Public Key Infrastructure; Certificate and CRL Profile*) [98] emitidos por Autoridades Certificadoras homologadas pela ICP-Brasil.

4.2.6 Certificado Digital da Ac-Raiz para Navegadores e Visualizadores de Arquivos

Os certificados da AC-Raiz devem ser instalados nos navegadores e visualizadores de arquivos conforme recomendado na Instrução Normativa nº 05, de 29 de abril de 2009

[99].

4.2.7 Carimbo de Tempo

Segundo o ITI, o carimbo de tempo é um documento eletrônico emitido por uma Autoridade Certificadora do Tempo – ACT, o qual serve como evidência de que uma informação digital existia numa determinada data e hora no passado e destina-se a associar a um determinado *HASH* de um documento assinado eletronicamente ou não, uma determinada hora e data de existência. Recomenda-se o uso de carimbo de tempo, conforme regulamentado pela ICP-Brasil nos documentos:

a) DOC-ICP-11 – versão 1.2 (Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil) [100];

b) DOC-ICP-12 - versão 1.1 (Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil) [101];

c) DOC-ICP-13 (Requisitos Mínimos para as Políticas de Carimbo do Tempo da ICP-Brasil) [102];

d) DOC-ICP-14 (Procedimentos para Auditoria do Tempo na ICP-Brasil) [103].

O carimbo de tempo deve estar de acordo com o padrão publicado na RFC 3628 – *Policy Requirements for Time-Stamping Authorities* (TSAs) [104].

4.2.8 Segurança em Transmissões Eletrônicas de Dados

Recomenda-se uso de medidas de segurança no meio utilizado para troca das mensagens e arquivos entre as partes envolvidas. Uma medida recomendada é a utilização do protocolo de segurança TLS – *Transport Layer Security*, que deve estar de acordo com a RFC 5246 (*The Transport Layer Security Protocol - Version* 1.2) [105] (atualizada pelas RFC 5746 (TLS - *Renegotiation Indication Extension*) [106], RFC 5878 (TLS - *Authorization Extensions*) [107] e RFC 6176 (*Prohibiting Secure Sockets Layer (SSL) Version 2.0*) [108]).

4.2.9 Segurança de Redes Ipv4

Para autenticação de cabeçalho do IP, recomenda-se a utilização do IPSec

Authentication Header, conforme RFC 4303 (IP *Encapsulating Security Payload* - ESP) [109] e RFC 4835 (*Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload* (ESP) *and Authentication Header* (AH) [110]) e seu componente IKE – *Internet Key Exchange*, conforme RFC 4306 (*Internet Key Exchange* (IKEv2) Protocol) [111].

4.2.10 Segurança de Redes Ipv6 (Camada de Rede)

O IPv6 definido na RFC 2460 (*Internet Protocol, Version* 6 (IPv6) *Specification*) [112] (atualizada pela RFC 5095 (*Deprecation of Type 0 Routing Headers in* IPv6) [113]), na RFC 5722 (*Handling of Overlapping IPv6 Fragments*) [114] e na RFC 5871 (*IANA Allocation Guidelines for the IPv6 Routing Header)* [115] apresenta implementações de segurança nativas no protocolo. As especificações do IPv6 definiram dois mecanismos de segurança: a autenticação de cabeçalho AH (*Authentication Header*), descrito na RFC 4302 (IP *Authentication Header*) [116] ou autenticação IP, e a segurança do encapsulamento IP, ESP (*Encrypted Security Payload*), descrita pela RFC 4303 [109].

4.2.11 Prevenção de DDoS

Recomenda-se a utilização de métodos para inibição do uso de IP *Spoofing* [117] em ataques de DDoS [118] nos termos do RFC 2827 (*Network Ingress Filtering: Defeating Denial of Service Attacks which employ - IP Source Address Spoofing*) [119] (atualizada pela RFC 3704 (*Ingress Filtering for Multihomed Networks*) [120]).

4.2.12 Transferência de Arquivos

Para transferência de arquivos, recomenda-se o uso SSH FTP versão 6 (SSH *File Transfer Protocol*), conforme *Draft* 13 de Julho de 2006 [121], *Securing* FTP com TLS, conforme padrão descrito na RFC 4217 (*Securing FTP with TLS*) [122] e HTTPS (*Secure HyperText Transfer Protocol*), conforme RFC 2660 [132] e RFC 2818 (*HTTP Over TLS*) [133].

4.2.13 Segurança em *Web Services*

Para segurança das mensagens SOAP (*Simple Object Access Protocol*) [126], a fim de garantir integridade e confidencialidade, recomenda-se o uso do *Web Services Security* (WS-Security): SOAP *Message Security Version* 1.1.1 [127], conforme padrão especificado pelo grupo OASIS (*Organization for the Advancement of Structured Information Standards*) [128].

4.3 Recomendações Operacionais

O presente conjunto de recomendações operacionais tem por objetivo orientar a equipe técnica do RIC na adoção e operacionalização de processos correlacionados com os protocolos de comunicação segura.

As normas e recomendações utilizadas neste capítulo podem ser obtidas diretamente nas referências descritas no final do documento.

4.3.1 Modelo a ser Seguido

O modelo de comunicação segura a ser seguido para garantia de confidencialidade é o do OpenPGP, conforme RFC 4880 (OpenPGP *Message Format*) item 2.1 (*Confidentiality via Encryption*) [123]. O OpenPGP combina criptografia de chave simétrica com criptografia de chave pública e seu fluxo está padronizado conforme abaixo:

1. o remetente gera uma mensagem;
2. gera-se um número aleatório para ser utilizado como uma chave de sessão para apenas esta mensagem;
3. a chave de sessão é criptografada usando a chave pública de cada destinatário;
4. criptografa-se a mensagem usando a chave de sessão.

Pode-se ainda, para garantir autenticação via assinatura digital, e conforme RFC 4880 - *OpenPGP Message Format - Item 2.2 (Authentication via Digital Signature)* [131], adicionar ao fluxo acima ao processo de assinatura, no qual o remetente gera uma assinatura da mensagem, concatena o resultado com a mensagem e somente após este

processo o passo 4 é efetuado, criptografando a assinatura e a mensagem juntas. Por consequência, o destinatário, após decifrar a mensagem, poderá conferi-la verificando a assinatura anexada.

Assim, o fluxo completo da aplicação (remetente) seria:

1. o remetente gera uma mensagem;
2. o *software* de envio gera um código de *hash* da mensagem;
3. o *software* de envio gera uma assinatura do código de *hash* utilizando a chave privada do remetente;
4. a assinatura é anexada à mensagem;
5. gera-se um número aleatório para ser utilizado como uma chave de sessão para apenas esta mensagem;
6. a chave de sessão é criptografada usando a chave pública de cada destinatário;
7. criptografa-se a mensagem (já com a assinatura concatenada) usando a chave de sessão.

No ponto de vista do servidor (destinatário), o fluxo seria:

1. o destinatário ao receber, decifra a chave de sessão usando a chave privada do destinatário;
2. o destinatário decifra a mensagem usando a chave de sessão;
3. o destinatário mantém uma cópia da assinatura da mensagem;
4. o destinatário gera um novo código *hash* para a mensagem recebida e o verifica utilizando a assinatura da mensagem enviada pelo remetente;
5. se a verificação for bem sucedida, a mensagem é aceita como autêntica.

4.3.2 Geração de Chave Aleatória

A geração de chave aleatória deverá seguir o processo descrito em HMAC *and the Pseudorandom Function*, Item 5 da RFC 5246 (*The Transport Layer Security (TLS) Protocol Version 1.2*) [105] [105a] [105b] e estar em conformidade com o item 4.7 (*Cryptographic Key Management*) da FIPS 140-2 (*Federal Information Processing Standards Publication - Security Requirements for Cryptographic Modules*) [124] e a RFC 4086 (*Randomness Requirements for Security*) [125].

4.3.3 Fluxos de Processos

Os fluxos de processos mapeados abaixo foram criados para que se possa ter uma referência gráfica do modelo de comunicação segura do OpenPGP, conforme RFC 4880 - OpenPGP *Message Format* - item 2.1 (*Confidentiality via Encryption*) [123] e RFC 4880 - OpenPGP *Message Format* - Item 2.2 (*Authentication via Digital Signature*) [131].

4.3.3.1 Gráfico do Fluxo de Processo - Aplicação (Remetente)

A Figura 4.3.1 abaixo faz referência ao fluxo completo do ponto de vista da aplicação (remetente), conforme item 4.1.

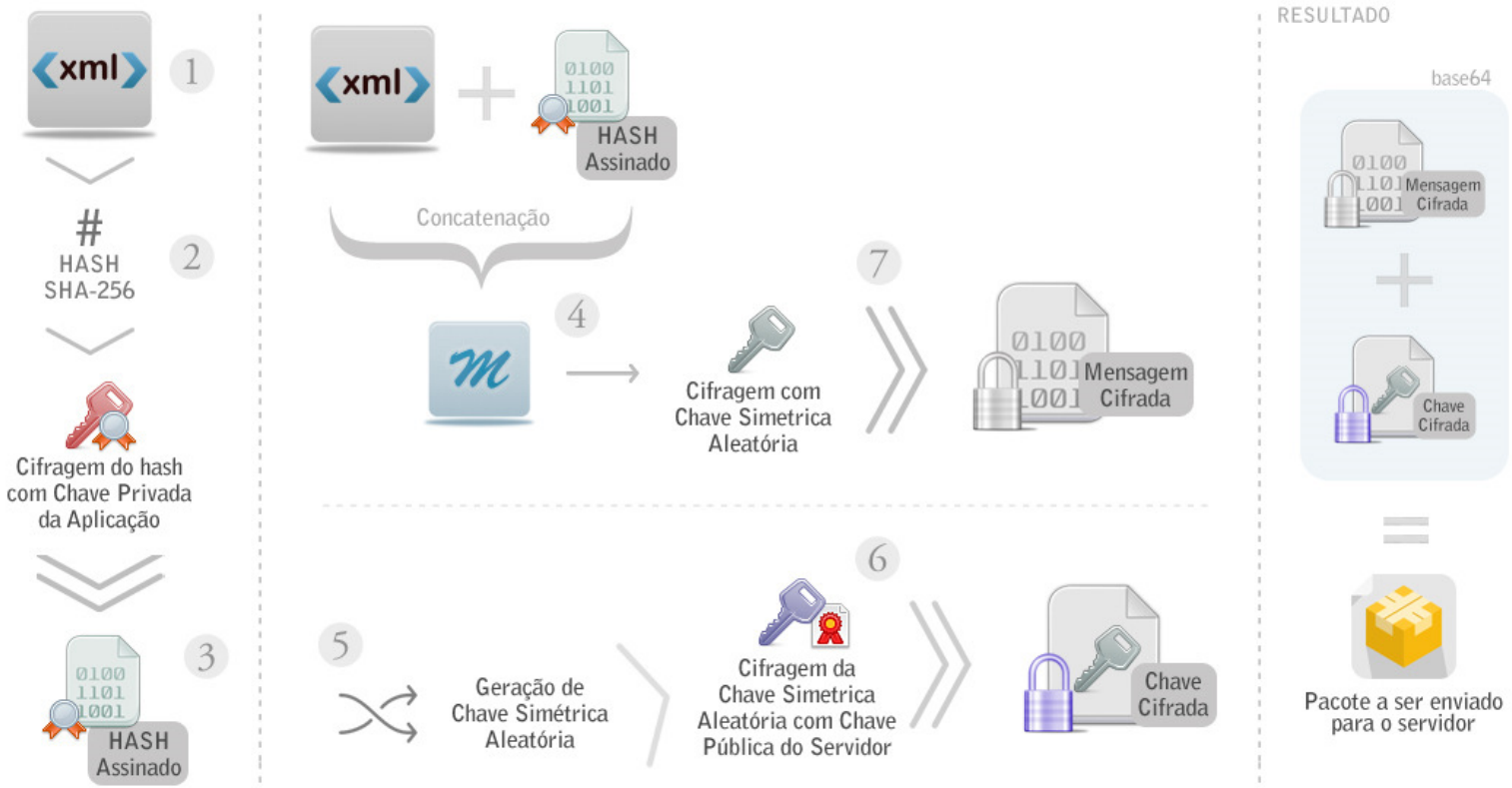

Figura 4.3.1 – Fluxo geral da aplicação (remetente).

4.3.3.2 Grafico do Fluxo de Processo - Servidor (Destinatário)

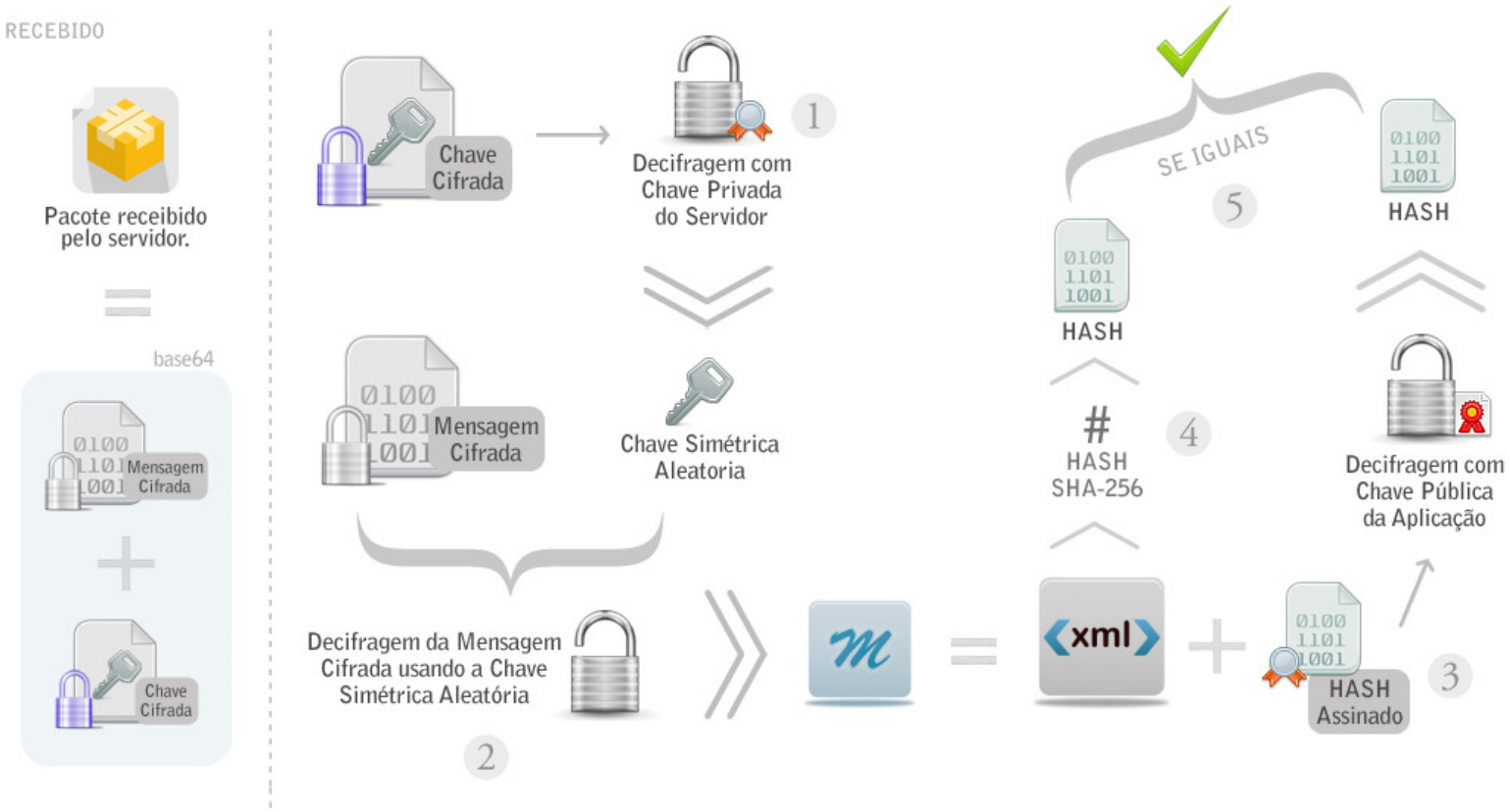

Figura 4.3.2 – Fluxo geral do servidor (destinatário).

4.3.3.3 Fluxo Geral - *Cryptool* 2 (Ct2)

O *CrypTool* 2 (CT2) [129] é um *software open-source* [130] que oferece uma interface inovadora para experiências reais com processos criptográficos. O gráfico abaixo foi criado dentro do *CrypTool* como uma referência aos fluxos previamente mostrados e como um modelo de validação dos processos mapeados. O esquema abaixo pode ser verificado utilizando o arquivo fluxo_cryptool.cwm.

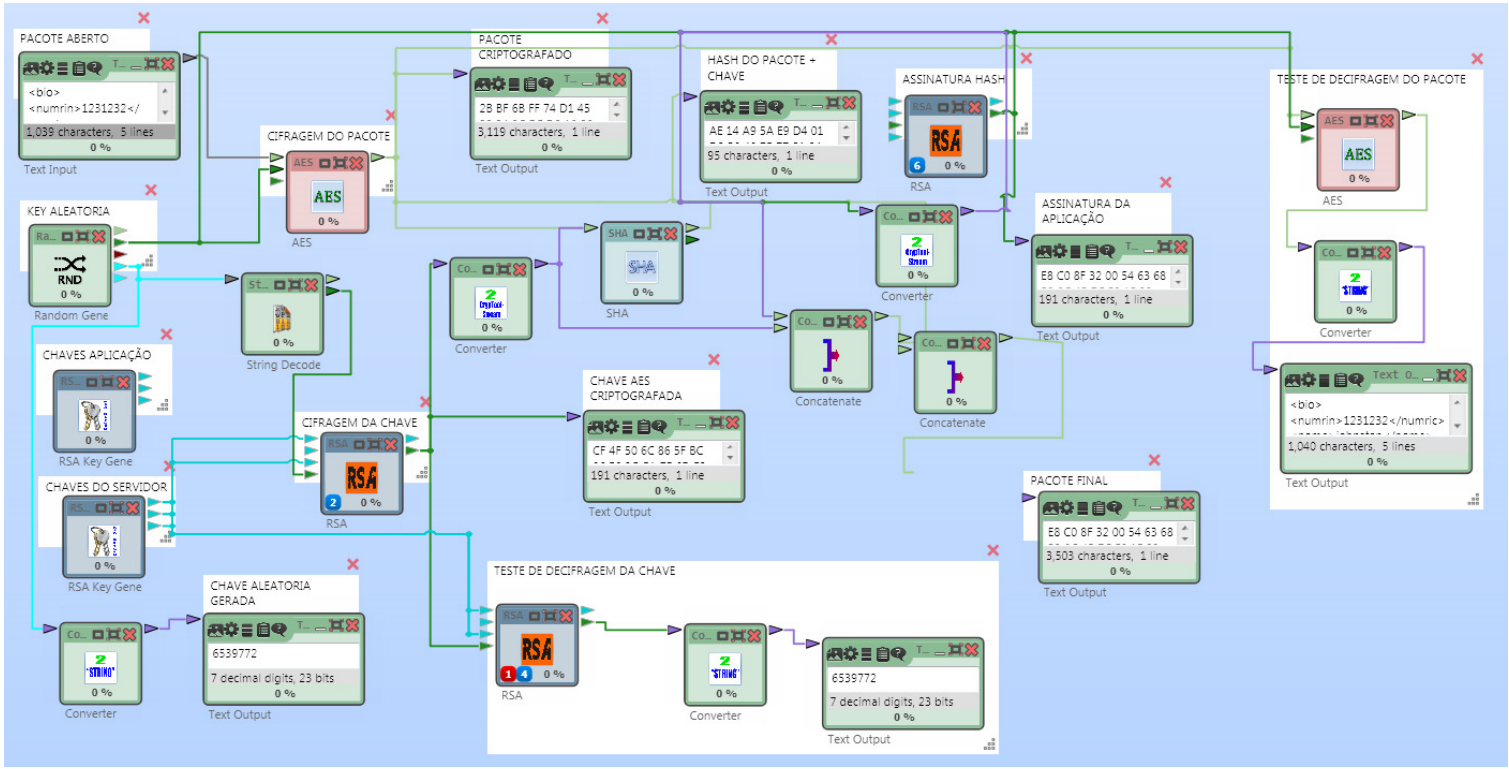

Figura 4.3.3 – Fluxo geral criado no *software Cryptool* 2 (CT2).

5 Conclusão

Este relatório técnico foi criado a partir de um trabalho coordenado e interdependente entre as equipes da MJ/SE e da Universidade de Brasília e não representa um produto final, e sim, um modelo para avaliação e sugestões sobre três importantes subáreas da Segurança da Informação: Segurança Física, Recomendações de Segurança da Informação para desenvolvimento de *softwares* e Políticas e Recomendações Técnicas e Operacionais para Protocolo de Comunicação Segura.

Sua revisão, é provável, após ciclos de análise e reavaliação e, principalmente, quanto do atendimento de requisitos parciais na realização das atividades envolvidas no subprojeto de Infraestrutura Tecnológica do Projeto RIC.

O principal objetivo deste relatório é dar suporte ao gestor para contratação das empresas que irão operacionalizar a infraestrutura tecnológica do Sistema Nacional do Registro de Identificação Civil, mais especificadamente a que envolve as atividades de Hospedagem da Infraestrutura Tecnológica do Projeto RIC, Desenvolvimento de *Softwares* e Comunicação Segura.

Ao iniciar o trabalho de pesquisa foi percebido que uma das características mais importantes, e um ponto de preocupação, é diretamente relacionado a estrutura contratual em que se baseia as regras e especificações de contratação dos serviços e o acordo entre as partes envolvidas.

Apesar de ser um assunto específico da área de prestação de serviços, as peculiaridades que englobam toda a área de atuação deste serviço são enormes. Desta forma, fica ainda mais evidente a necessidade de se iniciar por uma análise direta as características contratuais e a partir daí um desmembramento e desmistificação de termos, características, objetivos, necessidades e quaisquer outros fatores importantes envolvidos, principalmente fatores relativos a hospedagem de solução, acordos de níveis de serviço e desenvolvimento de sistemas.

A preocupação com a dissertação dos contratos, seus detalhamentos e especificidades também deve ser mantida em qualquer situação, já que foram observados diversos tipos e maneiras de pactuar estes tipos de acordos de serviços baseados em soluções tecnológicas, principalmente pela pouca abrangência da legislação brasileira.

Desta forma, como sugestão para um próximo relatório de avaliação do modelo de contratação para hospedagem da Solução RIC, que seja feito após a formalização de requisitos e objetivos específicos de funcionamento e manutenção constante da solução e que, se possível, também seja criado um modelo de avaliação baseada nos pesos de atendimento de cada requisito ou objetivo.

O processo de *software* e, consequentemente o desenvolvimento de sistemas, tem se mostrado cada vez mais importante para a organização, para os desenvolvedores e para seus usuários. Quanto mais cedo forem incorporados os controles de segurança ao processo de desenvolvimento de *software*, menores os riscos de incidentes, assegurando melhoria ao processo. Convém que este processo de integração entre segurança da informação e o desenvolvimento de *software* seja flexível.

É responsabilidade da equipe de desenvolvimento lidar com as preocupações de segurança claramente. Em geral, padrões para normalização de verificação e validação estão somente preocupados com os aspectos funcionais da operação do *software*. Questões de segurança são geralmente problemas colaterais que persistem em todas as fases do ciclo de vida do *software*, até que ele seja retirado de circulação.

Em cada fase do ciclo de desenvolvimento, deve-se considerar e implementar os requisitos funcionais de segurança, desde a fase de engenharia de requisitos, levantando junto aos usuários, às políticas de acessos aos dados do sistema. Posteriormente, deve-se passar pela fase de análise e projeto, projetando rotinas mais concisas e mais seguras. Já na fase de implementação, procurar seguir as boas práticas de desenvolvimento descritas neste documento, assim como outras existentes e que por ventura não foram pontuadas aqui.

Com uma abordagem de segurança de *software* abrangente e permanente fica mais simples planejar uma postura adequada de segurança para a aplicação. Mitigar os pontos levantados ao longo do ciclo de vida do *software,* com a ajuda de práticas e diretrizes aqui apresentadas, reduz a chance de exploração de problemas de segurança que podem ter consequências catastróficas.

Um outro fator de preocupação, o qual merece além de uma observação mais profunda, uma aplicação minuciosa, são as políticas e recomendações técnicas e operacionais em segurança da informação para o protocolo de comunicação segura da infraestrutura, comunicação e armazenamento do Sistema Nacional do Registro de

Identificação Civil.

O objetivo é fornecer meios normatizados, seguros e aplicáveis de se estabelecer mecanismos e controles para garantir a efetiva proteção dos dados e informações, bem como a redução de riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações.

As atividades envolvidas nesta etapa observaram formalmente a execução dos passos da metodologia elencada para gestão do projeto, PMI/PMBoK.

A equipe da UnB considera que teve acesso a todas as informações necessárias à boa condução dos trabalhos e que a disponibilização dessas informações pela equipe do MJ, assim como as atividades conjuntas de análise e discussão, levou a etapa do projeto a bom termo.

6 Referências

[A] Contrato de Prestação de Serviço N° 2008/8558-0569 – Serviços de Colocation Site Alternativo – entre o Banco do Brasil S.A. e o Serviço Federal de Processamento de Dados – SERPRO;

[B] Contrato padrão de Prestação de Serviços de Colocation da Global Village Telecom Ltda (GVT);

[C] Edital de Licitação (Pregão Eletrônico N° 22/2013) do Ministério do Planejamento, Orçamento e Gestão para contratação de empresa especializada para o fornecimento e instalação de solução de ambiente seguro de d*atacenter* nas dependências do Ministério.

[D] Contrato de Prestação de Serviços N. 013/2011/FERMP do Ministério Público do Estado de Santa Catarina.

[E] Processo de Compra Nº RJ-2013-9991 (Edital do Pregão Eletrônico Nº 30/2013) da Comissão de Valores Mobiliários.

[F] Minuta do Termo de Referência do documento de Planejamento de Contratação de Bens e Serviços de TI da Agência Nacional de Telecomunicações (Anatel).

[01] Kaufman, L.M., "Data Security in the World of Cloud Computing", Security & Privacy, IEEE, Volume:7 Issue:4, 2009.

[02] Machado, L. Cloud computing cresce 68% no Brasil. Disponível em: <www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=13161&sid=29>; Acesso em: 20/08/2014.

[03] Frost; Sullivan. Disponível em: <http://www.frost.com/>. Acesso em: 20/08/2014.

[04] Barros; Ricardo Dobelin. Segurança em Computação em Nuvem. Universidade Estadual de Campinas – UNICAMP.

[08] Price Of The Cloud Still Out Of Reach For Small Businesses; <http://www.forbes.com/sites/quickerbettertech/2012/01/23/price-of-the-cloud-still-out-of-reach-for-small-businesses>; Acesso em: 20/08/2014.

[10] Cloud Economics; <https://vijaygill.wordpress.com/2010/08/09/cloud-economics>; Acesso em: 20/08/2014.

[12] ROMER, Rafael; Tier: como é feita a classificação e quais as diferenças entre Data Centers?; <http://corporate.canaltech.com.br/noticia/hosting/Entenda-como-e-feita-a-classificacao-de-Data-Centers-e-como-escolher-o-melhor/>; Acesso em: 20/08/2014.

[13] VERAS, Manoel. Datacenter: Componente central da infraestrutura de TI. Rio de Janeiro: Brasport, 2009.

[14] Lautan Kencana; <http://lautankencana.com/data-center-solutions>;

[15] Data Center I: Técnicas e Práticas para a Construção de uma Instalação Segura; <http://www.teleco.com.br/tutoriais/tutorialdcseg1/pagina_2.asp>; Acesso em: 21/08/2014.

[16] Portugal Telecom. <http://www.telecom.pt/NR/rdonlyres/3855264A-959C-4642-9710-DCA9573365EE/1458346/NovoConceitodeDataCenter.pdf>; Acesso em: 21/08/2014.

[17] ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança

– Código de prática para controles de segurança da informação;

[18] ABNT NBR 15247 – Unidades de Armazenagem Segura – Salas cofres e Cofres para Hardware – Classificação e Métodos de Ensaio de Resistência ao Fogo;

[19] ABNT NBR 11515:2007 – Critérios de segurança física relativos ao armazenamento de Dados;

[20] EMERSON Network Power; <http://www.emersonnetworkpower.com/en-US/Brands/Liebert/Documents/White%20Papers/UPS%20Trap%20Doors%20for%20SMB.pdf>; Acesso em: 22/08/2014.

[21] ACECO TI; <www.acecoti.com.br>; Acesso em: 20/08/2014.

[22] Lampertz GmbH & Co.; <www.lampertz.de>; Acesso em: 20/08/2014.

[23] ANSI/BICSI 002-2011; Data Center Design and Implementation Best Practices; https://www.bicsi.org/uploadedfiles/bicsi_002_sample.pdf; Acesso em: 20/08/2014.

[24] ANSI/EIA/TIA 942 - Telecommunications Infrastructure Standard for Data Centers; <http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf>; Acesso em: 22/08/2014.

[25] ELLRAM, Lisa M; SIFERD, Sue P. Total cost of ownership: a key concept in strategic cost management decisions. Journal of business logistics, v.19, n.1, 1998, p. 55-84.

[28] Rack Cabinet Buying Guide; <http://www.tripplite.com/products/rack-buying-guide>; Acesso em: 29/08/2014.

[29] Ambiente Colocation; <http://www.digitrum.com.br/colocation>; Acesso em: 29/08/2014.

[30] HOELZLE, U., AND BARROSO, L. A. The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines. Morgan and Claypool Publishers, 2009; <http://www.cs.berkeley.edu/~rxin/db-papers/WarehouseScaleComputing.pdf>; Acesso em: 03/09/2014.

[31] RIBAS, Júlio César da Costa, Contratos de Nível de Serviço – Primeiro seminário do Projeto SLA Energia, Florianópolis, 2005.

[32] LABOUNTY, Char, "How to To Establish and Maintain Service Level Agreements", 2008. HDI Focus. Disponível em <http://www.hdibrasil.com.br/index2.php?option=com_content&do_pdf=1&id=379>. Acessado em 13/09/2014.

[33] LANZ, Luciano Quinto; LANZ, Renata. Modelos de Contratos em Projetos. 2013. PMKB – Project Management Knowledge Base. <http://pmkb.com.br>. Acessado em 13/09/2014.

[34] DUARTE, Diego. ITIL – Resumo de Acordo de Nível de Serviço (ANS) – *Service Licence Agreement* (SLA). 2013. Disponível em <http://www.purainfo.com.br/itil/itil-resumo-de-acordo-de-nivel-de-servico-ans-service-licence-agrement-sla>. Acessado em 13/09/2014.

[35] MCGRAW, G., CHESS, B., MIGUES, S. (2012) BSIMM - Buiding Security In Maturity Model, Cigital, Creative Commons.

[36] WADHWANI, S. IBM Software. How to achieve compliance with IEC 62304 for medical device software development. Disponível em: <https://www-950.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/IEC%2062304%20presentation/$file/IEC%2062304%20presentation.pdf>. Acesso em janeiro de 2015.

[40] CARDOSO et al. (2009) "Um Modelo de Controle Formal para o gerenciamento de riscos de processo em fábricas de software". Publicado em: Anais do IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais.

[41] COMPAGNA L., KHOURY P., KRAUSOVÁ A., MASSACCI F., ZANNONE N. (2008) "How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns" Publicado em: Springer Science+Business Media.

[42] MCGRAW G. Software Security: Building Security In. ISBN: 0-321-35670-5

[43] PAUL, M., (2011) Official (ISC)² Guide to the CSSLP, 1ª ed, Florida: CRC Press.

[44] GOERTZEL, K. M et al. (2007) Software Security Assurance: A State of the Art Report (SOAR), Information Assurance Technology Analysis Center (IATAC).

[45] BRINK, D. (2010) *Securing Your Applications*. [S.l.]. Disponível em: <http://midsizeinsider.com/en-us/article/securing-your-applications#.VHiF7RBgFd8>. Acesso em dezembro de 2014.

[46] ALLEN, J. H. et al. (2008) *Software Security Engineering: A Guide for Project Managers (The SEI Series in Software Engineering)*. 1. ed. [S.l.]: Addison-Wesley Professional. ISBN 032150917X, 9780321509178.

[47] FREIRE M. da S. (2014); Ferramenta de apoio a auditoria de programa de segurança de software – Brasília, DF - Universidade de Brasília – UnB; 53 p.

[48] RISPOLI, D. C. (2013). Boas práticas no ciclo de vida para melhoria da segurança de software para dispositivos médicos. Dissertação de Mestrado em Engenharia Biomédica, Publicação 010A/2013, Programa de Pós-Graduação em Engenharia Biomédica, Faculdade Gama, Universidade de Brasília, Brasília, DF, 127p.

[49] KNIGHT, J. C. (2002) Dependability of embedded systems, ICSE '02 Proceedings of the 24th International Conference on Software Engineering - ACM, pp 685-686, Nova York.

[50] WAGNER R., MACHADO A.; Níveis de segurança para processos de desenvolvimento de software seguro; Centro de Tecnologia – Universidade Federal de Santa Maria (UFSM).

[51] WAGNER R. (2011); Processos de desenvolvimento de software confiáveis baseados em padrões de segurança. 105 f; Centro de Tecnologia – Universidade Federal de Santa Maria (UFSM).

[52] BRAZ, F. (2009) Instrumentação da análise e projeto de software seguro baseada em ameaças e padrões. Tese (Doutorado em Engenharia Elétrica) - Faculdade de tecnologia, Brasília, Brasil.

[53] MCAFEE. Cybercrime cost $1 trillion last year. Disponível em:<http://news.zdnet.com/2100-9595_22-264762.html>. Acesso em dezembro de 2014.

[54] ERNST & YOUNG. (2008). Global Information Security Survey. Reino Unido, 2008. Disponível em:<http://www.ey.com/Global/assets.nsf/UK/Global_Information_Security_Survey_2008/$file/EY_Global_Information_Security_Survey_2008.pdf>. Acesso em dezembro de 2014.

[55] KHAN Muhammad U. A., Zulkernine, Mohammad. (2008) “Quantifying Security in Secure Software Development Phases” Annual IEEE International Computer Software and Applications Conference, pp. 905-960.

[56] The Ten Best Practices for Secure Software Development; (ISC)² - International Information Systems Security Certification Consortium;

[57] RAKITIN, S. R., (2006) Coping with Defective Software in Medical Devices Computer Magazine - IEEE Computer Society, v. 39, n. 4, pp. 40-45, doi: 10.1109/MC.2006.123.

[58] MCGRAW, G. (2006) Software security: building security in, Boston: Addison Wesley Professional.

[59] GORDON, Steven R.; GORDON, Judith R. (2006) Sistemas de informação: uma abordagem gerencial. 3. ed. Rio de Janeiro: LTC.

[60] HOWARD M.; Uma análise do ciclo de vida do desenvolvimento da segurança na Microsoft; Disponível em: <http://www.microsoft.com/brasil/msdn/Tecnologias/Seguranca/SDLdefault_US.mspx>. Acesso em janeiro de 2015.

[61] KROLL, J.; ORNELLAS, M.; FONTOURA, L.; Desenvolvimento de Sistemas de Gestão da Segurança da Informação através da Integração das Normas ISO/IEC 27001:2006 E ISO/IEC 21827 (SSE-CMM); Universidade Federal de Santa Maria (UFSM);

[62] FENZ, Stefan; GOLUCH, Gernot; EKELHART, Andreas; RIEDL, Bernhard; WEIPPL, Edgar, (2007). Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. 13th IEEE International Symposium on Pacific Rim Dependable Computing;

[63] KAJAVA, Jorma; ANTTILA, Juhani; VARONEN, Rauno; SAVOLA, Reijo; RONING, Juha, (2006). Information Security Standards and Global Business. Industrial Technology, 2006. ICIT 2006. IEEE International Conference;

[64] WAGNER, R.; FONTOURA, L.; Metodologia para a Adaptação de Processos de Software baseada no Modelo SSE-CMM; Universidade Federal de Santa Maria (UFSM);

[65] BATISTA, Carlos F. A., (2007). Métricas de Segurança de Software. Dissertação do Programa de Pós-graduação em Informática do Departamento de Informática da PUC-Rio. Universidade Pontifícia Católica, Rio de Janeiro.

[66] KHAN, Muhammad U. A., Zulkernine, Mohammad, (2009). “Activity and Artifact Views of a Secure Software Development Process”. International Conference on Computational Science and Engineering, pp. 339- 404.

[67] SANTOS, Marcelo A. dos. ISO 15.408 e Ciência da Informação. Disponível em:

<https://eciti.wordpress.com/2012/07/02/iso-15-408-e-ciencia-da-informacao/>. Acesso em janeiro de 2015.

[68] INTERNATIONAL ORGANISATION FOR STANDARDISATION, (1998). ISO/IEC TR 13335-n, Guidelines for the Management of IT Security (GMITS). International Organization for Standardization, Switzerland.

[69] SIEWERT, Vanderson C., Resumo da Norma ISO/IEC 13335-3. Disponível em: http://dpsti.blogspot.com.br/2009/10/resumo-da-norma-isoiec-13335-3.html. Acesso em janeiro de 2015.

[70] SCHUMACHER M, et al. Security Patterns. J.Wiley & Sons, 2006.

[71] ROSADO D. et al, (2006). A Study of Security Architectural Patterns. In: Proceedings of the First International Conference on Availability, Reliability and Security, Washington, USA.

[72] ROMANOSKY, S. (2002) Security design patterns, In: SecurityFocus. Disponível em <http://www.securityfocus.com/guest/9793> acesso em janeiro de 2015.

[73] TROWBRICGE D., (2003) Enterprise Solution Patterns Using Microsoft .NET, Microsoft Corporation.

[74] KIENZLE, Darrell M. et al. (2002) Security patterns repository version 1.0. DARPA, Washington DC.

[75] CAVALCANTI C. (2013). Security Quality Requirements Engennering (SQUARE). Disponível em: < http://carloscavalcanti.com/2013/06/security-quality-requirements-engineering-square/>. Acesso em janeiro de 2015.

[76] SEI. (2010) CMMI for Development Version 1.3, Technical Report, Carnegie Mellon University, Pittsburgh.

[77] OWASP. Software Assurance Maturity Model – A guide to building security into software development. Disponível em: < http://www.opensamm.org/downloads/SAMM-1.0.pdf> acesso em janeiro de 2015.

[78] Symantec Report on Attack Toolkits and Malicious Websites. Disponível em: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf>. Acesso em janeiro de 2015.

[79] OWASP – OWASP Top 10 (2013). Os dez riscos de segurança mais críticos em aplicações web.

[80] Referências seções 3.8 e 3.9:

- Termo de Referência: Ministério da Saúde. Aquisição de Solução de Informação Hospitalar Integrada ao Sistema de Registro Eletrônico de Saúde para Atenção Integral (RES-AI) com implantação nos seis Hospitais Federais do Rio de Janeiro (2009).

- Pregão Eletrônico – Registro de Preço: IBAMA. Contratação de empresa para a prestação de serviços técnicos especializados na área de tecnologia da informação, em desenvolvimento de novos sistemas e manutenção dos sistemas de informação do Ibama, no modelo de fábrica de software (2011).

- Termo de Referência: Empresa de Tecnologia da Informação e Comunicação do Mun. SP – PRODAM/SP. Fábrica de Software Código e Testes: serviços referentes à codificação e testes de sistemas de informação e/ou manutenções em sistemas legados.

- Termo de Referência: Secretaria da Fazenda do Estado do Rio de Janeiro – SEFAZ/RJ. Aquisição de uma Solução Integrada de Acompanhamento Orçamentário e Financeiro, denominada Aplicativo de Mercado.

- Termo de Referência: Agência Nacional do Petróleo – ANP. Contratação de Serviços Técnicos Especializados de Segurança da Informação na ANP (2008).

- Pregão Eletrônico: Ministério da Educação. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP. Prestação de serviços técnicos de Tecnologia da Informação, compreendendo o desenvolvimento e manutenção de sistemas de informação em regime de fábrica de software (2010).

- Termo de Referência: Ministério do Desenvolvimento, Indústria e Comércio Exterior. Contratação de serviços técnicos de desenvolvimento/manutenção de sistemas de informação (2011).

- NBR ISO/IEC 17799, 2005. Tecnologia da Informação. Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro.

- NBR ISO/IEC 27001, 2006. Tecnologia da Informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Associação Brasileira de Normas. Rio de Janeiro.

[81] RFC (*Request for Comments*) 3447. *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography - Specifications Version 2.1*. *The Internet Engineering Task Force (IETF).* Disponível em <http://tools.ietf.org/html/rfc3447>. Acesso em Dezembro/2014.

[82] Instituto Nacional de Tecnologia da Informação. Disponível em <http://www.iti.gov.br>. Acesso em Dezembro/2014.

[83] Instrução Normativa N° 1 de 04 de Junho de 2014. REGULAMENTA A CRIPTOGRAFIA DE CURVAS ELÍPTICAS BRAINPOOL PARA GERAÇÃO DE CHAVES ASSIMÉTRICAS NO ÂMBITO DA ICP-BRASIL (DOC-ICP-01.01). Disponível em <http://www.iti.gov.br/images/icp-brasil/legislacao/Instrucao/IN_2014-01_REGULAMENTA_CURVA_EL%C3%8DPTICA_BRAINPOOL_NO_DOC-ICP-01.01.pdf>. Acesso em Dezembro/2014.

[84] Diário Oficial da União Seção 1. ISSN 1677-7042. REGULAMENTA A CRIPTOGRAFIA DE CURVAS ELÍPTICAS BRAINPOOL PARA GERAÇÃO DE CHAVES ASSIMÉTRICAS NO ÂMBITO DA ICP-BRASIL (DOC-ICP-01.01). Disponível em < http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=4&data=06/06/2014>. Acesso em Dezembro/2014.

[85] Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Disponível em <http://www.iti.gov.br/icp-brasil>. Acesso em Dezembro/2014.

[86] *Federal Information Processing Standards Publication* (FIPS) 186-4. *National Institute of Standards and Technology*. Disponível em < http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>. Acesso em Dezembro/2014.

[87] *National Institute of Standards and Technology* (NIST). Disponível em <http://www.nist.gov>. Acesso em Dezembro/2014.

[88] FIPS 180-4. *Secure Hash Standard* (SHS). *National Institute of Standards and Technology*. Disponível em <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>. Acesso em Dezembro/2014.

[89] RFC 6234. *US Secure Hash Algorithms* (*SHA and SHA-based HMAC and HKDF*). *The Internet Engineering Task Force* (IETF). Disponível em <https://tools.ietf.org/html/rfc6234>. Acesso em Dezembro/2014.

[90] RESOLUÇÃO Nº 68. ALTERA OS PRAZOS ESPECIFICADOS NO PLANO DE ADOÇÃO DE NOVOS PADRÕES CRIPTOGRÁFICOS ANEXO II DA RESOLUÇÃO Nº 65, PUBLICADA EM 09 DE JUNHO DE 2009. Disponível em <http://www.iti.gov.br/images/icp-brasil/legislacao/Resolucoes/Resolucao_68.pdf>. Acesso em Dezembro/2014.

[91] RESOLUÇÃO Nº 65. APROVA A VERSÃO 2.0 DO DOCUMENTO PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL, E O PLANO DE MIGRAÇÃO

RELACIONADO. Disponível em <http://www.iti.gov.br/images/icp-brasil/legislacao/Resolucoes/resolucao65.pdf>. Acesso em Dezembro/2014.

[92] Decreto Nº 8.135 [12], de 4 de Novembro de 2013. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8135.htm>. Acesso em Janeiro/2014.

[93] Portaria SLTI/MP nº 92, de 24 de dezembro de 2014. Disponível em <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=50&data=26/12/2014>. Acesso em Janeiro/2014.

[94] Padrões de Interoperabilidade de Governo Eletrônico – ePING Disponível em <http://eping.governoeletronico.gov.br>. Acesso em Janeiro/2014.

[95] FIPS 197 – *Advanced Encryption Standard* (AES). *National Institute of Standards and Technology*. Disponível em <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>. Acesso em Janeiro/2014.

[96] FIPS 46-3 – *Data Encryption Standard* (DES). *National Institute of Standards and Technology*. Disponível em <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>. Acesso em Janeiro/2014.

[97] *Multipurpose Internet Mail Extensions* (MIME) *Part One: Format of Internet Message Bodies - 6.8. Base64 Content-Transfer-Encoding*. Disponível em <https://tools.ietf.org/html/rfc2045#page-24>. Acesso em Janeiro/2014.

[98] RFC 2459 - *Internet X.509 Public Key Infrastructure - Certificate and CRL Profile. The Internet Engineering Task Force (IETF).* Disponível em <https://www.ietf.org/rfc/rfc2459>. Acesso em Janeiro/2014.

[99] Instrução Normativa Nº 05, de 29 de abril de 2009. Instituto Nacional de Tecnologia da Informação - ITI. Disponível em <www.iti.gov.br/images/icp-

brasil/legislacao/Instrucao/IN_2009-05.pdf>. Acesso em Janeiro/2014.

[100] DOC-ICP-11 – versão 1.2. Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil. Disponível em <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-11_-_Versao_1.2.pdf>. Acesso em Janeiro/2014.

[101] DOC-ICP-12 - versão 1.1. Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil. Disponível em <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-12.pdf>. Acesso em Janeiro/2014.

[102] DOC-ICP-13. Requisitos Mínimos Para as Políticas de Carimbo do Tempo da ICP-Brasil. Disponível em <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-13.pdf>. Acesso em Janeiro/2014.

[103] DOC-ICP-14 (Procedimentos para Auditoria do Tempo na ICP-BRASIL). Disponível em <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-14.pdf>. Acesso em Janeiro/2014.

[104] RFC 3628 – *Policy Requirements for Time-Stamping Authorities* (TSAs). *The Internet Engineering Task Force (IETF).* Disponível em <https://www.ietf.org/rfc/rfc3628.txt>. Acesso em Janeiro/2014.

[105] RFC 5246 – *The Transport Layer Security (TLS) Protocol - Version 1.2*. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc5246>. Acesso em Janeiro/2014.

[105a] *HMAC and the Pseudorandom Function* - RFC 5246 – *The Transport Layer Security (TLS) Protocol - Version* 1.2. *The Internet Engineering Task Force (IETF).* Disponível em <http://tools.ietf.org/html/rfc5246#page-14>. Acesso em Janeiro/2014.

[105b] SSL and TLS - *An Overview of A Secure Communications Protocol*. Simon Horman aka Horms. *The Internet Engineering Task Force (IETF).* Disponível em <http://horms.net/projects/ssl_and_tls/stuff/ssl_and_tls.pdf>. Acesso em Janeiro/2014.

[106] RFC 5746. TLS - *Renegotiation Indication Extension. The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc5246>. Acesso em Janeiro/2014.

[107] RFC 5878. TLS - *Authorization Extensions*. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc5246>. Acesso em Janeiro/2014.

[108] RFC 6176. *Prohibiting Secure Sockets Layer* (SSL) *Version* 2.0. Disponível em <https://tools.ietf.org/html/rfc5246>. Acesso em Janeiro/2014.

[109] RFC 4303. *IP Encapsulating Security Payload* – ESP. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc4303>. Acesso em Janeiro/2014.

[110] RFC 4835. *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload* (ESP) *and Authentication Header* (AH). *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc4835>. Acesso em Janeiro/2014.

[111] RFC 4306. *Internet Key Exchange* (IKEv2) *Protocol*. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc4306>. Acesso em Janeiro/2014.

[112] RFC 2460. *Internet Protocol, Version* 6 (IPv6) *Specification*. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc2460>. Acesso em Janeiro/2014.

[113] RFC 5095. *Deprecation of Type 0 Routing Headers in* IPv6. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc5095>. Acesso em Janeiro/2014.

[114] RFC 5722. *Handling of Overlapping IPv6 Fragments*. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc5722>. Acesso em Janeiro/2014.

[115] RFC 5871. *IANA Allocation Guidelines for the IPv6 Routing Header*. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc5871>. Acesso em Janeiro/2014.

[116] RFC 4302. *IP Authentication Header*. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc4302>. Acesso em Janeiro/2014.

[117] *IP Spoofing: An Introduction.* Disponível em <http://www.symantec.com/connect/articles/ip-spoofing-introduction>. Acesso em Janeiro/2014.

[118] *Distributed Denial-of-Service Attack* (DDoS). Disponível em <http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack>. Acesso em Janeiro/2014.

[119] RFC 2827. Ne*twork Ingress Filtering: Defeating Denial of Service Attacks which employ - IP Source Address Spoofing*. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc2827>. Acesso em Janeiro/2014.

[120] RFC 3704. *Ingress Filtering for Multihomed Networks*. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc3704>. Acesso em Janeiro/2014.

[121] SSH *File Transfer Protocol* Draft 13 - draft-ietf-secsh-filexfer-13.txt. Disponível em <http://tools.ietf.org/html/draft-ietf-secsh-filexfer-13>. Acesso em Janeiro/2014.

[122] RFC 4217. *Securing* FTP *with* TLS. *The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc4217>. Acesso em Janeiro/2014.

[123] RFC 4880. *OpenPGP Message Format Item 2.1 - Confidentiality via Encryption*; *The*

Internet Engineering Task Force (IETF). Disponível em <http://tools.ietf.org/html/rfc4880#section-2.1>. Acesso em Janeiro/2014.

[124] *Federal Information Processing Standards Publication* 140-2 - *Security Requirements for Cryptographic Modules - Cryptographic Key Management*. Disponível em <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>. Acesso em Janeiro/2014.

[125] RFC 4086. *Randomness Requirements for Security. The Internet Engineering Task Force (IETF).* Disponível em <http://tools.ietf.org/html/rfc4086>. Acesso em Janeiro/2014.

[126] Simple Object Access Protocol – SOAP. Disponível em <http://www.w3.org/TR/soap>. Acesso em Janeiro/2014.

[127] Web Services Security (WS-Security): SOAP Message Security Version 1.1.1. Disponível em <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.pdf>. Acesso em Janeiro/2014.

[128] Organization for the Advancement of Structured Information Standards - OASIS. Disponível em <https://www.oasis-open.org>. Acesso em Janeiro/2014.

[129] About CrypTool 2. Disponível em <https://www.cryptool.org/en/cryptool2-en>. Acesso em Janeiro/2014.

[130] What is open source?. Disponível em <http://opensource.com/resources/what-open-source>. Acesso em Janeiro/2014.

[131] RFC 4880. *OpenPGP Message Format Item 2.2 - Authentication via Digital Signature; The Internet Engineering Task Force (IETF).* Disponível em <https://tools.ietf.org/html/rfc4880#section-2.2>. Acesso em Janeiro/2014.

[132] RFC 2660; *The Secure HyperText Transfer Protocol*. Disponível em <https://tools.ietf.org/html/rfc2660>. Acesso em Janeiro/2014.

[133] RFC 2818; *HTTP Over TLS*. Disponível em <https://tools.ietf.org/html/rfc2818>. Acesso em Janeiro/2014.

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br – www.cdt.unb.br – www.latitude.eng.br