Pós-Graduação em Ciência da Computação

MILTON VINICIUS MORAIS DE LIMA

UMA METODOLOGIA PARA AVALIAR A MATURIDADE DAS CONFIGURAÇÕES DE SEGURANÇA EM AMBIENTES DE DATA CENTER: UMA ESTRUTURA SISTEMÁTICA COM MULTIPERSPECTIVA

Universidade Federal de Pernambuco
posgraduacao@cin.ufpe.br
www.cin.ufpe.br/~posgraduacao

RECIFE
2017

Milton Vinicius Morais de Lima

Uma Metodologia para Avaliar a Maturidade das Configurações de Segurança em Ambientes de Data Center: Uma Estrutura Sistemática com Multiperspectiva

Este trabalho foi apresentado à Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Ciência da Computação.

ORIENTADOR: **Prof. Dr Ricardo Massa Ferreira Lima**
CO-ORIENTADOR: **Prof. Dr Fernando Antônio Aires Lins**

RECIFE
2017

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

L732m Lima, Milton Vinicius Morais de
Uma metodologia para avaliar a maturidade das configurações de segurança em ambientes de data center: uma estrutura sistemática com multiperspectiva / Milton Vinicius Morais de Lima. – 2017.
134 f.:il., fig., tab.

Orientador: Ricardo Massa Ferreira Lima.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2017.
Inclui referências e apêndices.

1. Segurança da informação. 2. Métricas de segurança. I. Lima, Ricardo Massa Ferreira (orientador). II. Título.

005.8 CDD (23. ed.) UFPE- MEI 2017-175

Milton Vinicius Morais de Lima

Uma Metodologia para Avaliar a Maturidade das Configurações de Segurança em Ambientes de Data Center: Uma Estrutura Sistemática com Multiperspectiva

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Aprovado em: 20/07/2017

BANCA EXAMINADORA

_____

Prof. Dr. Nelson Souto Rosa
Centro de Informática / UFPE

_____

Prof. Dr. Fernando Ferreira de Carvalho
Instituto Federal de Pernambuco – Campus Recife

_____

Prof. Dr. Ricardo Massa Ferreira Lima
Centro de Informática / UFPE
(**Orientador**)

Dedico este trabalho a minha mãe Vera Lúcia Morais de Lima (IN MEMORIAN)

Agradecimentos

Primeiramente agradeço a Deus e a seu filho Jesus Cristo pelo amor infinito.

A minha avó **Amara Maria,** meus pais **Milton Vasconcelos** e **Vera Lúcia (*IN MEMORIAN*)** e meus familiares.

Ao Dr. **Ricardo Massa Ferreira Lima** (por me estender a mão) e ao Dr. **Fernando Antônio Aires Lins** (por me ensinar a "vender o peixe")**,** vocês são muito mais que orientadores.

A minha rainha e companheira de todos os momentos **Mônica Moreira Vieira.**

Aos demais docentes do programa de Pós-Graduação do Centro de Informática da UFPE pela competência com que transmitiram os conteúdos e ensinamentos.

Agradeço a todos os amigos que tive a oportunidade de conhecer no Centro de Informática, que por muitas vezes me ajudaram durante todo o meu mestrado, pois sem as trocas de ideias esta pesquisa não seria possível.

A todos os meus amigos que de alguma forma contribuíram e participaram na realização deste trabalho.

Ao CAPES e ao CIn – UFPE pelo apoio financeiro para realização desta pesquisa.

A todos, os meus mais sinceros agradecimentos.

“Mas Deus escolheu as coisas loucas deste mundo para confundir as sábias; e Deus escolheu as coisas fracas deste mundo para confundir as fortes”;

1 Corintios 1:27

Resumo

As ameaças à segurança da informação podem ter um grande impacto nas finanças e na reputação da empresa. As metodologias tradicionais para avaliar a maturidade dos *data centers* investigam os parâmetros de segurança para determinar a conformidade dos *data centers* e as normas internacionais de segurança. Este trabalho propõe dois procedimentos de avaliação para capturar outras perspectivas de segurança em ambientes de *data centers*: (1) análise ponderada – pondera os controles de segurança, simultaneamente presentes em um número maior de normas; (2) análise contextual - é sensível ao nível de importância que a organização atribui a cada controle de segurança. Através da metodologia proposta, os engenheiros de segurança podem identificar problemas de segurança, caracterizar a maturidade da segurança e sugerir novas políticas para melhorar as configurações de segurança dos *data centers*. Este trabalho também inclui um estudo de caso para avaliar os benefícios da metodologia em cenários do mundo real. Os resultados demonstraram que a metodologia proposta avalia os elementos de segurança mais relevantes para a empresa, onde as abordagens tradicionais consideram todos os aspectos de segurança como igualmente importantes.

Palavras-chave: *Data Center*. Segurança da Informação. Avaliação da Maturidade. Métricas de Segurança. ISO/IEC 27002. NIST SP 800-53.

Abstract

Threats to information security can have great impact on business finances and company's reputation. Traditional methodologies for evaluating the maturity of data centers investigate security parameters to determine the compliance of data centers and international security norms. This work proposes two innovative evaluation procedures to capture other security perspectives on data center environments: (1) weighted analysis - it weights higher security controls simultaneously present in a higher number of norms; (2) contextual analysis - it is sensitive to the importance level that the organization assigns to each security control. Through the proposed methodology, security engineers can identify security issues, characterize the security maturity, and suggest new policies improve security configurations of data centers. This work also includes a case study to evaluate the benefits of the methodology in real-world scenarios. Results demonstrated that the proposed methodology evaluates higher the security elements more relevant for the company, where as traditional approaches consider all security aspects to be equally important.

Keywords: Data Center. Security Information. Maturity Evaluation. Security Metrics. ISO/IEC 27002. NIST 800-53.

Lista de Figuras

Lista de Quadros

Lista de Tabelas

Lista de Abreviações

ISO - *International Organization for Standardization*

IEC - *International Electrotechnical Commission*

NIST - *National Institute of Standards and Technology*

DoS – *Denial of Service*

DDoS - *Distributed Denial of Service*

COBIT - *Control Objectives for Information and related Technology*

CMM - *Capability Maturity Model*

SEI - *Software Engineering Institute*

SBC - *Server Business Compliance*

SOS - *Server Operating System Security*

SAS - *Server Application Security*

SSP - *Server Security Preserving*

HP - *Hewlett-Packard*

AD – *Active Directory*

Sumário

1. INTRODUÇÃO

Este capítulo relata as principais motivações para realização deste trabalho, como também lista os objetivos de pesquisa almejados e, finalmente, mostra como está estruturado o restante da presente dissertação.

1.1 Contexto

O cenário atual no campo da tecnologia da informação mostra que os riscos de incidentes de segurança são inaceitavelmente altos, e a principal razão para isso está relacionada ao fato de que os investimentos das empresas em tecnologia de segurança ainda são modestos (NIEKERK; JACOBS, 2015). Além disso, há um grande número de especialistas em segurança, mas o uso de dispositivos de segurança, leis e regulamentos ainda são ineficientes para proteger dados corporativos (CHATZIPOULIDIS; MAVRIDIS, 2010).

De acordo com NIEKERK e JACOBS (2015) as organizações gastaram em 2013 uma média de US$ 17 milhões em produtos de software nas operações de seus *data centers*). A necessidade de configuração e monitoramento contínuo de vários softwares, sistemas operacionais e aplicativos, torna a gestão uma tarefa desafiadora (MONTESINO; FENZ, 2011).

Os *data centers* nas organizações evoluíram consideravelmente nos últimos anos. Os mesmos passaram de um modelo que colocou vários *data centers* mais perto dos usuários para um modelo dinâmico mais centralizado. Os fatores que influenciam essa evolução são variados, mas podem ser atribuídos principalmente à regulamentação, melhoria do nível de serviço, economia de custos e capacidade de gerenciamento. À medida que o custo para operar *data centers* aumentou, as arquiteturas se adequaram para a consolidação de servidores e aplicativos, a fim de melhor utilizar os recursos e reduzir a expansão de servidores. Quanto mais diversificado e distribuído o ambiente do *data center*, mais complexo será gerenciá-lo (LEWIS; FRIEDMAN, 2011).

Analisando o contexto acima, entende-se que as empresas dependem cada vez mais de seus *data centers*. *Data centers* controlam quase todas as áreas operacionais nas oganizações. Por meio deles transitam inúmeros dados que viabilizam a continuidade do negócio. Com o passar do tempo, os *data centers vêm* se tornando cada vez mais complexos, exigindo várias soluções de modo integrado, exigindo um alto grau de confiabilidade para garantir a continuidade das operações, que dependem de seu perfeito funcionamento (FULLER et al., 2013).

Tratando-se de *data center*, falhas podem gerar um custo alto para as organizações, podendo assim levar a paralisia de seus serviços, trazendo grandes prejuízos financeiros ou em sua reputação. Prejuízos citados anteriormente são possivelmente maiores que os custos de investimentos na segurança do *data center*. Diante disto, as organizações enfrentam muitos desafios à medida que trabalham para ampliar sua capacidade de processamento de informações e acompanhar a demanda (CISCO SYSTEMS, 2014). Entretanto, nem todas as organizações tem um *data center* maduro em suas configurações de segurança. Uma organização madura realiza as atividades de forma sistemática e as imaturas alcançam seus resultados graças aos esforços heróicos dos indivíduos, usando abordagens que eles criam espontaneamente (WOODHOUSE, 2008).

1.2 Motivação

A crescente dependência de computadores em rede para ajudar a gerir negócios e manter o controle de informações pessoais, além da informatização de indústrias inteiras torna necessário que a formação da rede de computadores sigam as melhores recomendações de práticas de segurança. As empresas têm solicitado o conhecimento e as habilidades dos especialistas em segurança para auditar sistemas adequadamente e adaptar soluções para atender às necessidades operacionais da organização (FULLER et al., 2013).

A dinâmica atual das organizações, com funcionários e clientes acessando recursos de TI localmente ou remotamente, eleva a prioridade em se manter ambientes computacionais seguros. Infelizmente, em parte das organizações, os processo de segurança são negligenciados em favor da produtividade e preocupações orçamentárias. Desta forma, a implementação da segurança adequada ocorre muitas vezes depois de um evento de intrusão, falha ou omissão (FULLER et al., 2013).

Várias empresas deveriam começar a perceber que a gestão da segurança da informação é uma disciplina (CHATZIPOULIDIS; MAVRIDIS, 2010). A gestão de segurança pode apoiar os *data centers*, contra constantes ataques e eventos de segurança que não têm uma orientação metodológica, tornando todo o processo de segurança vulnerável a erros e omissões (TAUBENBERGER; JÜRJENS, 2008) (LI, 2014), (SPIESS et al., 2014).

Hackers cada vez mais têm focado nos *data centers*, roubando informações relevantes das organizações. Estudos segundo realizados pelo instituto Ponemon, demonstram que invasões a *data centers geraram* 34% de inatividade no ano de 2013, 19% a mais se comparado ao ano de 2010. D'avila (2014), apontou que muitas das ações contra *data centers* são devidas a banda larga de alto nível que é utilizada.

Segundo a Convergência Digital (2015), os *data centers* foram alvos de ataques de grande impactos:

> Mais de um terço dos operadores de data center passou por ataques DDoS que esgotaram sua largura de banda de Internet. Isso demonstra a importância desse problema para operadores de data center: o tempo de inatividade não resulta apenas em perda de negócios para o operador de data center, mas em danos que se estendem aos seus clientes que têm na nuvem infraestrutura crítica para seus negócios.
> A despesa operacional é o maior custo que os operadores de *data center* atribuem aos eventos DDoS. A perda de receita devido a ataques DDoS cresce cada vez mais: 44% dos entrevistados do setor de data center enfrentaram perdas de receita devido a ataques DDoS. Pouco menos da metade dos entrevistados relata que seus firewalls enfrentaram ou contribuíram para interrupção devido a ataques DDoS, contra 42% no relatório anterior. Também houveram problemas com os balanceadores de carga, que registraram falhas devido a ataque DDoS.

Em 2016, devido a ataques contra *data centers*, mais de um terço das organizações obtiveram perdas substanciais de clientes, oportunidades e receitas de mais de 20% (RELEASE, 2017). Noventa por cento dessas organizações estão tentando melhorar suas tecnologias e processos de defesa após esses ataques. Formas de melhorar a TI partiram de segregação de funções, treinamentos, conscientização de segurança e implementação de técnicas. No relatório da Release (2017) cerca de três mil chefes de segurança e lideres de operações de segurança de treze países. Este relatório destaca grandes desafios para equipes de segurança que defedem seus *data centers* dos cibercriminosos. Entre um dos principais problemas está à falta de profissionais especializados diante de ambientes tão complexos. É fundamental que nas organizações seja medida a eficácia das práticas de segurança em face de tantos ataques (RELEASE, 2017).

Diante dessas informações, proteger data centers torna-se um grande desafio nas organizações. Definir objetivos de segurança do *data center*, alcançá-los, mantê-los e melhorar os controles que os apoiam, podem garantir a competitividade, rentabilidade, conformidade dos requisitos legais e manutenção da imagem da organização na sociedade. Acredita-se que modelos de maturidade possam ajudar a alcançar esses objetivos (WOODHOUSE, 2008). Portanto, a proposta de uma metodologia que avalie a maturidade das configurações do *data center* poderá fornecer uma indicação do estado atual do data center de uma organização e orientá-los através das ações que serão definidas, implementadas e melhoradas.

Infelizmente, a maior parte da literatura sobre análise de segurança se limita a sugestões de métricas de segurança. Um número reduzido de trabalhos ataca o problema para avaliar métricas de segurança numa perspectiva prática (MIANI; ZARPELÃO; MENDES, 2014).

1.3 Objetivo Geral

O objetivo geral desta dissertação é propor uma metodologia para avaliar a maturidade das configurações de segurança de servidores em ambiente de *data center*. Essa metodologia apresentará um conjunto de atividades para definir em qual nível de maturidade estão as configurações de segurança do *data center*, envolvendo aspectos técnicos, organizacionais e humanos.

1.4 Objetivos Específicos

Os objetivos específicos desta metodologia são:

- Realizar análise de segurança das configurações baseada em um conjunto de controles de segurança que foram extraídas das normas NIST SP 800-53 e ISO/IEC 27002;
- Avaliar e classificar o nível de maturidade das organizações utilizando três abordagens de avaliação;
- Apresentar resultados apresentando relatórios quantitativos;
- Apresentar programas de melhorias apontando áreas relevantes para melhorar o estado atual da segurança e um guia de suporte para que a equipe de segurança tome decisões futuras; e
- Promover a extração/cruzamento dos controles de segurança das normas de segurança ISO 27002 e NIST 800-53 para atender os necessidades das configurações de segurança no ambiente de *data center*.

1.5 Estrutura da Dissertação

O restante da dissertação está estruturado da seguinte maneira:

- **Capítulo 2 – Fundamentos:** Este capítulo introduz os conceitos fundamentais a serem utilizados nesta dissertação, tais como: segurança de *data center*, normas de segurança e modelos de maturidade.
- **Capítulo 3 – Avaliando e Melhorando o Estado de Segurança do Ambiente do *Data Center*:** Este capítulo descreve cada conceito e atividade para a utilização da metodologia e geração dos resultados.
- **Capítulo 4 – Avaliações:** Este capítulo apresenta dois estudos de caso no qual foi aplicada a metodologia.

- **Capítulo 5 – Trabalhos Relacionados:** Este capítulo apresenta os trabalhos relacionados referentes a modelos de maturidade de segurança que contribuíram para o desenvolvimento desta dissertação.
- **Capítulo 6 – Conclusões e Trabalhos Futuros:** Este capítulo compreende as considerações finais sobre o desenvolvimento do trabalho, a avaliação e a contribuição da metodologia para as organizações

2. Fundamentação Teórica

Este capítulo apresenta os principais conceitos utilizados neste trabalho. Inicialmente, são abordados conceitos sobre *data centers* e sua segurança. Em seguida, os conceitos de normas de segurança da informação utilizadas neste trabalho são apresentados. Por fim, são abordados modelos de maturidade de processos.

2.1. Visão Geral sobre *Data Center*

Um *data center* pode ser definido como um departamento dentro da organizações que além de abrigar, mantém sistemas, servidores, *mainframe* e bancos de dados. Anteriormente os sistemas eram lojados de forma centralizada. O objetivo de um *data center* é fornecer conexões centralizadas, utilizando poderosos recursos de computação para implatanção de variados serviços. Cada vez mais as organizações estão implantando suas aplicações em *data centers* por causa da confiabilidade, disponibilidade e baixo custo. (LI, 2014) (NIEKERK; JACOBS, 2015).

Data centers dentro das organizações podem fornecer uma variedade de serviços, tanto para acesso local ou remoto. Muitos servidores podem armazenar ou processar informações confidenciais. Normalmente em *data centers* é mais fácil encontrar servidores de serviços web, de banco de dados e de arquivos, porém outros servidores como de e-mail, virtualização podem ser encontrados nas organizações (SCARFONE; JANSEN; TRACY, 2008).

Data centers possuem algumas características essenciais (LI, 2014) que serão descritas a seguir:

- **Acesso sob demanda** – Os usuários especificam os requisitos (número de CPU´s necessárias e o armazenamento) que são automaticamente fornecidos pelo *data center*;
- **Serviço medido** - Os requisitos de serviço indicados devem ser mensuráveis para que os consumidores possam ser cobrados pelo uso de recursos.
- **Acesso à rede** - Um portal ou plataforma deve ser fornecido aos usuários para que eles possam enviar e gerenciar seus trabalhos.
- **Agrupamento de Recursos** - Os recursos no *data center* podem ser compartilhados por consumidores com acordos de nível de serviço (ACL´s) diferentes.
- **Virtualização** - A topologia do *data center* não deve importar ao usuário. As aplicações são facilmente migradas entre plataformas de hardware à medida que as demandas e as alterações de uso ocorrem. Isso acontece automaticamente.

- **Confiabilidade** - Existem múltiplas cópias redundantes de conteúdo armazenado.
- **Manutenção** - Esta é tratada por uma equipe de TI profissional e dedicada.

Desta forma, fica claro que devido ao grande número de características os seguintes elementos lógicos precisam de proteção: uso adequado de protocolos de comunicação, quais serviços/aplicações serão utilizados. Além disso, elementos físicos também precisam de proteção: rede, acesso físico e os componentes físicos (NIEKERK; JACOBS, 2015).

2.2. Segurança em *Data Center*

Esta seção aborda conceitos fundamentais sobre segurança de *data center*, que são divididos entre segurança física e segurança lógica.

Como foi apresentado anteriormente, todas as informações valiosas de quase todas as organizações podem estar armazenadas em *data centers.* Desta forma é imprescindível que os dados e servidores sejam protegidos de pessoas com intenção maliciosa. Impedir acesso não autorizado é extremamente importante (JAYASWAL, 2006)(GREENBERG et al., 2009)(SHIEH et al., 2011). A segurança lógica de *data center* precisa ter o objetivo de dificultar qualquer intruso de conseguir acesso não autorizado. Porém esta segurança não está relacionada apenas aos servidores, mas também a outros *hosts* de acesso, como por exemplo terminais que têm acesso remoto ao servidor. Além disso, outras medidas são recomendadas:

- Desabilitação de serviços desnecessários que utilizem portas de comunicação (menos de 1024);
- Construir mais de uma camada de autenticação, e permitir que apenas alguns usuários tenham acessos a essas camadas;
- Os usuários devem se autenticar num servidor de *login* central, e assim esta máquina estará com acesso direto aos consoles da rede.

Como foi apresentado nessa seção, alguns pontos são essenciais na segurança lógica do *data center*, já que um *data center* é composto por uma variedade de dispositivos. Na seção seguinte, serão apresentados conceitos de segurança de servidores em ambientes de *data center*.

2.2.1. Segurança de Servidores em Ambientes de Data Center

Servidores dentro das organizações podem fornecer uma variedade de serviços, tanto para acesso local ou remoto. Muitos servidores podem armazenar ou processar informações confidenciais (SCARFONE; JANSEN; TRACY, 2008). Normalmente podemos encontrar servidores de serviços de internet, banco de dados e servidores de arquivos. Servidores são frequentemente alvos de ataque por causa da importância dos seus dados.

Alguns exemplos de ameaças a servidores podem ser idenficadas:

- Entidades mal-intencionadas podem explorar *bugs* de software no servidor ou seu sistema operacional;
- Ataques de Negação de Serviço (*DoS* ou *DDoS*), impedindo os usuários de acessarem seus serviços;
- Acesso de pessoas não autorizadas a informações sensíveis;
- Algum indivíduo pode obter acesso não autorizado a outros recursos da rede através de uma vulnerabilidade do servidor;

Quando se trata de segurança em servidores existem alguns princípios que ajudam a resolver problemas de segurança:

- Simplicidade – Os sistemas de informação devem ser o mais simples possível. Complexidade sem necessidade pode ser um agravante na segurança;
- Falha na segurança – Caso ocorra uma falha, ela tem que ocorrer de forma mínima, sem que haja perda nos controles e configurações de segurança;
- Utilização de mediadores – Uso de permissões a sistemas de arquivos, *proxies*, *firewalls* e *gateways*;
- *Open Design* – A segurança em servidores não pode ser dependente de configurações sigilosas.
- Separação dos privilégios das funções – Na medida do possível, devem-se separar as funções.
- Menor privilégio – Determinar direitos mínimos para execução de tarefas/processos pelos usuários ou sistemas;
- Aceitabilidade psicológica – Os usuários devem entender a necessidade de segurança por meio de treinamento e educação;

- Defesa de profundidade – As organizações devem entender que um único mecanismo de segurança em geral é insuficiente;
- Fator de trabalho – As organizações devem entender qual o esforço para um invasor quebrar a segurança, a realização de análise de risco do ambiente pode ser uma saída;
- Registros – Registro e *logs* devem ser mantidos, para que em caso de comprometimento da segurança a organização tenha evidências do ataque, falha ou omissão disponíveis.

Várias organizações dependem de regulamentações e regras que são estabelecidas por órgãos especializados, como por exemplo: *IEEE e AMA.* Desta forma, isso também é válido para a segurança da informação (KRÁTKÝ et al., 2016) (FULLER et al., 2013).

2.3. Normas de Segurança da Informação

Normas de segurança da informação são necessárias no âmbito organizacional, pois permitem a redução de custos de produtos além de dar subterfúgio para se realizar avaliações. As normas de segurança podem fornecer medidas comuns para avaliações. Elas podem dar apoio para realizar avaliações utilizando critérios e orientações (BARKER; NELSON, 1988).

BARKER e NELSON (1988) explicam:

> "As normas de segurança também permitem a compatibilidade entre os produtos dos fornecedores. Compatibilidade que serve como uma conveniência para os clientes e aumenta a concorrência, que eventualmente diminui o custo dos produtos. A menos que a segurança seja barata e conveniente, ela será usada apenas para aplicativos muito sensíveis e muitas aplicações permanecerão desprotegidas. Normas para a segurança da informação não são fáceis de estabelecer. Os requisitos do usuário são diversos; De fato, os requisitos de um usuário podem entrar em conflito com os de outra pessoa".

No final dos anos 80, BARKER e NELSON (1988) já acreditavam que em um futuro próximo pudesse existir uma necessidade considerável das empresas aderirem normas de segurança para que conseguissem reduzir custos e aumentar a qualidade de seus produtos. Entretanto os autores consideraram também a hipótese de uma maior complexidade da aplicabilidade das normas de segurança no futuro devido à criação de várias comunidades comerciais e a grande carência de sistemas e políticas para diversas necessidades e filosofias sobre segurança.

Geralmente normas de segurança da informação são publicadas sob responsabilidade de órgãos onde membros são amplamente respeitados por sua experiência em segurança da informação. Essas normas podem ser adotadas por equipes técnicas tanto para empresas públicas ou privadas (BAYUK, 2010).

Ao incorporar normas de segurança nos processos organizacionais ou avaliações de segurança, muitas organizações que auditam sistemas, produtos e serviços podem caracterizar a segurança estando em conformidade com a organização ou não. Grande parte das normas de segurança foram criadas ou estabelecidas por partes que têm grande interesse em segurança da informação, por exemplo, a ISO/IEC 27002 (ISO/IEC 27002, 2013) e NIST(NIST, 2014) (BAYUK, 2010).

As normas de segurança da informação até o ano de 2010 foram formadas por contribuições de várias organizações que compilaram inúmeros controles de segurança após análises de falhas, ameaças e ataques conhecidos. De certa forma, adoação de normas de segurança depende de abordagens que facilitem o consenso industrial e não qualquer tentativa de justificativa acadêmica. (BAYUK, 2010).

Em ambientes empresariais, a perda de informações pode ocasionar em desvantagem competitiva e no pior dos cenários pode custar à falência da empresa. Acredita-se que o uso de normas de segurança podem reduzir custos, perda de informações e dar suporte a gestão da segurança nas organizações através de metodologias provenientes destas normas (HOLIK et al., 2015).

Para atender as necessidades de segurança, muitas empresas, institutos e disciplinas acadêmicas estão trabalhando em conjunto no desenvolvimento de normas para apoiar a garantia de segurança dos sistemas e serviços de TI, bem como outros campos do conhecimento (HOLIK et al., 2015).

O uso destas normas de segurança depende da legitimidade de seu uso nas organizações, além de ser analisado de modo significado a eficiência e o desempenho econômico (UWIZEYEMUNGU; POBA-NZAOU, 2012).

O interesse na utilização de normas de segurança é diminuir as falhas e suas consequências. Apesar de um crescente uso em normas pela indústria para garantir os processos de TI, várias técnicas e métodos surgiram nos últimos tempos para realização de ataques. Acredita-se que o uso de normas de segurança possa apoiar processos de monitoramento dos controles técnicos contra ataques dentro das organizações (MADAN; MADAN, 2010).

Conforme alguns conceitos encontrados na literatura, acredita-se que o uso de normas de segurança seja fundamental para agregar valor a sistemas, processos e serviços dentro das organizações. Além de dar embasamento em avaliações periódicas, onde a alta direção e até mesmo engenheiros de sistemas podem adotar as melhores decisões com base em relatórios.

No contexto deste trabalho, foram escolhidas duas normas de segurança da informação existentes, a ISO/IEC 27002 (2013) e NIST SP 800-53 (2014). A seguir são apresentadas as duas normas, bem como os conceitos principais, famílias e os controles de segurança;

2.3.1. ISO/IEC 27002 - Código de Prática para Controles de Segurança da Informação

Esta norma estabelece diretrizes e procedimentos para iniciar, implementar, manter e melhorar a gestão de segurança numa organização. Ela provê recomendações gerais para apoiar a segurança da informação e pode servir como guia prático para o desenvolvimento de procedimentos de segurança da informação e eficientes práticas para ajudar a dar confiança nas atividades das organizações (ISO/IEC 27002, 2013).

A norma ISO/IEC 27002 fornece um modelo para criação e operação de um sistema de gestão de segurança da informação. Este modelo incorpora as características em que especialistas na área chegaram a um consenso como sendo um estado da arte internacional. Além disso, ela oferece uma ampla variedade de controles. Esses controles podem partir desde técnicos e funcionais, incluindo éticos e lógicos, tais como: políticas, procedimentos e processos.

Esta norma parte da família de normas ISO/IEC 27000. Esta família destina-se a ajudar as organizações de todos os tipos e tamanhos para implementar e operar um sistema de gestão de segurança da informação e consiste em quinze normas (ISO/IEC 27000, 2014), no qual a norma ISO 27002 desta família contribuiu com este trabalho.

As referências das famílias dos controles de segurança da norma ISO/IEC 27002 estão listadas no Quadro 1 a seguir. Os detalhes dos controles de segurança que foram extraídos destas famílias são apresentados no Apêndice A deste trabalho.

Quadro 1: Referência das famílias dos controles da norma ISO/IEC 27002

Controles de Segurança
A.5 - Políticas de segurança da informação
A.6 - Organização da segurança da informação
A.7 - Segurança em recursos humanos
A.8 - Gestão de ativos
A.9 - Controle de acesso
A.10 – Criptografia
A.11 - Segurança física e do ambiente
A.12 - Segurança nas operações
A.13 - Segurança nas comunicações
A.14 - Aquisição, desenvolvimento e manutenção de sistemas
A.15 - Relacionamento na cadeia de suprimento
A.16 - Gestão de incidentes de segurança da informação
A.17 - Aspectos da segurança da informação na gestão da continuidade do negócio
A.18 - Conformidade

Fonte: ISO/IEC 27002 (2013)

2.3.2. NIST SP 800-53 - Controles de Segurança e Privacidade para Sistemas em Organizações Federais de Informação

A norma NIST SP 800-53 é uma das normas de segurança que ajudam as organizações a abordarem questões de gestão de segurança em seu ambiente. Ela ajuda a gerenciar controles de acesso a sistemas de informação. Esta norma é de uso obrigatório de agências federais, mas também é recomendada para governos e setores privados. (NWAFOR et al., 2012) (BREAUX et al., 2013). Segundo o Instituto Nacional de Normas e Tecnologia dos Estados Unidos da América (NIST), foram desenvolvidos controles de segurança para alcançar os objetivos para gerenciar riscos e manter sistemas de informações mais seguros (NIST, 2014).

A norma NIST SP 800-53 consiste de 26 normas, mas para atender o objetivo deste trabalho e aproximação quanto ao conteúdo dos controles da norma ISO 27002, foi selecionada a norma NIST 800-53. As referências das famílias dos controles de segurança desta norma estão

listadas no Quadro 2 a seguir. Assim como na ISO 27002, os detalhes dos controles de segurança que foram extraídos destas famílias da norma NIST 800-53 estão apresentados no apêndice A deste trabalho.

Quadro 2: Referências das famílias dos controles da norma NIST SP 800-53

Controles de Segurança
AC - Controle de Acesso
AT - Conscientização e Treinamento
AU - Auditoria e Responsabilização
CA - Avaliação e Autorização de Segurança
CM - Gerenciamento de Configuração
CP - Planejamento de Contingência
IA - Identificação e autenticação
IR - Resposta de Incidente
MA - Manutenção
MP - Proteção de Mídias
PE - Proteção Física e Ambiental
PL - Planejamento
PS - Segurança Pessoal
AR - Avaliação de risco
SA - Aquisição de Sistemas e Serviços
SC - Sistema de Proteção de Comunicações
SI - Sistema de Integridade de Informação
PM - Gerenciamento de Programa

Fonte: NIST(2014).

2.4. Modelos de Maturidade

2.4.1. Visão Geral

Um modelo de maturidade de segurança pode fornecer guias de segurança de forma abrangente. Ele pode definir quais recursos de segurança podem ser implementados dentro da organização (RIGON; WESTPHALL, 2013). Eles incentivam o uso de normas e melhores práticas (WOODHOUSE, 2008) e devem ser entendidos como capacidades de repetir entregas de forma previsível (SEI, 2010). Além disso, modelos de maturidade de segurança podem identificar lacunas que representam riscos. Assim, poderão ser realizados programas de melhorias na segurança da informação da organização (RIGON; WESTPHALL, 2013).

Modelos de maturidade normalmente são usados para avaliar e orientar qualquer tipo de melhoria de processos, desde desenvolvimento de software até mesmo aquisição de produtos, gestão de produtos e gestão de segurança. Além disso, tais modelos são baseados em processos, fornecendo melhorias nesses processos. Em outras palavras, quanto maior o nível de maturidade, melhor a organização poderá definir e melhorar a capacidade de seus processos (WOODHOUSE, 2008).

Em ambientes corporativos a informação é o principal ingrediente para que as organizações ganhem vantagem no mercado. Essas informações impulsionam a maioria dos processos. Esses processos podem envolver funcionários em qualquer escala hierárquica, ou seja, desde a alta gerência até o funcionário do nível mais baixo. Desta forma, modelos de maturidade têm se tornado cada vez mais importantes para a gestão organizacional.

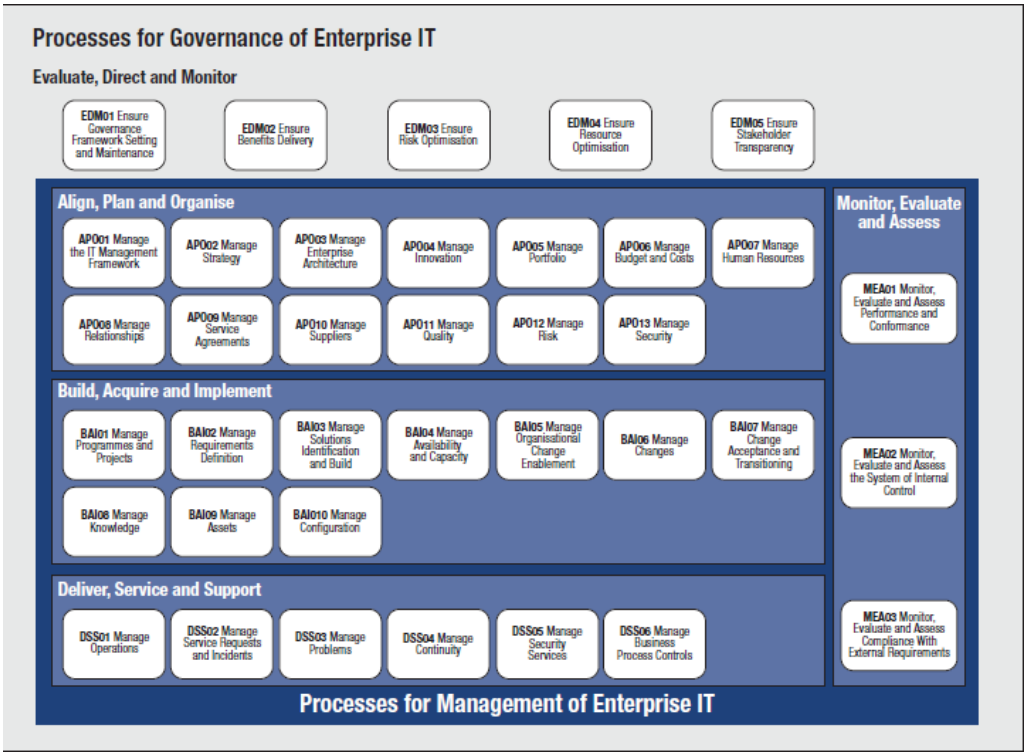
Partindo destas premissas, esta seção apresenta dois dos principais modelos de maturidade existentes na literatura, os modelos CobiT (ISACA, 2012) e CMM (SEI, 2010). Além disso, esses modelos deram origem a vários outros. Alguns trabalhos que se basearam nesses dois modelos são apresentados no capítulo 5, capítulo esse que relaciona vários trabalhos que têm como foco modelos de maturidade de segurança da informação.

2.4.2. Cobit

2.4.2.1. Visão Geral do Cobit

O Cobit fornece boas práticas através de um modelo de domínios e processos e apresenta atividades numa estrutura lógica e gerenciável. O Cobit tem um foco maior na execução de seus controles. Desta forma, práticas ajudarão a aperfeiçoar as atividades e investimentos em TI nas organizações, além de assegurar a entrega dos serviços (ISACA, 2012). O modelo Cobit tem como base ser um modelo de processos de TI, que são subdivididos em cinco domínios e trinta e sete processos:

Figura 1: Domínios e Processos do COBIT



Fonte: ISACA (2012).

Esses domínios tem a responsabilidade de planejar, construir, executar e monitar para prover uma visão geral da TI na organização (JANSSEN, 2008) (ISACA, 2012).

O documento do Cobit desenvolvido pela ISACA (2012) foi dividido em quatro partes. A primeira é chamada de Sumário Executivo, por se tratar de uma introdução ao Cobit. Em seguida temos os Objetivos dos Controles e Orientações de Gerenciamento, e por fim Modelos de Maturidade, que é o foco desta seção.

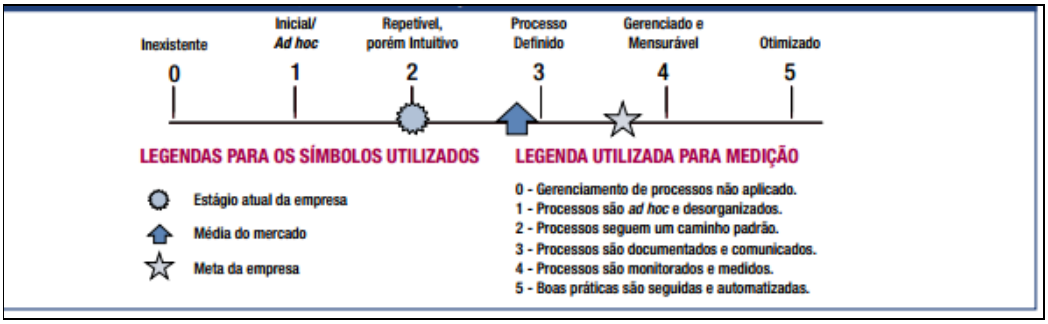
2.4.2.2.Modelo de Maturidade do Cobit

O modelo de maturidade do Cobit é descrito para que seja possível avaliar cada processo. Esses modelos são importantes para saber qual o grau de maturidade de um processo na organização, além de se estabelecer objetivos claros que a organização pretende atingir.

Segundo a ISACA (2012) “as organizações precisam avaliar os processos e onde são requeridas melhorias, bem como implementar um conjunto de ferramentas de gerenciamento para atingir esses aprimoramentos”. O modelo de maturidade do Cobit identifica cinco níveis de maturidade para controle de gestão da TI nas organizações que são pontuadas entre 0 e 5, e que permite identificar quais melhorias podem ser realizadas. O Cobit descreve um modelo através de atividades que formam um processo. Para os seis níveis de maturidade, eles não se tornam absolutos, pois não se pode ter precisão total, já que várias implementações serão realizadas em diferentes níveis (JANSSEN, 2008) (JACOBS; ARNAB; IRWIN, 2013).

A base de medição do Cobit é realizada em uma escala simples de maturidade. Nessa escala é desmonstrada a evolução de um processo, podendo ser esta maturidade inexistente, evoluindo até capacidade otimizada. A representação gráfica é apresentada na Figura 2.

Figura 2: Escala Gráfica de Maturidade do Cobit



Fonte: ISACA (2012).

Essa escala de maturidade é bastante similar ao modelo CMM, mas é interpretada de acordo com a natureza de cada processo (ISACA, 2012). As descrições dessa escala de maturidade são apresentadas no Quadro 3.

Quadro 3: Escala de Maturidade do Cobit

Nível	Descrição
0 - Inexistente	Completa falta de um processo reconhecido. A empresa nem mesmo reconheceu que existe uma questão a ser trabalhada.
1 - Inicial / Ad hoc	Existem evidências que a empresa reconheceu que existem questões e que precisam ser trabalhadas. No entanto, não existe processo padronizado; ao contrário, existem enfoques *Ad Hoc* que tendem a ser aplicados individualmente ou caso-a-caso.
2 - Repetível, porém Intuitivo	Os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa. Não existe um treinamento formal ou uma comunicação dos procedimentos padronizados e a responsabilidade é deixado com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e consequentemente erros podem ocorrer.
3 - Processo Definido.	Procedimentos foram padronizados, documentados e comunicados através de treinamento. É mandatório que esses processos sejam seguidos; no entanto, possivelmente desvios não serão detectados. Os procedimentos não são sofisticados, mas existe a formalização das práticas existentes.
4 - Gerenciado e Mensurável.	A gerência monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando muito bem. Os processos estão debaixo de um constante aprimoramento e fornecem boas práticas. Automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada.
5 - Otimizado.	Os processos foram refinados a um nível de boas práticas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade como outras organizações. TI é utilizada como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e efetividade, tornando a organização rápida em adaptar-se.

Fonte: ISACA (2012)

2.4.3. CMM

O modelo CMM (*Capability Maturity Model*) surgiu pela necessidade de melhorar a qualidade dos softwares nas organizações. Dessa forma, deveria ser feita uma avaliação de processos de desenvolvimento de software usando uma ferramenta nas empresas que fornecem softwares e sistemas (SEI, 2010).

A partir de 1991 o SEI começou a desenvolver CMMs para várias disciplinas, que partem de modelos para engenharia de sistema, Engenharia de Software, Aquisição de Software, Gestão e Desenvolvimento de Força de Trabalho e Desenvolvimento Integrado de Processo e Produto (IPPD) (SEI, 2010). Para o SEI (2010) "os CMMs focam na melhoria de processo em uma organização. Eles contêm os elementos essenciais de processos efetivos para uma ou mais disciplinas e descrevem um caminho de melhoria evolutiva desde processos imaturos, ou *ad hoc*, até processos maduros, disciplinados, com qualidade e eficácia melhoradas".

Um problema que foi identificado no uso desses múltiplos modelos foi uma grande diferença entre eles, já que cada modelo era orientado a disciplinas específicas. Desta forma esses modelos não eram utilizados de forma integrada, tornando o custo de sua implantação muito elevado.

Uma saída para o SEI foi criar um modelo totalmente integrado com cada disciplina. Através da criação de um *framework* integrado, haveria um menor esforço na busca de melhoria de seus processos. Inicialmente foram integrados os modelos *Capability Maturity Model for Software* (SW-CMM) v2.0; *Systems Engineering Capability Model* (SECM), e *Integrated Product Development Capability Maturity Model* (IPD-CMM) (SEI, 2010).

A integração desses modelos recebeu o nome de CMMI (*Capability Maturity Model Integration*). Um modelo integrado não apenas significou uma simples combinação, mas sim um *framework* de múltiplas disciplinas, tornando-o totalmente flexível para apoiar as diferentes abordagens.

O CMM identifica os níveis de maturidade como uma forma de evolução bem definida para os processos de software. Cada nível de maturidade compreende um conjunto de processos assim que os objetivos são satisfeitos e estabiliza um componente do processo. Cada nível do quadro de maturidade refere-se a componentes diferentes do processo de software. Desta forma o CMM organizou o modelo em cinco níveis de maturidade para promover ações e melhorias no processo de software. Os níveis de maturidade são apresentados a seguir nano Quadro 4.

Quadro 4: Escala de Maturidade do CMM

Nível	Descrição
Inicial	Os processos são *ad hoc* e caóticos. Esse tipo de organização não fornece um ambiente estável para apoiar os processos. O sucesso depende da competência e do heroísmo das pessoas e não do uso dos processos comprovados.
Gerenciado	Os projetos da organização têm a garantia de que os processos são planejados e executados de acordo com uma política; os projetos empregam pessoas experientes que possuem recursos adequados para produzir saídas controladas; envolvem partes interessadas relevantes; são monitorados, controlados e revisados; e são avaliados para verificar sua aderência em relação à descrição de processo.
Definido	Os processos são bem caracterizados e entendidos, e são descritos em padrões, procedimentos, ferramentas e métodos. O conjunto de processos-padrão da organização, que é a base para o nível de maturidade 3, é estabelecido e melhorado ao longo do tempo.
Gerenciado Quantitativamente	A organização e os projetos estabelecem objetivos quantitativos para qualidade e para desempenho de processo, utilizando-os como critérios na gestão de processos. Objetivos quantitativos baseiam-se nas necessidades dos clientes, dos usuários finais, da organização e dos responsáveis pela implementação de processos.
Otimizado	Uma organização melhora continuamente seus processos com base no entendimento quantitativo das causas comuns de variação inerentes ao processo.

Fonte: SEI (2010)

2.5. Considerações Finais

Conforme foi apresentado neste capítulo, foram destacados fundamentos importantes dentro do contexto da temática deste trabalho.

- Conforme apresentado na Subseção 2.4, foram apresentados dois dos principais modelos de maturidade existentes. Esses modelos foram escolhidos, pois servem como base para muitos modelos que existem tanto na esfera comercial ou acadêmica. Após uma investigação na literatura, foi identificado que existem alguns modelos de maturidade de segurança da informação para diversas áreas da segurança.

3. AVALIANDO E MELHORANDO O ESTADO DE SEGURANÇA DE SERVIDORES EM AMBIENTES DE *DATA CENTER*

Este capítulo apresenta uma metodologia, que visa avaliar o nível de maturidade da configuração de segurança de servidores em *data centers*. Inicialmente, tem-se uma visão geral das atividades e componentes para facilitar a compreensão da metodologia como um todo. Em seguida, são apresentados os detalhes de cada atividade e como realizar a avaliação usando esta metodologia. Por fim, são discutidos o uso e a importância desta metodologia.

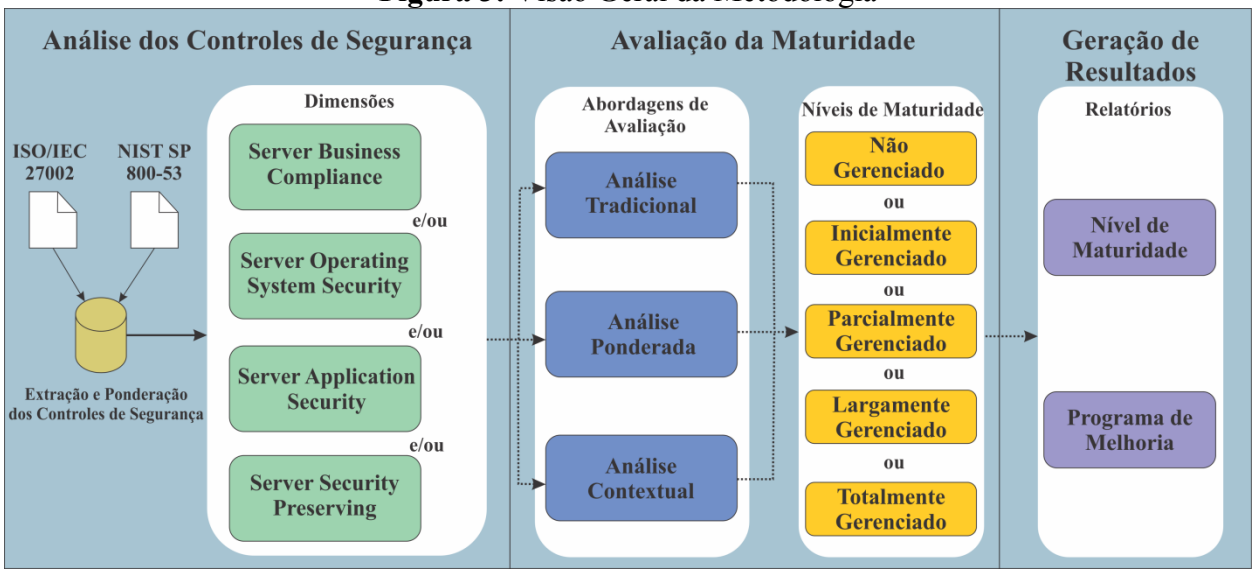
3.1. Visão Geral

O objetivo principal da metodologia proposta neste trabalho é melhorar o nível de segurança do *data center* das organizações, independente do sistema operacional utilizado no *data center*, serviços e versões. Em outras palavras, ela permite a avaliação e melhoria da maturidade das configurações de segurança do servidor em ambientes de *data center*.

Com esta metodologia é também possível avaliar as políticas de segurança existentes em normas internacionais voltadas para configurações de servidores e fornecer diretrizes para avaliar a maturidade de segurança das organizações.

A seguir (Figura 3), é apresentada uma visão geral desta metodologia e uma breve descrição de cada atividade da metodologia.

Figura 3: Visão Geral da Metodologia



Fonte: Elaborado pelo autor

1. **Análise dos Controles de Segurança**. É baseada na seleção das dimensões de segurança, que contém um conjunto de controles de segurança para apoiar a configuração do *data center*. Esta atividade é composta pela seleção de quais controles de segurança serão analisados e avaliados na organização. Os controles de segurança são divididos em quatro áreas: servidor em conformidade com diretrizes do negócio, segurança do sistema operacional, aplicações utilizadas no servidor e mantendo a segurança do servidor. Estes controles de segurança foram extraídos a partir das normas de segurança da informação *ISO/IEC 27002* e *NIST-SP 800-53* (ISO/IEC 27002, 2013) (NIST, 2014);
2. **Avaliação de Maturidade**: Esta atividade é composta pela seleção do tipo de abordagem de avaliação a ser utilizada. A metodologia propõe três abordagens: *análise tradicional*, *análise ponderada* e *análise contextual*. A análise tradicional segue apenas os controles de segurança e considera o mesmo nível de importância a todos os controles. A análise ponderada é comparativamente mais complexa, pois adota mais de uma norma de segurança. Se em cada controle de segurança aparecer as duas normas como base, maior será sua importância para a análise que estará sendo realizada. Eventualmente, análise contextual é semelhante à análise ponderada, que também considera a opinião da organização sobre o nível de importância de cada controle de segurança. Cada abordagem de avaliação produz um nível de maturidade da configuração de segurança do servidor após a análise.
3. **Geração de Resultados**. Esta atividade final da metodologia reporta o nível de maturidade em que se encontram as configurações de segurança do servidor após a avaliação, entregando a alta direção da organização dados quantitativos em alto nível (*Nível de Maturidade*), além de entregar uma política de segurança adequada para atender os requisitos encontrados, incluindo um conjunto de recomendações de melhorias (*Programa de melhoria*), informando os pontos fortes e fracos de segurança da empresa com o intuito de auxiliar o monitoramento dos objetivos de segurança da informação na organização.

Nas seções seguintes são apresentados os detalhes de cada atividade desta metodologia

3.2. Análise dos Controles de Segurança

Durante o processo de revisão da literatura, foram identificadas e analisadas dezessete normas internacionais de segurança para extração de controles de segurança ou boas práticas de segurança da informação:

- ISO/IEC 27001 (ISO 27001, 2013);
- ISO/IEC 27002 (ISO/IEC 27002, 2013);
- ISO/IEC 27004 (ISO/IEC, 2016);
- ISO/IEC 27005 (ISO/IEC, 2011);
- NIST SP 800-53 (NIST, 2014b);
- NIST SP 800-123 (SCARFONE; JANSEN; TRACY, 2008);
- NIST SP 800-39 (CHRISTOPHER ALBERTS, 2011),
- NIST SP 800- 126 (BANGHART; JOHNSON, 2011),
- NIST SP 800-44v2 (WINOGRAD; TRACY; JANSEN, 2007)
- NIST SP 800-14 (SWANSON; GUTTMAN, 1996);
- NIST SP 800-17 (KELLER; SMID, 1998);
- NIST SP 800-20 (SERVICES et al., 1999);
- NIST SP 800-128 (JOHNSON, 2011);
- OWASP (OWASP, 2017);
- OWASP TOP 10 (OWASP et al., 2013);
- OWASP *Application Security Verification Standard* v3 (OWASP, 2017);
- TIA 942 (TIA, 2005);

Também foram identificados e analisados cinco documentos relacionados a recomendações sobre configurações e serviços de servidor:

- Microsoft Baseline (MICROSOFT, 2017);
- Guia de Implantação do Red Hat Linux (SMITH, 2007);
- Manual Oficial Debian (HERTZOG; MAS, 2012);
- IBM Secure Hardening Guide (VAULT, 2016).

Após a revisão, foram realizadas extrações dos controles de segurança a partir das normas ISO/IEC 27002 (ISO/IEC 27002, 2013) e NIST SP 800-53 (NIST, 2014). Essas normas foram selecionadas por contemplarem a maior parte dos controles recomendados por outras normas. Em outras palavras, essas duas normas são as que melhor representam as demais normas avaliadas.

3.2.1. Ponderação dos Controles de Segurança

Durante a extração dos controles de segurança foram realizadas comparações e identificação de semelhanças entre os controles das normas ISO 27002 e NIST SP 800-53. Desta forma, um controle de segurança desta metodologia que está presente nas normas ISO 27002 e NIST SP 800-53 é considerado mais valioso e recebe um peso 2. Os controles de segurança presentes em apenas uma destas duas normas recebe peso 1. A ponderação dos controles de segurança é uma métrica usada para fornecer peso a cada controle de segurança da presente metodologia. A metodologia utiliza tal ponderação nas análises ponderada e contextual.

Como forma de exemplificar o conceito de ponderação dos controles de segurança, é apresentada na Tabela 1 uma breve lista de ponderação destes controles.

Tabela 1: Exemplo de ponderação dos controles de segurança desta metodologia

Controles de Segurança	**Normas Extraídas**		**Peso/ Ponderação**
	ISO/IEC 27002	**NIST SP 800-53**	
SAS 5.3 - Execução de Software Antivírus	A. 12.2.1	SI-3	2
SBC 2.1 - Identificação da Legislação e conformidades contratuais	A.12.1.1	SA-5	2
SOS 1.4 - Restauração do Sistema Operacional	A. 12.5.1	Nulo	1
SBC 8.1 - Informação da Arquitetura de Segurança do *Data Center*	Nulo	PL-8	1
SAS 3.1 - Restrições de acesso à informação	A.9.4.1	AC-3, AC-24	2
SSP 6.1 - Autorização para Ambiente de Teste	A.14.3.1(a)	Nulo	1
SSP 6.5 - Teste de Penetração	Nulo	RA-5	1

Fonte: Elaborado pelo autor

3.2.2. Dimensões

As dimensões, no contexto da metodologia proposta neste trabalho, são conjuntos de controles e medidas de segurança que têm como objetivo abordar aspectos específicos e relacionados com o mesmo tema da segurança das configurações dos servidores. Essas

dimensões favorecem a compreensão sobre os controles de segurança, pois cada dimensão tem seu objetivo bem definido.

As dimensões desta metodologia foram projetadas visando níveis organizacionais que pudessem estar ligados a configurações de segurança dos servidores em ambientes de *data center*. Desta forma é possível apoiar as políticas de segurança para um determinado foco. Em outras palavras, essas dimensões podem atuar com políticas de segurança entre o alto e baixo nível nas configurações de segurança dos servidores.

Cada dimensão contém um grupo de famílias. Uma família inclui uma série de controles de segurança associados a um assunto específico. Um controle de segurança é uma política, prática ou alienações definidas para atingir um propósito específico.

A metodologia propõe quatro dimensões:

- *Server Business Compliance* (SBC);
- *Server Operating System Security* (SOS);
- *Server Application Security* (SAS);
- *Server Security Preserving* (SSP).

Durante a avaliação da maturidade, a organização estará livre para escolher quais dimensões serão utilizadas. A seguir são apresentadas as quatros dimensões propostas neste trabalho.

3.2.2.1. *Server Business Compliance* (SBC)

Esta dimensão visa alinhar os objetivos de negócio com configuração de segurança do servidor no ambiente do *data center*. Ela se concentra em aspectos de documentação do baixo (sistemas) e alto nível (administração da organização) para oferecer suporte às configurações de segurança e tem seus controles baseados em requisitos de conformidade legal e documentações sobre procedimentos de segurança. No total, esta dimensão é composta por oito famílias e dezoito controles de segurança. As famílias e os controles de segurança desta dimensão são apresentados na Tabela 2 a seguir. Os detalhes (propostas e guia de implementação) destes controles são apresentados no Apêndice A deste trabalho.

Tabela 2: Famílias e controles de segurança da dimensão *Server Business Compliance*

Famílias	Controles de Segurança
SBC 1 - Orientações Acerca da Configuração do *Data Center* e o Negócio	SBC 1.1 - Estratégia para Configuração da Segurança do *Data Center*
	SBC 1.2 - Análise Crítica das Políticas para Configuração de Segurança do *Data Center*
	SBC 1.3 - Documentação do Sistema Utilizado no *Data Center*
SBC 2 - Conformidade com os Requisitos Legais e Contratuais	SBC 2.1 - Identificação da Legislação e Conformidades Contratuais
	SBC 2.2 - Direitos de Propriedade Intelectual
	SBC 2.3 - Privacidade nas Informações Pessoais
	SBC 2.4 - Controles de Criptografia
SBC 3 - Contratação de Profissionais	SBC 3.1 - Seleção dos Profissionais
	SBC 3.2 - Termos e Condições de Contrato
SBC 4 - Conscientização, e Treinamento para Configuração de Segurança do *Data Center*	SBC 4.1 - Sanções Disciplinares
	SBC 4.2 - Treinamento da Segurança do *Data Center*
SBC 5 - Requisitos do Negócio para Controle de Acesso	SBC 5.1 - Políticas de Controle de Acesso
SBC 6 - Classificação da Informação no *Data Center*	SBC 6.1 - Classificação da Informação
	SBC 6.2 - Marcação da Informação
SBC 7 - Documentação dos Procedimentos de Segurança	SBC 7.1 - Responsabilidades e Procedimentos Operacionais
	SBC 7.2 - Políticas e Procedimentos de Manutenção do *Data Center*
	SBC 7.3 - Políticas e Procedimentos de Avaliação de Risco de Configuração do *Data Center*
SBC 8 - Informação da Arquitetura de Segurança do *Data Center*	SBC 8.1 - Informação da Arquitetura de Segurança do *Data Center*

Fonte: Elaborado pelo autor

3.2.2.2.*Server Operating System Security* (SOS)

Esta dimensão visa apoiar as políticas de segurança que tem como foco as configurações de segurança do(s) sistema(s) operacional(is) utilizado(s) no *data center*. Um número considerável de problema de segurança pode ser evitado se o sistema operacional estiver configurado corretamente. Como a indústria não está ciente da necessidade particular de seus clientes, servidores que armazenam as informações das organizações precisam ser instalados e configurados de acordo com os requisitos da organização.

No total esta dimensão é composta por seis famílias e trinta e seis controles de segurança. As famílias e os controles de segurança desta dimensão são apresentados na Tabela 3 a seguir. Os detalhes destes controles são apresentados no Apêndice A deste trabalho.

Tabela 3: Famílias e controles de segurança da dimensão *Server Operating System Security*

Famílias	Controles de Segurança
SOS 1 - Segurança no *Deploy* do Sistema Operacional	SOS 1.1 - Configuração da Partição do Sistema de Arquivos
	SOS 1.2 - Segurança no Bootloader do Sistema Operacional
	SOS 1.3 - Segurança dos Dispositivos de Entrada e Saída do *Data Center*
	SOS 1.4 - Restauração do Sistema Operacional
	SOS 1.5 - Segurança na Memória do Sistema Operacional
SOS 2 - Atualização de Patches do Sistema Operacional	SOS 2.1 - Execução por Profissionais Treinados
	SOS 2.2 - Teste de Atualização do Sistema Operacional
	SOS 2.3 - Atualização no Sistema Operacional
SOS 3 - Segurança do Sistema Operacional	SOS 3.1 - Remoção e Desativação de Serviços e Protocolos desnecessários
	SOS 3.2 - Criptografia no Sistema de Arquivo
	SOS 3.3 - Envio de Chave de Decodificação
SOS 4 - Controle de Acesso	SOS 4.1 - Registro e remoção de usuários
	SOS 4.2 - Atribuir Credenciais do Usuário
	SOS 4.3 - Criação de Grupos de Usuário
	SOS 4.4 - Renomear as contas de administrador
	SOS 4.5 - Limitação de Acesso nas Estações de Trabalho
	SOS 4.6 - Remoção de Contas Padrão do Sistema
SOS 5 - Autenticação do Usuiário do Sistema Operacional	SOS 5.1 - Senhas Sólidas
	SOS 5.2 - Usuários e Senhas Exclusivas
	SOS 5.3 - Criação de Senha de Dois Fatores
	SOS 5.4 - Bloqueio de Tela por Inatividade
SOS 6 - Segurança de Redes no Sistema Operacional	SOS 6.1 - Controles de Redes - Responsabilidades Operacionais
	SOS 6.2 - Controles de Redes - Proteção da Disponibilidade e Integridade dos Dados
	SOS 6.3- Controles de Redes - Gerenciamento dos Serviços de Rede
	SOS 6.4 - Controles de Redes - Sistemas sobre Redes
	SOS 6.5 - Controles de Redes - Conexão sobre Sistemas à Rede
	SOS 6.6 - Controles de Redes - Registro de Atividades da Rede
	SOS 6.7 - Isolamento do Servidor
	SOS 6.8 - Remoção de Conteúdo
	SOS 6.9 - Restrição de Acesso na Internet
	SOS 6.10 - Segurança de Serviço de Redes
	SOS 6.11 - Segregação de Redes em Domínio
	SOS 6.12 - Transferência das Informações
	SOS 6.13 - Segurança na Resolução de Nomes (Autoritativo)
	SOS 6.14 - Segurança na Resolução de Nomes (Caching e Recursivo)

Fonte: Elaborado pelo autor

3.2.2.3.*Server Application Security* (SAS)

Essa dimensão inclui controles de segurança para melhorar o nível de segurança de aplicações utilizadas no servidor. Ela envolve a instalação de procedimentos como, verificação de novas vulnerabilidades, configuração de privilégios de acesso, política de transferência de arquivos e muitos outros aspectos que representam uma ameaça ao usar uma determinada aplicação. Esta dimensão considera os controles que oferecem suporte a segurança das aplicações na instalação, configuração, privilégios e na transferência de arquivos.

No total esta dimensão é composta por cinco famílias e vinte e dois controles de segurança. As famílias e os controles de segurança desta dimensão são apresentados na Tabela 4 a seguir. Os detalhes (propostas e o guia de implementação) destes controles são apresentados no Apêndice A deste trabalho.

Tabela 4: Famílias e controles de segurança da dimensão *Server Application Security*

Famílias	Controles de Segurança
SAS 1 - Instalação Segura dos Softwares	SAS 1.1 - Política e Procedimento para Aquisição de Software ou Serviço
	SAS 1.2 - Desinstalação de Softwares Desnecessários
	SAS 1.3 - Atualização dos Softwares e Aplicativos
	SAS 1.4 - Limite de Privilégio na Operacionalização dos Softwares
	SAS 1.5 - Configuração de Software em Ambiente de Teste
	SAS 1.6 - Execução de Códigos
	SAS 1.7 - Contingência dos Softwares
	SAS 1.8 - Arquivamento dos Softwares
SAS 2 - Restrições aos Recursos do Servidor	SAS 2.1 - Configuração da Partição do Sistema de Arquivos de Softwares
	SAS 2.2 - Controle de Acesso Concorrente
SAS 3 - Controle de Acesso do Software	SAS 3.1 - Restrições de acesso à Informação
	SAS 3.2 - Segurança no Login do Software
	SAS 3.3 - Software de Gerenciamento de Senha
	SAS 3.4 - Software Utilitários Privilegiados
	SAS 3.5 - Controle ao Código Fonte dos Softwares
SAS 4 - Segurança em Softwares de Transferência de Arquivos	SAS 4.1 - Criptografia na Transferência dos Dados
SAS 5 - Instalação e Configuração de Controles de Segurança Adicionais	SAS 5.1 - Instalação de Software Antivírus
	SAS 5.2- Atualização de Software Antivírus
	SAS 5.3 - Execução de Software Antivírus
	SAS 5.4 - Notificação de falha da Segurança no Software
	SAS 5.5 - Verificação Automatizada da Segurança
	SAS 5.6 - Relatório da Segurança

Fonte: Elaborado pelo autor

3.2.2.4.*Server Security Preserving* (SSP)

Esta dimensão fornece recomendações gerais para gerenciar com segurança as configurações do *data center*. Esta atividade inclui gerenciamento, monitoramento, registro e auditoria de incidentes de segurança de *data centers*. Finalmente, os gerentes devem manter continuamente a segurança após o processo de implantação.

No total esta dimensão é composta por seis famílias e vinte e três controles de segurança. As famílias e os controles de segurança desta dimensão são apresentados na Tabela 5 a seguir. Os detalhes destes controles são apresentados no Apêndice A deste trabalho.

Tabela 5: Famílias e controles de segurança da dimensão Server Security Preserving (SSP)

SSP 1 - Gestão de Incidente de Segurança do *Data Center*	SSP 1.1 - Responsabilidades e Procedimentos no *Data Center*
	SSP 1.2 - Notificação de fragilidade do Sistema do *Data Center*
	SSP 1.3 - Avaliação e Decisão dos Eventos de Segurança do *Data Center*
	SSP 1.4 - Resposta aos Incidentes de Segurança do *Data Center*
SSP 2 - Registro e Monitoramento	SSP 2.1 - Sistemas de Relatórios e Registros em Tempo Real
	SSP 2.2 - Proteção da Informação Auditada
	SSP 2.3 - Registro dos Administradores e Operadores do *Data Center*
	SSP 2.4 - Retenção de Registros
	SSP 2.5 - Sincronização do Relógio
SSP 3- Auditoria	SSP 3.1 - Capacidade de Auditoria
	SSP 3.2 - Auditoria e Geração de Relatórios Otimizados
	SSP 3.3 - Auditoria Alternativa
SSP 4 - *Backup*	SSP 4.1 - Cópias de Segurança - Completude e Exatidão das Cópias
	SSP 4.2 - Cópias de Segurança - Abrangência e Frequência
	SSP 4.3 - Cópias de Segurança - Armazenamento Remoto
	SSP 4.4 - Cópias de Segurança - Criptografia
SSP 5 - Redundância	SSP 5.1 - Disponibilidade dos Recursos de Configuração do *Data Center*
SSP 6 - Teste de Segurança do *Data Center*	SSP 6.1 - Proteção dos Dados para Teste
	SSP 6.2 - Autorização para Ambiente de Teste
	SSP 6.3- Exclusão dos Dados no Ambiente de Teste
	SSP 6.4 - Registro do Uso dos Dados no Ambiente de Teste
	SSP 6.5 - *Scanning* de Vulnerabilidades
	SSP 6.6 - Teste de Penetração

Fonte: Elaborado pelo autor

3.3. Avaliação da Maturidade

Os modelos de maturidade incentivam o uso de padrões e melhores práticas. Devido a isso, muitas organizações estão integrando novas soluções de tecnologia para modernizarem-se e desenvolverem-se. Muitas organizações tentam fornecer sistemas de informação confiáveis, embora não seja possível desenvolver sistemas de informação apenas com solução técnica de TI, pois os programas de segurança também envolvem aspectos humanos e organizacionais (WOODHOUSE, 2008).

O foco principal da presente metodologia é medir a maturidade da configuração de segurança do *data center*. Assim, deve ser analisado, compreendido e adaptado às características da organização. Ao fazer a avaliação, pode ser possível melhorar a qualidade da configuração de segurança do *data center*. Nesta seção são apresentadas as abordagens de avaliação que são propostas nesta metodologia e os níveis de maturidade respectivamente.

3.3.1. Abordagens de Avaliação

As métricas de segurança nesta metodologia podem ajudar a fornecer diretrizes, além de específicar critérios para que seja possível alcançar o nível de maturidade desejado. Essas métricas podem ser importantes para tomadas de decisão, garantindo assim a qualidade das configurações de segurança do servidor.

Considerando o contexto deste trabalho, as métricas propostas nas abordagens de avaliação são apresentadas na Tabela 6.

Tabela 6: Métricas propostas para as abordagens de avaliação

Iniciais	Métricas	Descrição
EV	Valor da Evidência	Valor obtido na coleta de evidências. Determina o grau de implementação do controle avaliado.
CW	Peso do Controle	Valor obtido no peso de cada controle.
OW	Peso Organizacional	Nível de importância que a empresa atribui a cada controle.
MaxEV	Valor máximo da Evidência	Valor máximo que pode ser atribuído ao grau de implementação do controle durante a coleta de evidências.

Fonte: Elaborado pelo autor

Como apresentado anteriormente três abordagens de avaliação foram desenvolvidas para utilizar as métricas descritas na Tabela 6, com o objetivo de analisá-las a partir de diferentes

perspectivas. Embora sejam abordagens diferentes, uma não exclui a outra. Ao contrário, elas se completam. Essas abordagens são chamadas de análises *tradicional, ponderada e contextual*.

3.3.1.1.*Análise Tradicional*

A *análise tradicional* avalia o nível de maturidade do *data center* com base exclusivamente na coleta de evidências que comprovem que algum controle de segurança foi implementado.

Uma evidência pode ser de dois tipos:

- Artefatos tangíveis - documentações, contratos, termos e normas;
- Artefatos intangíveis - código-fonte, arquivos de *log*, arquivos de configurações e configurações de software.

É utilizada uma escala (valor da evidência) de 0 a 4 para classificar a evidência de que a configuração do *data center* respeita o controle de segurança, onde:

- 0 - Nenhuma evidência: não há evidência mínima de uma implementação;
- 1 - Não implementado: Os artefatos são considerados inapropriados. Nenhuma outra evidência dá suporte à implementação dos controles de segurança;
- 2 - Parcialmente implementado: Os artefatos são considerados inapropriados. As evidências coletadas sugerem que alguns aspectos práticos devem ser implementados;
- 3 - Amplamente implementado: Existem artefatos suficientes, que ajudam a manter o estado de segurança atual do *data center*. Os resultados mostram que são adequados e confirmam o desempenho do controle de segurança. Entranto, deficiências ainda são encontradas;
- 4 - Totalmente implementado: Os artefatos são suficientes, o que ajuda a manter o estado de segurança atual do *data center*. Os resultados mostram que esses artefatos são adequados e confirmam o desempenho do controle de segurança. Não existem evidências de deficiência.
-

O nível de maturidade nesta abordagem é calculado através da Equação 1, onde n é o número de controles de segurança analisados, EVi é o valor de evidência obtida após sua análise e MaxEV é 4 multiplicado pelo número de controles analisados.

$$\overline{\boldsymbol{X}} = \frac{\sum_1^n \boldsymbol{EVi}}{\boldsymbol{MaxEV}} \quad (1)$$

3.3.1.2.*Análise Ponderada*

A análise ponderada atribui peso aos controles de segurança. Se um determinado controle de segurança está presente tanto na norma ISO/IEC 27002 (ISO/IEC 27002, 2013) como NIST SP 800-53 (NIST, 2014), receberá uma ponderação mais alta (peso 2) do que se foi extraído de apenas uma única norma (peso 1). Para isso, foram comparados os controles de segurança das normas para identificar semelhanças.

A análise ponderada considera que os controles de segurança que aparecem nas duas normas precisam de mais atenção e são ponderados mais altos do que aqueles que estão presentes em apenas uma norma.

O nível de maturidade nesta abordagem é calculado através da Equação 2, onde n é o número de controles de segurança analisados, EVi é o valor de evidência obtida após sua análise, CWi é o peso do controle de segurança e 4 é o valor máximo de evidência.

$$\overline{X} = \frac{\sum_1^n EVi \; x \; CWi}{\sum_1^n 4 \; x \; CWi} \quad (2)$$

3.3.1.3.*Análise Contextual*

A análise contextual utiliza as mesmas métricas que as análises *tradicional* e *ponderada*, mas introduz o conceito de perspectiva da organização, que define o nível de importância que a empresa atribui a cada controle de segurança. Ao introduzir a perspectiva organizacional, a análise contextual avalia não apenas a conformidade com os controles de segurança recomendados pelas normas internacionais. Ela também leva em conta as particularidades de cada organização. Assim, embora não totalmente alinhado com as normas, a empresa pode avaliar se suas prioridades estão sendo respeitadas.

A análise contextual adota a escala de Likert (LIKERT, 1932) para definir o nível de importância que a organização dá aos controles de segurança. Desta forma é possível medir as atitudes e conhecer o grau de conformidade do respondente com a afirmação dos controles de segurança, expressando com detalhes sua opinião e capturar a intensidade de seus sentimentos, onde:

- 5 - Totalmente de acordo. O controle de segurança é absolutamente relevante para a organização;
- 4 - Parcialmente de acordo. O controle de segurança é parcialmente relevante para a organização;
- 3 - Indeciso. Há dúvidas se o controle de segurança é relevante para a organização;
- 2 - Parcialmente em desacordo. O controle de segurança é parcialmente irrelevante;
- 1 - Totalmente em desacordo. O controle não tem relevância para a organização.

O nível de maturidade nesta abordagem é calculado através da Equação 3, onde n é o número de controles de segurança analisados, EVi é o valor de evidência obtida após sua análise, CWi é o peso do controle de segurança, OWi é o valor da importância que a organização atribui ao controle de segurança e 4 é o valor máximo de evidência.

$$\overline{X} = \frac{\sum_1^n EVi \; x \; CWi \; x \; OWi}{\sum_1^n 4 \; x \; CWi \; x \; OWi} \tag{3}$$

3.3.2. Níveis de Maturidade

O modelo de maturidade proposto nesta metodologia é composto por cinco níveis de maturidade, numerados numa escala de 0 a 4. Cada nível é um estágio evolutivo e tem um conjunto de metas de segurança relacionadas à configuração de um dado componente de um *data center*. Na Tabela 7, são apresentados os níveis de maturidade, descrevendo a escala numérica do nível de maturidade, a nomenclatura de cada nível e o percentual de controles de segurança atendidos.

Os intervalos dos níveis de maturidade foram definidos por uma margem de porcentagem para que fosse possível produzir um índice de maturidade, informando a qualidade de configuração do servidor, conforme proposto no trabalho de Muthukrishnan e Palaniappan (2016).

Tabela 7: Níveis de maturidade propostos nesta metodologia

Níveis de Maturidade	Nomenclatura	Controles Atendidos
0	Não Gerenciado (UM)	0-19,99 % dos controles
1	Inicialmente Gerenciado (IM)	20-39,99 % dos controles
2	Parcialmente Gerenciado (PM)	40-59,99 % dos controles
3	Largamente Gerenciado (WM)	60-79,99 % dos controles
4	Totalmente Gerenciado (FM)	80-100 % dos controles

Fonte: Elaborado pelo autor

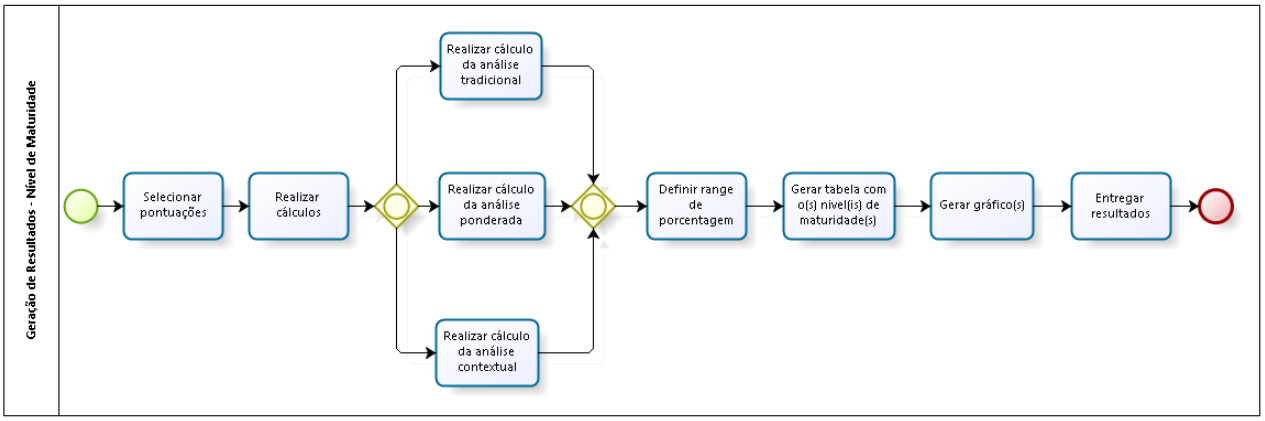
3.4. Geração de Resultados

Por fim, esta atividade tem como objetivo gerar relatórios que possam ser compreendidos tanto pelo responsável técnico como pela alta direção da organização. Como resultados, esta atividade é composta por dois componentes: o *nível de maturidade* e *programas de melhoria.* Esses componentes são apresentados a seguir.

3.3.3. Nível de Maturidade

Neste componente, informações quantitativas são apresentadas. Os gráficos apresentam as pontuações que foram obtidas com base em cada abordagem de avaliação utilizada. Além disso, são apresentados quadros com as porcentagens referentes a cada nível de maturidade e qual dimensão foi utilizada. Os passos deste componente são apresentados na Figura 4 e descritos a seguir.

Figura 4: Componente Nível de Maturidade da Atividade Geração de Resultados



Fonte: Elaborado pelo autor

- **Identificar pontuações**: neste passo são identificadas as pontuações que serão utilizadas em cada abordagem de avaliação, conforme apresentado na seção 3.3;
- **Realizar cálculos**: neste passo as pontuações são selecionadas conforme a abordagem de avaliação escolhida;
    - **Realizar cálculo da análise tradicional**: neste passo é utilizado o cálculo da análise tradicional conforme apresentado na seção 3.3.1.1;
    - **Realizar cálculo da análise ponderada**: neste passo é utilizado o cálculo da análise ponderada conforme apresentado na seção 3.3.1.2;

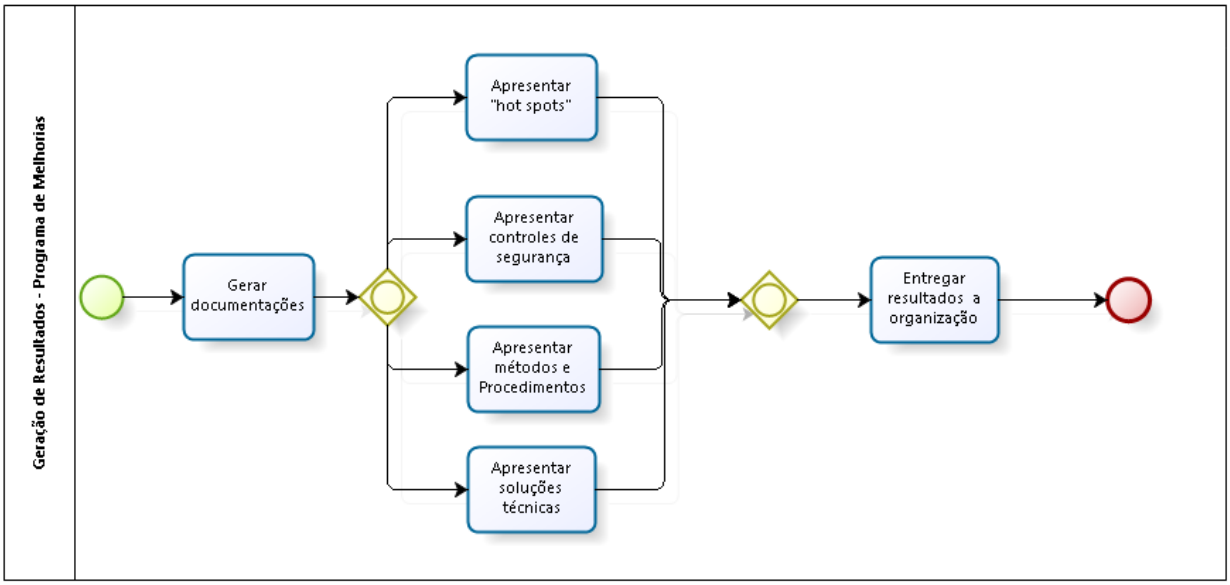
- **Realizar cálculo da análise contextual**: neste passo é utilizado o cálculo da análise contextual conforme apresentado na seção 3.3.1.3;

- **Definir *range* de porcentagem**: neste passo é definido o percentual da maturidade alcançada conforme seção 3.3.1 e Tabela 7;
- **Gerar tabela com o(s) nível (is) de maturidade:** neste passo é gerada uma tabela apresentando os níveis de maturidade alcançados pela organização avaliada, descrevendo as dimensões, abordagens de avaliação utilizadas e o percentual de controles atendidos;
- **Gerar gráfico(s)**: neste passo é (são) gerado(s) gráfico(s) apresentando as pontuações obtidas após a avaliação.
- **Entregar resultados**: neste passo é entregue a organização, os resultados quantitativos da avaliação da maturidade.

3.3.4. Programa de Melhorias

Neste componente são apresentados "*hot spot"* ou áreas relevantes para melhorar o estado atual de segurança. Além disso, é gerado um documento que deve conter um conjunto de controles de segurança, incluindo métodos e procedimentos para realização das melhorias necessárias e um guia de suporte para a equipe de segurança tomar decisões futuras e possíveis soluções.

Figura 5: Componente Programa de Melhorias da Atividade Geração de Resultados



Fonte: Elaborado pelo autor

- **Gerar documentações:** neste passo são gerados documentos para apoiar a equipe de segurança da organização a tomar decisões futuras;
    - **Apresentar "*hotspots*":** neste passo são apresentadas as áreas significativas da organização que necessitam de melhoria do estado de segurança do *data center;*
    - **Apresentar os controles de segurança:** neste passo são apresentados a organização a lista dos controles de segurança necessários para melhoria da segurança do *data center*;
    - **Apresentar métodos e procedimentos:** neste passo são apresentados os métodos e procedimentos necessários para melhorar o estado de segurança do *data center*;
    - **Apresentar soluções técnicas:** neste passo são apresentados possíveis soluções técnicas (se for o caso), para melhorar o estado de segurança do *data center.*
- **Entregar resultados:** neste passo é entregue à organização os resultados do programa de melhorias.

4. AVALIAÇÕES

Neste capítulo são apresentados os estudos de caso realizados para avaliar a utilização da metodologia proposta neste trabalho. Dois estudos de casos foram realizados utilizando todas as dimensões propostas. Visando validar a generalidade desta metodologia, foram avaliados servidores de diferentes fabricantes e com contextos distintos. No primeiro estudo de caso, descrito na Seção 4.1, são apresentados os passos e resultados no servidor de uma empresa privada que tem como foco o comércio alimentício, e tem servidores *Microsoft* em sua infraestrutura. O segundo estudo de caso, apresentado na Seção 4.2, faz uma avaliação de um servidor *GNU/Linux Ubuntu* que está hospedado num *data center* de um órgão público do governo do Estado de Pernambuco. Este servidor tem como foco prover serviços para funcionamento de uma rede social educacional.

4.1. Estudo de Caso 1

4.1.1. Visão Geral

A franquia desta empresa privada está presente nos cinco continentes e em mais de noventa países. A rede conta com mais de quatorze mil restaurantes ao redor do mundo e emprega mais de duzentos e cinquenta mil funcionários apenas nos Estados Unidos da América. No Brasil, são mais de noventa restaurantes distribuídos por estados de todo o país, atingindo o número de um milhão de pessoas consumindo os produtos por mês.

O servidor avaliado em uma das franquias da rede, localizada no Munícipio do Recife, capital de Pernambuco, é um ProLiant DL20 G9 830700-S05 / HP, tem o *Windows Server* 2012 R2 como sistema operacional na sua versão Standard, contendo duas unidades de disco rígido de 500GB e 8GB de memória RAM, além dos serviços e aplicações utilizados: *Software* para PDV (Point of Sale), *NCR Aloha* e dependências, *Teamviewer*, *Tight VNC*, *Aloha Configuration Center*, *Virtual Clone* e *Aloha Menu Lin*k (Software de Cadastro).

4.1.2. Seleção das Dimensões

A avaliação do servidor foi realizada usando todas as dimensões propostas neste trabalho: (*Server Business Compliace* – SBC, *Server Application Security* – SAS, *Server System Operating Security* – SOS e *Server Security Preserving* - SSP). As avaliações das dimensões foram separadas em turnos, uma pela manhã e outra pela tarde. Dessa forma toda a avaliação durou dois dias corridos. Essa escala foi determinada pelo gestor de tecnologia responsável pelos servidores, considerando as necessidades da organização no momento.

4.1.3. Avaliação da Maturidade

Nesta subseção é apresentada a aplicação das três abordagens de avaliação propostas (seção 3.3.1.1 análise tradicional, seção 3.3.1.2 análise ponderada e seção 3.3.1.3 análise contextual). Durante a análise tradicional, foram coletadas evidências da implementação de cada controle de segurança de todas as dimensões avaliadas:

- Artefatos intangíveis (dinâmicos) - arquivos de *log* do servidor *Windows*, verificando cada registro de software, verificação da ferramenta *Event Viewer* da *Microsoft*;
- Artefatos intangíveis (estáticos) – arquivos de configuração, arquivos de registros do *Windows Server*, padrões de software e softwares produzidos por terceiros.

Finalmente foi realizada uma análise documental com a detentora da franquia e o fornecedor do servidor visando à verificação de artefatos tangíveis - documentações de softwares, prestadores de serviços, informações sobre o negócio, incluindo regras, políticas e funcionários, utilizados para certificar a precisão das informações coletadas anteriormente.

Durante a análise ponderada, foram atribuídos pesos a cada controle de segurança de todas as dimensões utilizadas. Os controles de segurança presentes em ambas as normas (ISO 27002 e NIST 800-53) receberam peso 2. Os restantes dos controles foram ponderados com valor 1.

Para efeitos da análise contextual, foram realizadas entrevistas com o gerente de TI da empresa. A partir dos dados coletados, foi possível identificar quais controles de segurança são mais relevantes para a organização, dentre os quais se destacam: Restrições de Acesso à Informação, Segurança no Software de Login, Software de Gerenciamento de Senhas, Utilitários de Software Privilegiados, Controle no Código Fonte do Software, Criptografia nos Dados Transferência, Notificação de Falha de Segurança no Software. As pontuações obtidas através das três abordagens de avaliação (tradicional, ponderada e contextual) neste estudo de caso são apresentadas no Apêndice B.

4.1.4. Geração dos Resultados

Nesta subseção apresentamos os resultados avaliados através do estudo de caso. Foram analisadas todas as dimensões e suas famílias respectivamente (Figuras 6, 7, 8 e 9):

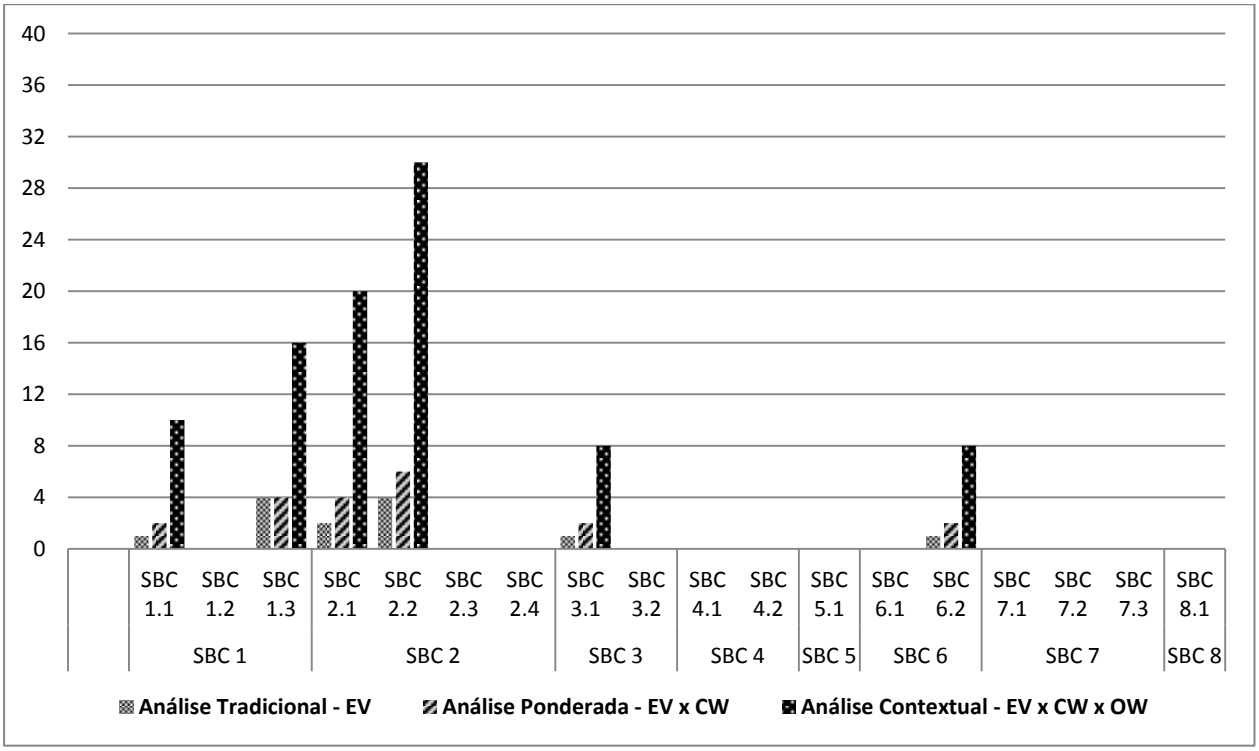
- *Server Business Compliance* – SBC-1, SBC-2, SBC-3, SBC-4, SBC-5, SBC-6, SBC-7, SBC-8;
- *Server Security Operating System* – SOS-1, SOS-2, SOS-4, SOS-5, SOS-6;
- *Server Application Security* – SAS-1, SAS-2, SAS-3, SAS-4, SAS-5, SAS-6;
- *Server Security Preserving* – SSP-1, SSP-2, SSP-3, SSP-4, SSP-5.

4.1.4.1. *Definição do Nível de Maturidade*

As barras representam o valor calculado para cada controle usando uma abordagem de avaliação específica. Quando a barra não aparece para um determinado controle, indica que não existe evidência de que o controle foi implementado.

A Figura 6 apresenta os quantitativos do primeiro estudo de caso utilizando as três abordagens de avaliação (tradicional, ponderada e contextual) utilizando a dimensão *Server Business Compliance*.

Figura 6: Estudo de Caso 1 - Resultados na Dimensão Server Business Compliance**.**



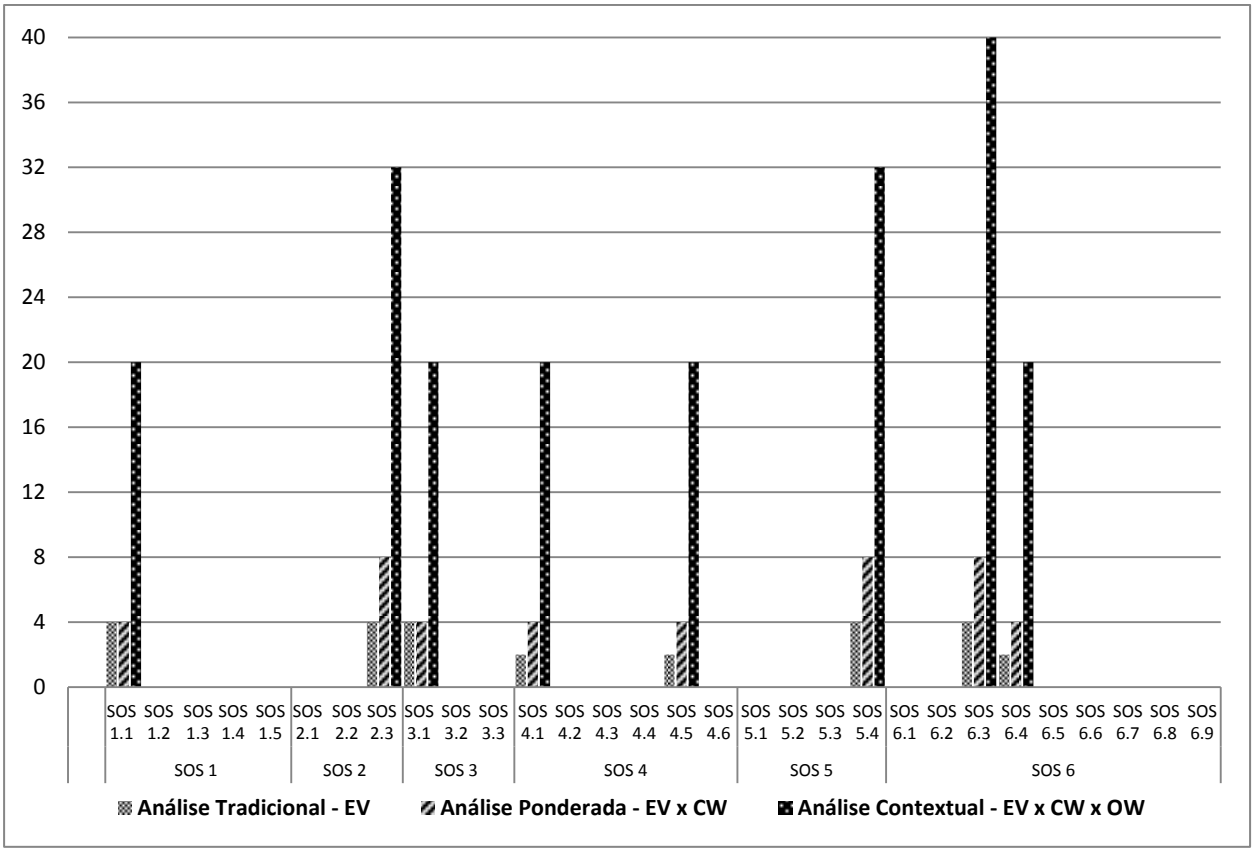
Fonte: Elaborado pelo autor

- Análise de Tradicional - O valor máximo da pontuação na análise tradicional seria 72. Mas a organização obteve 13 pontos, indicando que em porcentagem obteve 18% nesta abordagem. Isso representa um nível de maturidade 0 ou nível Não Gerenciado (UM);
- Análise Ponderada - Os resultados indicam 16% de conformidade com os controles de segurança da dimensão analisada. No entanto, mesmo existindo um decréscimo de 2% na pontuação, o nível de maturidade é o mesmo que o calculado através da análise tradicional.
- Análise Contextual - Esta análise revelou um fato interessante. A empresa considerou alguns controles de segurança como mais importantes, mas não os implementou.

Portanto, sua pontuação diminuiu novamente para 15%, continuando seu nível de maturidade em 0, que é um nível Não Gerenciado (UM).

A Figura 7 apresenta os quantitativos do primeiro estudo de caso utilizando as três abordagens de avaliação (tradicional, ponderada e contextual) utilizando a dimensão *Server Security Operating System.*

Figura 7: Estudo de Caso 1 - Resultados na Dimensão Server Security Operating System



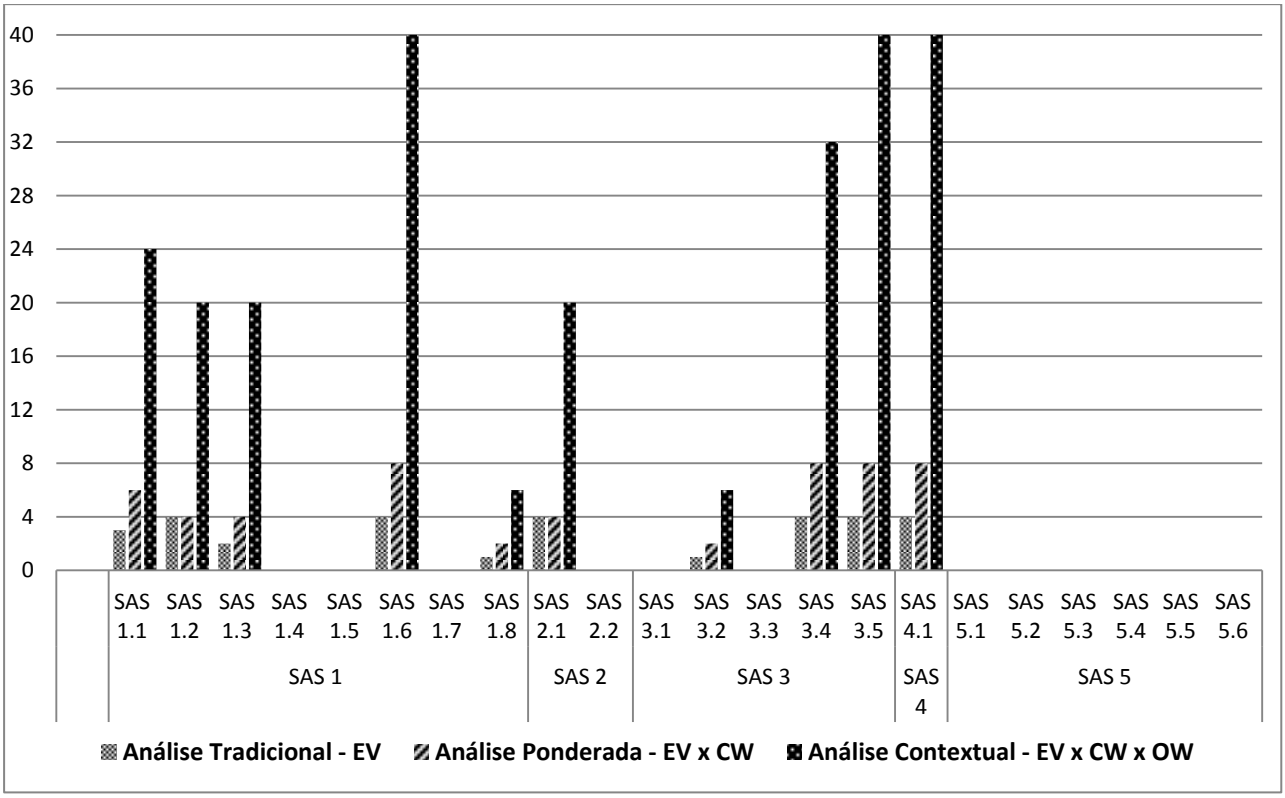
Fonte: Elaborado pelo autor

- Análise Tradicional - O valor máximo da pontuação na análise de evidências poderia chegar a 120. Porém a organização obteve 26 pontos, indicando que em porcentagem obteve 21% nesta abordagem. Isso representa um nível de maturidade 1 ou nível Inicialmente Gerenciado (IM);
- Análise Ponderada - Os resultados nesta abordagem indicam 19%. No entanto, houve um decréscimo de 2% na pontuação em relação à análise tradicional, o que ocasionou queda no nível de maturidade, passando para o nível de maturidade 0 ou nível Não Gerenciado (UM);
- Análise Contextual – Os resultados nesta abordagem indicam 24%, chegando ao nível de maturidade Inicialmente Gerenciado (IM). O aumento de 3% em relação a análise

tradicional e 5% em relação a análise ponderada dar-se pela empresa obter as melhores pontuações na coleta de evidências nos controles que obtiveram maiores pontuações na análise da importância que a organização atribuiu a cada controle de segurança.

A Figura 8 apresenta os quantitativos do primeiro estudo de caso utilizando as três abordagens de avaliação (tradicional, ponderada e contextual) utilizando a dimensão *Server Application Security.*

Figura 8: Estudo de Caso 1 - Resultados na Dimensão Server Application Security

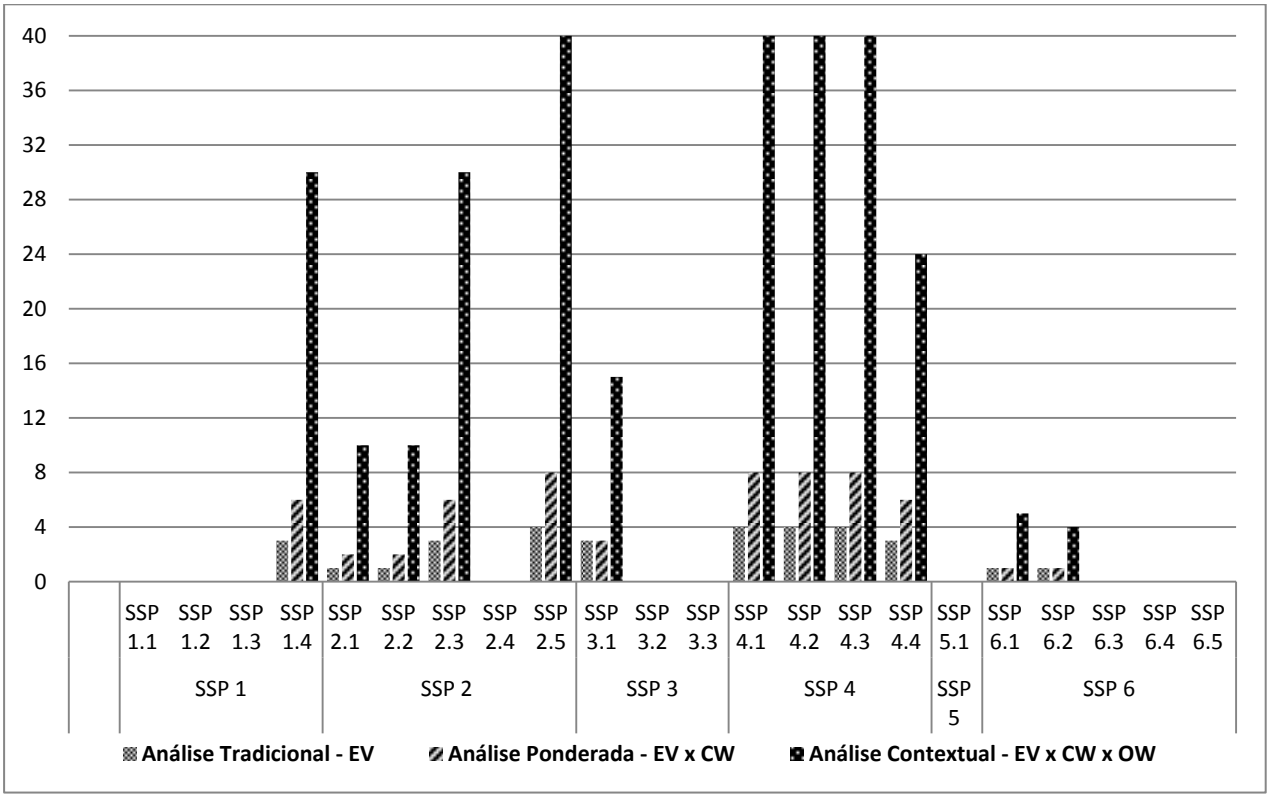


Fonte: Elaborado pelo autor

- Análise Tradicional - Nesta abordagem a empresa obteve 31 pontos de 88 possíveis, indicando que em porcentagem obteve 35%. Isso representa um nível de maturidade 1 ou nível Inicialmente Gerenciado (IM);
- Análise Ponderada - Os resultados nesta abordagem indicam também 35%. Representando um nível de maturidade 1 ou nível Inicialmente Gerenciado (IM);
- Análise Contextual – Os resultados nesta abordagem indicam 36%, chegando ao mesmo nível de maturidade das abordagens anteriores. O aumento de 1% dar-se pela empresa obter as melhores pontuações na coleta de evidências em alguns controles que obtiveram maiores pontuações na análise da importância que a organização atribuiu.

A Figura 9 apresenta os quantitativos do primeiro estudo de caso utilizando as três abordagens de avaliação (tradicional, ponderada e contextual) utilizando a dimensão *Server Security Preserving.*

Figura 9: Estudo de Caso 1 - Resultados na Dimensão Server Security Preserving



Fonte: Elaborado pelo autor

- Análise Tradicional - A organização nesta abordagem obteve 32 pontos de 88 possíveis, indicando que em porcentagem obteve 36%. Representando um nível de maturidade 1 ou nível Inicialmente Gerenciado (IM);
- Análise Ponderada - Os resultados nesta abordagem indicam o crescimento de 5% em relação à abordagem anterior, atingindo 41%. Representando um nível de maturidade 2 ou nível Parcialmente Gerenciado (PM);
- Análise Contextual – Os resultados nesta abordagem indicam 41%, chegando ao mesmo nível de maturidade da análise ponderada.

A Tabela 8 descreve os dados quantitativos relacionados às dimensões avaliadas, utilizando as três abordagens de avaliação, mostrando suas porcentagens e seu nível de maturidade.

Tabela 8: Quantitativos dos Resultados – Estudo de Caso 1

Dimensão	**Abordagem de Avaliação**	**Porcentagem**	**Nível de Maturidade**
Server Business Compliance	Análise Tradicional	18%	Não Gerenciado - UM
	Análise Ponderada	16%	Não Gerenciado - UM
	Análise Contextual	15%	Não Gerenciado - UM
Server Security Operating System	Análise Tradicional	21%	Inicialmente Gerenciado - IM
	Análise Ponderada	19%	Não Gerenciado - UM
	Análise Contextual	24%	Inicialmente Gerenciado - IM
Server Application Security	Análise Tradicional	35%	Inicialmente Gerenciado - IM
	Análise Ponderada	35%	Inicialmente Gerenciado - IM
	Análise Contextual	36%	Inicialmente Gerenciado - IM
Server Security Preserving	Análise Tradicional	36%	Inicialmente Gerenciado - IM
	Análise Ponderada	41%	Parcialmente Gerenciado - PM
	Análise Contextual	41%	Parcialmente Gerenciado - PM

Fonte: Elaborado pelo autor

4.1.4.2. *Programa de Melhorias*

Foi identificado que, embora a empresa não tenha implementado vários dos controles de segurança, eles ainda são relevantes para a organização. Esta subseção apresenta no quadro 5 as áreas relevantes que necessitam de melhorias ("*hot spots*").

O grau de criticidade e urgência são determinados pelas células com um plano de fundo destacado em cinza, o que indica pontuações muito baixas ou nulas nesta avaliação.

Quadro 5: Estudo de Caso 1 - Áreas Críticas no *Data Center*

Documentações e Conformidade com o Negócio	**Sistema Operacional**	**Softwares Utilizados**	**Monitoramento do *Data Center***
Análise Crítica das Políticas de Segurança	Segurança na Implantação	Instalações Seguras dos Softwares	Gestão de Incidentes
Privacidade nas Informações Pessoais	Atualização de Pacthes	Recursos do *Data Center*	Monitoramento Automatizado
Expertise Profissional	Controle de Acesso	Controle de Acesso aos Softwares	Auditoria
Políticas de Controle de Acesso	Autenticação de Usuários	Utilização de Antivírus	Backup
Procedimentos de Segurança no *Data Center*	Segurança na Rede	-	-
Arquitetura de Segurança do *Data Center*	-	-	-
Classificação das Informações do *Data Center*	-	-	-

Fonte: Elaborado pelo autor

Além disso, no Apêndice C deste trabalho, estão descritos todas as recomendações para melhorar o ambiente do *data center*, (soluções técnicas e documentais) para que o nível de maturidade possa atingir níveis maiores e que haja a possibilidade de a empresa ter um guia de suporte para a equipe de segurança ou tecnologia tomar decisões futuras.

4.1.5. Considerações Finais

Após os resultados, a organização avaliou que a metodologia se mostrou útil, que agrega valor e pode gerar informações importantes para o time de segurança, promovendo melhorias na segurança do *data center*. Sendo assim, a franqueada pretende num futuro próximo avaliar as outras lojas no estado e sugerir a detentora da franquia que sejam realizadas essas avaliações nas

outras lojas pelo Brasil, bem como treinamento para os profissionais de tecnologia para que as medidas de melhoria na segurança dos servidores sejam implementadas.

4.2. Estudo de Caso 2

4.2.1. Visão Geral

O segundo estudo de caso analisou uma comunidade de software livre que desenvolve um ambiente de aprendizagem de código aberto, idealizado por pesquisadores do centro de informática da Universidade Federal de Pernambuco para proporcionar meios de colaboração entre alunos e professores utilizando diferentes mídias e tipos de interação virtual.

Este estudo de caso avalia a configuração de segurança de um servidor GNU Linux Ubuntu 14.04 hospedado no *data center* de uma organização pública brasileira. Este servidor suporta os serviços de execução de uma rede educacional social com mais de 40.000 usuários registrados.

Os seguintes serviços e aplicativos estão instalados no servidor: *mongodb, collectd, nginx, unicorn_rails, monit, java, ssh, mysqld, ruby*.

4.2.2. Seleção das Dimensões

A avaliação do servidor que hospeda os serviços do *Openredu* também foi realizada usando todas as dimensões propostas nesta dissertação (*Server Business Compliace* – SBC, *Server Application Security* – SAS, *Server System Operating Security* – SOS e *Server Security Preserving* - SSP).

As avaliações das dimensões eram realizadas semanalmente, ou seja, apenas uma dimensão era avaliada. Essa avaliação ocorreu às terças-feiras após as 18:00 no horário de Brasília.

A avaliação inteira durou em torno de um mês. Essa escala foi definida pelo líder técnico, que é responsável, tanto pela implantação da aplicação do *Openredu* nos servidores, além de ser o líder da equipe de desenvolvimento.

4.2.3. Avaliação da Maturidade

Assim como no primeiro estudo de caso, esta subseção descreve a aplicação das três abordagens de avaliação propostas (tradicional, ponderada e contextual). Durante as análises de evidências, foram coletadas evidências da implementação de cada controle de segurança de todas

as dimensões avaliadas. Sempre que possível o servidor era acessado remotamente usando o serviço ssh (*secure shell*), para que fosse possível comprovar as evidências.

- Artefatos intangíveis (dinâmicos) - arquivos de log do servidor localizados no diretório /var no Ubuntu, verificando cada registro dos softwares;
- Artefatos intangíveis (estáticos) – arquivos de configuração, padrões de software, que vêm em pacotes pré-definidos a partir do servidor ou software produzido por terceiros.
- Artefatos tangíveis - documentações de softwares, prestadores de serviços, informações sobre o negócio, incluindo regras, políticas e colaboradores, utilizados para certificar a precisão das informações também foram verificadas. Por se tratar de uma comunidade de software livre, o *Openredu,* em termos de documentações mostrou-se limitado, o que dificultou a avaliação.

Com base na análise de similaridade entre as normas ISO 27002 e NIST 800-53, ponderamos os controles de segurança das dimensões utilizadas. Os controles de segurança recomendados por ambas as normas foram ponderados com valor 2. Os outros foram ponderados com valor 1.

Para fins de análise contextual, foram realizadas entrevistas com o líder técnico do *Openredu* para definir a importância que a comunidade dá aos controles de segurança avaliados.

As pontuações obtidas através das três abordagens de avaliação (tradicional, ponderada e contextual) neste estudo de caso são apresentadas no Apêndice B.

4.2.4. Geração dos Resultados

Esta subseção apresenta os resultados avaliados através do segundo estudo de caso. Foram analisadas todas as dimensões e suas famílias (Figuras 10, 11, 12 e 13):

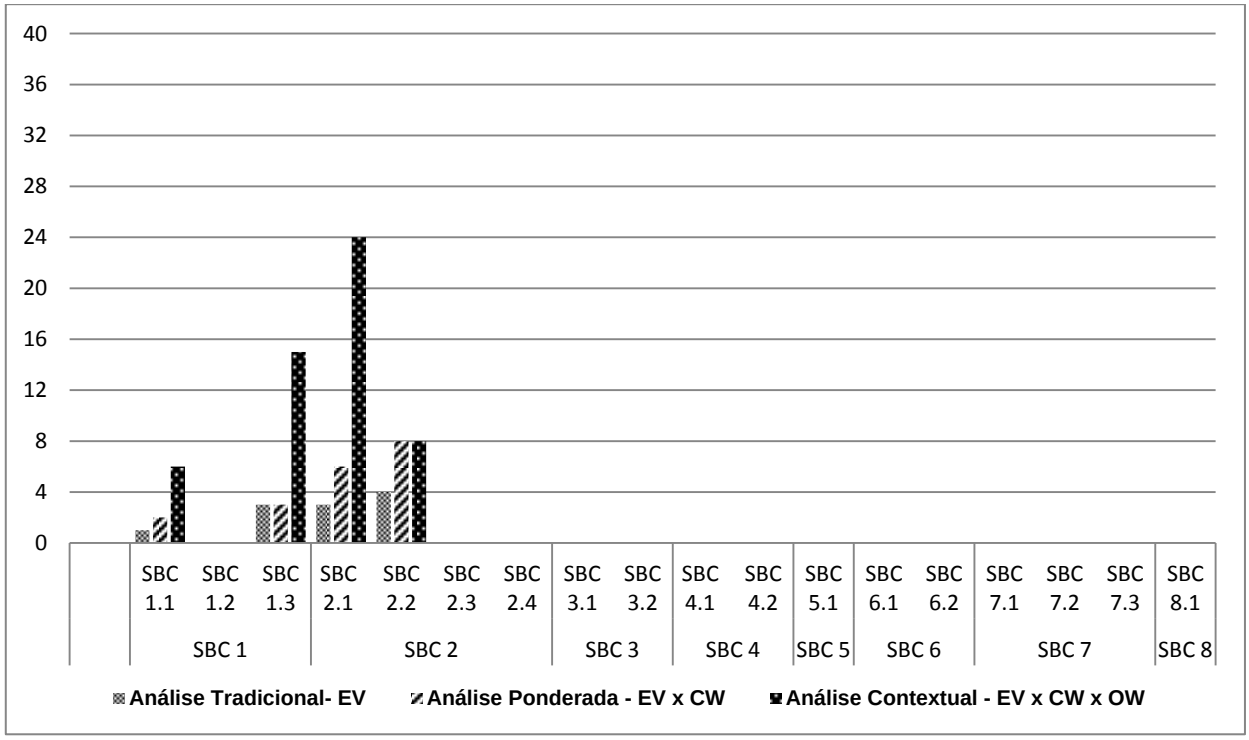
- *Server Business Compliance* – SBC-1, SBC-2, SBC-3, SBC-4, SBC-5, SBC-6, SBC-7, SBC-8;
- *Server Security Operating System* – SOS-1, SOS-2, SOS-4, SOS-5, SOS-6;
- *Server Application Security* – SAS-1, SAS-2, SAS-3, SAS-4, SAS-5, SAS-6;
- *Server Security Preserving* – SSP-1, SSP-2, SSP-3, SSP-4, SSP-5.

4.2.4.1. *Definição do Nível de Maturidade*

Assim como no primeiro estudo de caso, as barras representam o valor calculado para cada controle usando uma abordagem de avaliação específica. Quando a barra não aparece para um determinado controle, indica que não existe evidência de que o controle foi implementado.

A Figura 10 apresenta os quantitativos do segundo estudo de caso utilizando as três abordagens de avaliação (tradicional, ponderada e contextual) na dimensão *Server Business Compliance.*

Figura 10: Estudo de Caso 2 - Resultados na Dimensão Server Business Compliance



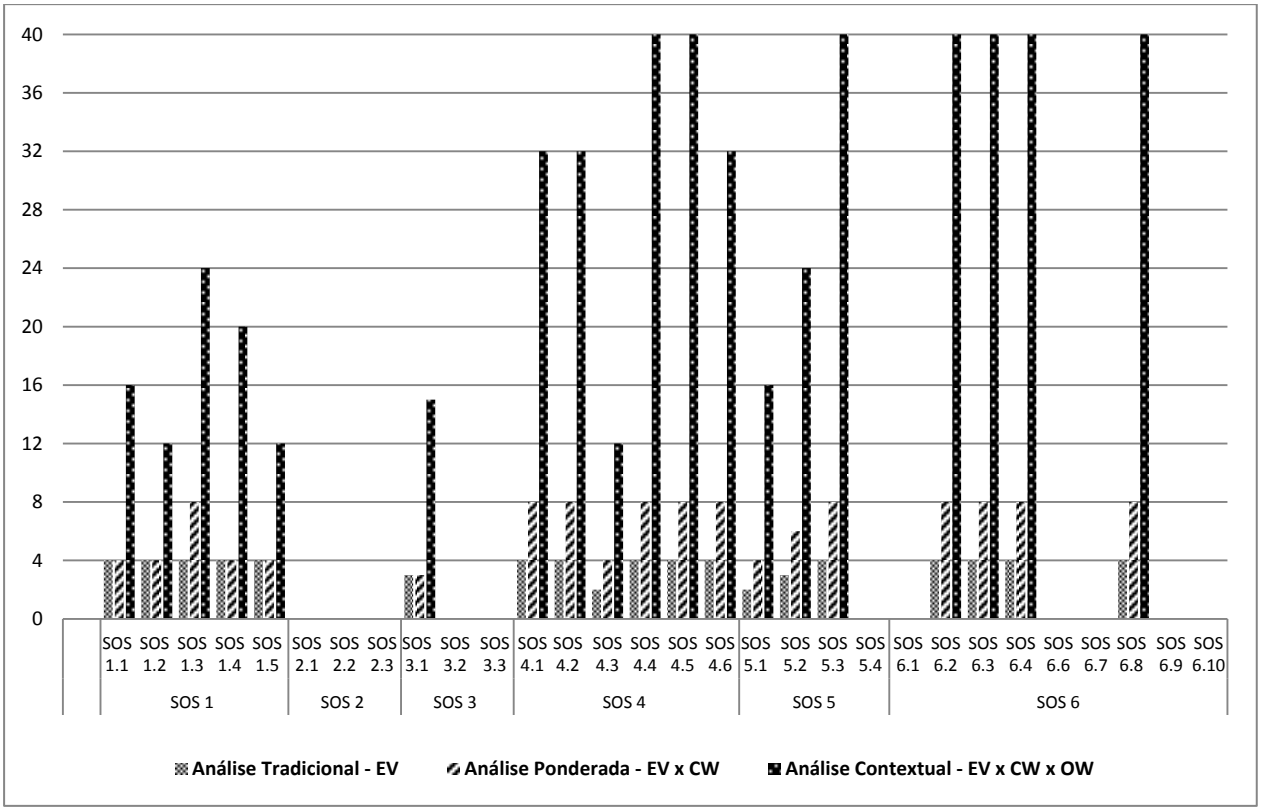
Fonte: Elaborado pelo autor

- Análise Tradicional - A organização nesta abordagem obteve 11 pontos de 72 possíveis, indicando que em porcentagem obteve 15%. Representando um nível de maturidade 0 – Não Gerenciado (UM);
- Análise Ponderada - Os resultados nesta abordagem indicam o decrescimento de 1% em relação à abordagem anterior, atingindo 14%. Representando o mesmo nível de maturidade 0 – Não Gerenciado;
- Análise Contextual – Os resultados nesta abordagem indicam 11%, chegando ao mesmo nível de maturidade das abordagens anteriores. Nesta abordagem foi identificado que a

organização não priorizou os controles com maiores pontuações obtidos da análise tradicional. O que ocasionou baixa de 4% da tradicional e 3% da ponderada, respectivamente.

A Figura 11 apresenta os quantitativos do segundo estudo de caso utilizando as três abordagens de avaliação (tradicional, ponderada e contextual) na dimensão *Server Security Operating System.*

Figura 11: Estudo de Caso 2 - Resultados na Dimensão Server Security Operating System



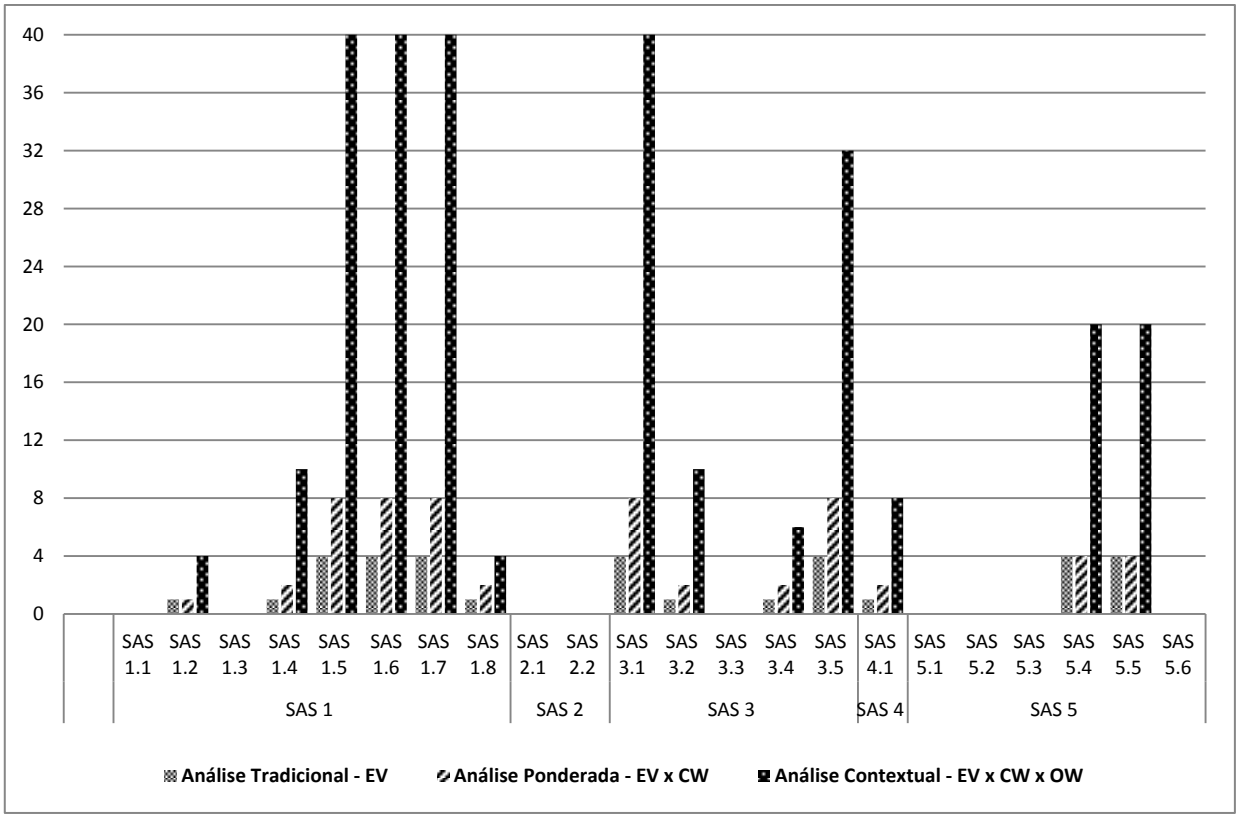
Fonte: Elaborado pelo autor

- Análise Tradicional - O valor máximo da pontuação na análise de evidências poderia chegar a 120. Porém, a organização obteve 70 pontos, indicando que em porcentagem obteve 58% nesta abordagem. Isso representa um nível de maturidade 2 ou nível Parcialmente Gerenciado (PM);
- Análise Ponderada - Os resultados nesta abordagem indicam também 58%, chegando ao mesmo nível de maturidade que a abordagem anterior;
- Análise Contextual – Os resultados nesta abordagem indicam 60%, chegando ao nível de maturidade 3 ou nível Largamente Gerenciado (WM). Os resultados indicam que a

organização está consistentemente priorizando a implementação de controles de segurança que a empresa classifica com pontuação mais alta.

A Figura 12 apresenta os quantitativos do segundo estudo de caso utilizando as três abordagens de avaliação (tradicional, ponderada e contextual) na dimensão *Server Application Security.*

Figura 12: Estudo de Caso 2 - Resultados na Dimensão Server Application Security

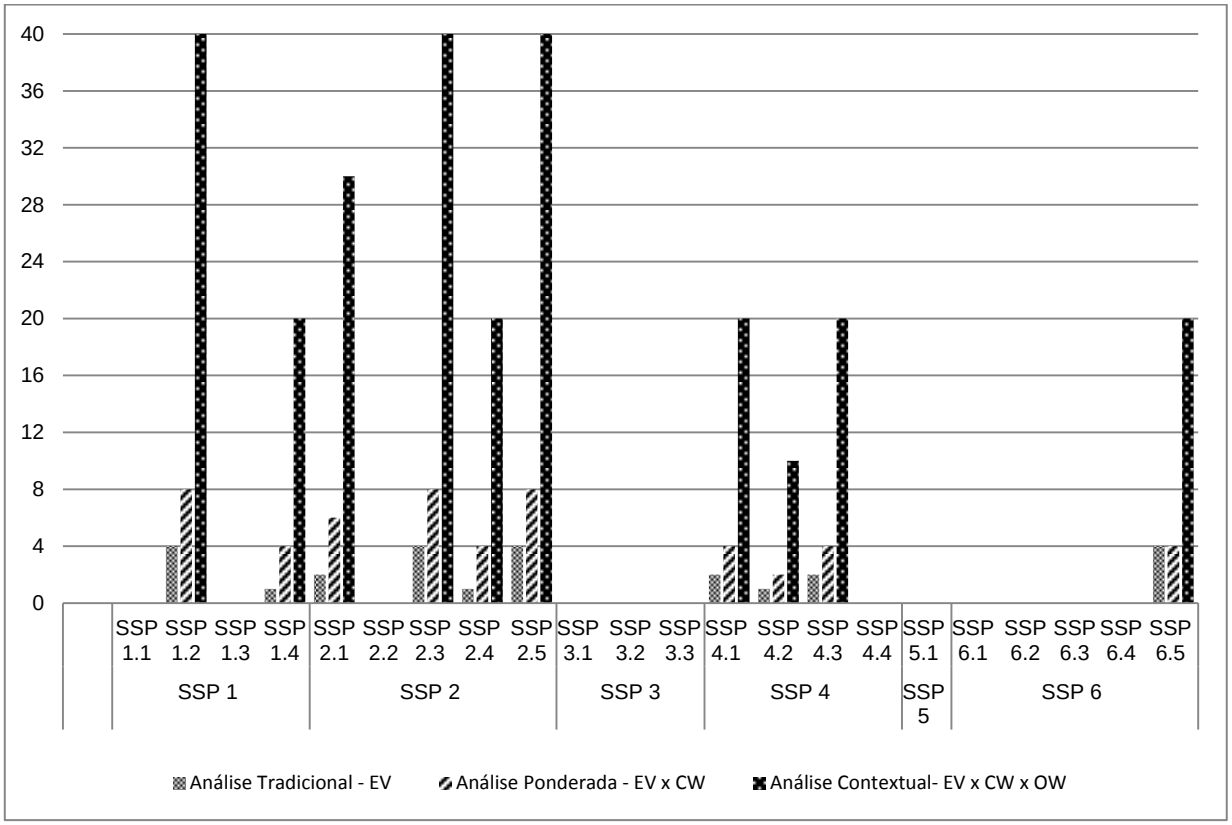


Fonte: Elaborado pelo autor

- Análise Tradicional - A organização nesta abordagem obteve 34 pontos de 88 possíveis, indicando que em porcentagem obteve 38%. Isso representa um nível de maturidade 1 ou nível Inicialmente Gerenciado (IM);
- Análise Ponderada - Os resultados nesta abordagem indicam também 38%, representando um nível de maturidade 1 ou nível Inicialmente Gerenciado (IM);
- Análise Contextual – Os resultados nesta abordagem indicam 43%, chegando ao nível de maturidade 2 ou nível Parcialmente Gerenciado (PM).

A Figura 13 apresenta os quantitativos do segundo estudo de caso utilizando as três abordagens de avaliação (tradicional, ponderada e contextual) na dimensão *Server Application Security.*

Figura 13: Estudo de Caso 2 - Resultados na Dimensão Server Security Preserving



Fonte: Elaborado pelo autor

- Análise Tradicional - A organização nesta abordagem obteve 26 pontos de 88 possíveis, indicando que em porcentagem obteve 28%. Representando um nível de maturidade 1 - Inicialmente Gerenciado (IM);
- Análise Ponderada - Os resultados nesta abordagem indicam o crescimento de 7% em relação à abordagem anterior, atingindo 36%. Representando o mesmo nível de maturidade;
- Análise Contextual – Os resultados nesta abordagem indicam 40%, chegando ao nível de maturidade 2 ou nível Parcialmente Gerenciado – (PM). Desta forma o resultado aponta que a organização priorizou os controles de segurança com maiores pontuações.

A Tabela 9 descreve os dados quantitativos relacionados às dimensões avaliadas, utilizando as três abordagens de avaliação, mostrando suas porcentagens e seu nível de maturidade.

Tabela 9: Quantitativos dos Resultados – Estudo de Caso 2

Dimensão	**Abordagem de Avaliação**	**Porcentagem**	**Nível de Maturidade**
Server Business Compliance	Análise Tradicional	15%	Não Gerenciado - UM
	Análise Ponderada	14%	Não Gerenciado - UM
	Análise Contextual	11%	Não Gerenciado - UM
Server Security Operating System	Análise Tradicional	58%	Parcialmente Gerenciado - PM
	Análise Ponderada	58%	Parcialmente Gerenciado - PM
	Análise Contextual	60%	Largamente Gerenciado - WM
Server Application Security	Análise Tradicional	38%	Inicialmente Gerenciado - IM
	Análise Ponderada	38%	Inicialmente Gerenciado - IM
	Análise Contextual	43%	Parcialmente Gerenciado - PM
Server Security Preserving	Análise Tradicional	28%	Inicialmente Gerenciado - IM
	Análise Ponderada	36%	Inicialmente Gerenciado - IM
	Análise Contextual	40%	Parcialmente Gerenciado - PM

Fonte: Elaborado pelo autor

4.2.4.2. *Programa de Melhorias*

Foram identificadas várias lacunas, principalmente nos controles de segurança que têm como foco a conformidade com o negócio.

O Quadro 6 apresenta as áreas relevantes que precisam de atenção para melhorar a segurança da organização, tanto em aspectos documentais como técnicos.

O grau de criticidade e urgência são determinados pelo plano de fundo destacado em cinza, o que indica pontuações muito baixas ou nulas nesta avaliação.

Quadro 6: Estudo de Caso 2 - Áreas Críticas no *Data Center*.

Documentações e Conformidade com o Negócio	**Sistema Operacional**	**Softwares Utilizados**	**Monitoramento do *Data Center***
Análise Crítica das Políticas de Segurança	Atualização de Pacthes	Instalações Seguras dos Softwares	Gestão de Incidentes
Privacidade nas Informações Pessoais	Controle de Acesso	Recursos do *Data Center*	Monitoramento Automatizado
Expertise Profissional	Autenticação de Usuários	Controle de Acesso aos Softwares	Auditoria
Políticas de Controle de Acesso	Segurança na Rede	Transferência de Arquivos	Backup
Procedimentos de Segurança no *Data Center*		Relatórios de Segurança	Redundância de Servidores
Arquitetura de Segurança do *Data Center*	-	-	Testes de Segurança
Classificação das Informações do *Data Center*	-	-	-

Fonte: Elaborado pelo autor

Estão descritos, no Apêndice C deste documento, todos os detalhes dos pontos relevantes para que a organização possa atingir níveis maiores de maturidade, tendo um guia de suporte que auxilie a equipe de segurança ou tecnologia em decisões futuras.

4.2.5. Considerações Finais

Após a avaliação e resultados, a equipe da comunidade de software livre decidiu criar posteriormente uma equipe de colaboradores na área de segurança da informação para mitigar os erros e omissões identificados no programa de melhoria. Desta forma, acredita-se que a metodologia se tornou útil para avaliar o servidor que a comunidade de software livre utiliza e contribuir com futuras tomadas de decisões.

4.3. Análise da Aplicabilidade da Metodologia

Esta seção apresenta considerações finais quanto à aplicabilidade da metodologia em ambos os estudos de caso. Nas subseções a seguir, são apresentados possíveis conflitos das políticas de segurança desta metodologia que podem impactar nas atividades técnicas ou regras de negócio. Desta forma, dois pontos cruciais foram identificados:

1. Alguns controles na análise contextual obtiveram pontuações baixas, já que para as organizações eles não tinham relevância, porém as normas ISO 27002 (ISO/IEC 27002, 2013) e NIST 800-53 (NIST, 2014b), apontavam como importantes, e em nível de segurança, a falta de implementação destes controles pode gerar riscos à organização.
2. Alguns controles nas entrevistas da análise contextual obtiveram pontuações altas, porém, esses controles acabam por impactar nas regras de negócio da empresa.

4.3.1. Conflitos no Estudo de Caso 1

4.3.1.1. Adoção do *Active Diretory* (AD) no *Windows Server* 2012 R2

Conforme apresentado na Seção 4.1 deste trabalho, o servidor avaliado no primeiro estudo de caso funciona na plataforma *Microsoft.* As regras de negócio desta empresa valem para todas as lojas da rede franqueada.

Segundo o gerente de TI, as implementações dos controles *SOS 4.3 - Criação de Grupos de Usuário, SOS 4.4 - Renomear as Contas de Administrador, SOS 4.6 - Remoção de Contas Padrão do Sistema,* esses controles apoiam a criação de políticas através de GPO's (Groups Policies) que atuam sob domínios de uma rede *Microsoft*.

Os controles *SOS 6.9 - Segurança na Resolução de Nomes (Autoritativo) e SOS 6.10 - Segurança na Resolução de Nomes (Recursivo)* que apoiam a segurança em servidores de DNS

(*Domain Name System*) tornam-se impossíveis no atual momento. A detentora da franquia tem em contrato a utilização dos softwares *NCR Aloha*, *Aloha Menu Lin*k (Software de Cadastro) e *Aloha Configuration Center* que não funcionam corretamente em domínios de rede de computadores.

Outro impacto, é que todas as lojas da franquia não estão autorizadas a configurar servidores de domínio por determinação de cláusula de contrato com a fornecedora do software *NCR Aloha*. Desta forma, isso resulta no impedimento de diversos benefícios para a organização: sistema centralizado, unindo segurança; disponibilidade de recursos; administração simplificada; políticas administrativas; extensibilidades dos objetos criados (usuários, impressoras, unidades organizacionais); escalabilidade; sistemas de busca e replicação das informações.

4.3.1.2. Utilização de Antivírus

Conforme mencionado anteriormente, os softwares *NCR Aloha*, *Aloha Menu Lin*k (Software de Cadastro) e *Aloha Configuration Center* não funcionam numa de rede com base em nomes de domínios. Outro conflito encontrado foi na utilização de softwares antivírus. Existe uma lista de softwares antivírus que bloqueam os softwares da NCR. Sendo assim, no servidor não existe antivírus instalado.

Acredita-se que após a entrega dos resultados, esse conflito possa ser revisto em contratos entre a detentora da franquia e seus fornecedores de software. A lista de softwares antivírus não foi disponibilizada para o gerente de TI por força de contrato.

Em resumo, os controles *SAS 5.1 - Instalação de Software Antivírus, SAS 5.2- Atualização de Software Antivírus,* e *SAS 5.3 - Execução de Software Antivírus* nesta organização não foram implementados, o que, com base nas normas que apoiam os controles, torna-se uma grande lacuna de segurança, aumentando os riscos de *malware*, ou até mesmo ataques de *ransomware* no servidor.

Por fim, acredita-se que possam existir outras franquias que tenham problemas similares relacionados a sistemas antigos que não estão em conformidade com políticas de seguranças atuais. Sendo assim, acredita-se que esta metodologia possa ser usada em outras empresas.

4.3.2. Conflitos no Estudo de Caso 2

4.3.2.1. Informações Detalhadas sobre o *Data Center*

Conforme apresentado na Seção 4.2 deste trabalho, o servidor avaliado no segundo estudo de caso funciona na plataforma GNU/Linux Ubuntu.

Por se tratar de uma plataforma *opensource*, e manter seus serviços num *data center* de um órgão público, o *comunidade de* software livre acaba entrando em conflito com alguns controles, por exemplo: *SBC 1.2 - Análise Crítica das Políticas para Configuração de Segurança do Data Center, SBC 2.3 - Privacidade nas Informações Pessoais. SBC 3.1 - Seleção dos Profissionais, SBC 3.2 - Termos e Condições de Contrato, SBC 5.1 - Políticas de Controle de Acesso, SBC 7.2 - Políticas e Procedimentos de Manutenção do Data Center, SBC 7.3 - Políticas e Procedimentos de Avaliação de Risco de Configuração do Data Center e SBC 8.1 - Informação da Arquitetura de Segurança do Data Center.* Os controles citados acima entram em conflito pois não foi encontrado acordos e contratos de uso e documentações entre a comunidade de software livre e o proprietário do data center que descreva a adoção desses controles.

Com base nos controles desta metodologia, os responsáveis pela plataforma educacional têm sérias dificuldades em descrever as informações sobre as evidências de cada controle citado acima. Durante a avaliação foi identificado que o órgão público apenas hospedou os serviços no servidor, entretanto não foram disponibilizadas quaisquer documentações relacionadas com as preocupações de segurança já citadas. Em resumo, o órgão público responsável pelo *data center* não se mostrou interessado em detalhar seu modelo de negócio ou documentações que comprovassem a adoção dos controles. Assim, é nítido o conflito com os controles desta metodologia, e que os responsáveis pela própria plataforma possam obter informações claras sobre o *data center*.

4.3.2.2. Informações sobre Procedimentos do *Data Center*

Outro ponto que está em conflito consiste nos procedimentos de segurança do *data center:* controles *SSP 1.1 - Responsabilidades e Procedimentos no Data Center, SSP 1.3 - Avaliação e Decisão dos Eventos de Segurança do Data Center*. Por se tratar de um órgão público, a administração *data center* e seus serviços de tecnologia são terceirizados, ou seja, os procedimentos estão (por força de contrato entre a terceirizada e a empresa pública) com a empresa que administra o *data center*. Desta forma não foi possível identificar a adoção desses controles, nem mesmo se houve interesse da empresa terceirizada em fornecer essas informações.

5. TRABALHOS RELACIONADOS

Neste capítulo são apresentados trabalhos que são relacionados com esta dissertação, com base na revisão da literatura, apresentandoa o estado da arte referente a modelos de maturidade de segurança da informação. Para facilitar a análise das contribuições dos trabalhos relacionados foram escolhidos dois aspectos para orientar a apresentação: *1) Processos de Segurança da Informação; 2) Sistemas de Gerenciamento de Segurança da Informação*. Desta forma este capítulo está estruturado da seguinte forma:

- A seção 5.1 - Extração e Seleção dos Trabalhos Relacionados: apresenta como foi realizada a extração e seleção dos trabalhos;
- A seção 5.2 - Processos da Segurança da Informação: apresenta os trabalhos *An ISMS (im)-Maturity Capability Model,* Woodhouse (2008) *e A Security Engineering Capability Maturity Model,* Regulwar et al. (2010);
- A seção 5.3 - Sistemas de Gerenciamento de Segurança da Informação: apresenta os seguintes trabalhos *Assessment Methodology on Maturity Level of ISMS,* Leem et.al(2005)*, Best Practices Show the Way to Information Security,* Lessing (2008), *Modelling Cyber Security Governance Maturity,* De Bruin e Von Solms (2016) e *Security Metrics Maturity Model for Operational Security,* Muthukrishnan e Palaniappan (2016);
- A seção 5.4 - apresenta uma análise comparativa entre os trabalhos;
- A seção 5.5 - apresenta as considerações deste capítulo.

5.1. Extração e Seleção dos Trabalhos Relacionados

O processo de revisão da literatura é importante para o desenvolvimento de uma pesquisa científica. A revisão sistemática é uma metodologia útil em ciência da computação, dado que possibilita identificar as melhores evidências e sintetizá-las, para fundamentar propostas de mudanças nas áreas de gestão da segurança da informação, controle, monitoramento e reabilitação.

A metodologia de pesquisa utilizada para este trabalho foi baseada na revisão sistemática da literatura (KITCHENHAM et al., 2010). Ou seja, nesta dissertação apenas foram seguidos alguns princípios de uma revisão sistemática.

Para extração dos trabalhos, foi utilizada apenas a busca manual para identificar os trabalhos que mais se aproximavam com os objetivos desta pesquisa.

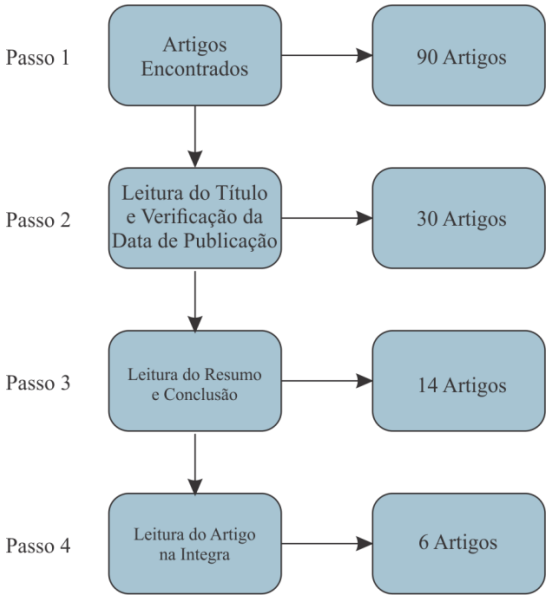
5.1.1. Busca Manual

Foram realizadas buscas no IEEE Explorer[1]. Foram considerados limitação de trabalhos entre os anos de 2005 e 2016. Para esta busca foi pesquisado apenas abordagens sobre modelos de maturidade de segurança da informação.

As palavras chaves nesta busca foram: *Maturity Models* AND *Information Security*, criando a seguinte *String*: ***("Maturity Models") AND ("Information Security")***. A seleção dos artigos seguiu os seguintes passos:

1. Após o uso da *String* de busca, esta pesquisa inicialmente encontrou noventa artigos. Com os resultados, iniciamente os trabalhos foram separados por título e data de publicação. Trabalhos que foram publicados antes do ano de 2005 foram descartados;
2. Após a leitura dos títulos restaram trinta trabalhos onde foram analiasados os resumos e conclusões;
3. Após a leitura dos resumos e conclusões restaram quatorzes trabalhos onde foram analisados os escopos de pesquisa de cada um;
4. Após a leitura na íntegra dos quatorzes trabalhos, seis trabalhos foram selecionados. A Figura 14 apresenta cada passo.

Figura 14: Passos da seleção dos trabalhos relacionados atráves da busca manual



Fonte: Elaborado pelo autor

[1] http://ieeexplore.ieee.org/

5.2. Processos de Segurança da Informação

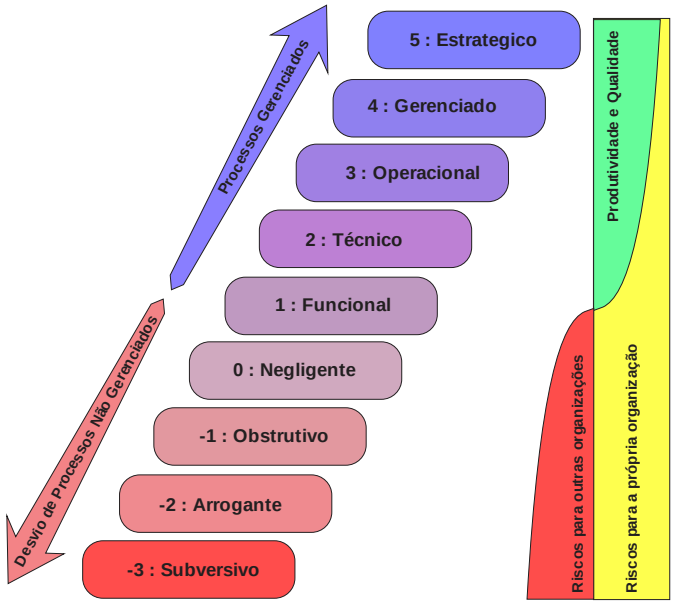
Modelos de maturidade de capacidade têm sido usados para avaliar e orientar iniciativas de melhoria de processos para várias áreas das organizações, desde desenvolvimento de software até engenharia de sistemas, aquisição de produtos, gerenciamento de equipes e segurança da informação para citar alguns. Estes modelos baseiam-se na melhoria dos processos e fornecem uma estrutura para orientar e medir a implementação e melhoria dos processos (WOODHOUSE, 2008). Esta seção apresenta dois trabalhos com contribuições significativas que tem como aspecto processos de segurança da informação.

5.2.1. An ISMS (im)-Maturity Capability Model, Woodhouse (2008)

No trabalho proposto por Woodhouse (2008), é desenvolvido um modelo de maturidade de processo inovador para avaliar a capacidade e maturidade dos processos que afetam Sistemas de Gestão de Segurança da Informação (*ISMS*) dentro de uma organização. Nesse sentido, a intenção de Woodhouse é destacar o papel crítico que a cultura corporativa desempenha no processo de segurança da informação.

Para Woodhouse se as pessoas dentro da organização são participantes ativos ao invés de observadores passivos, a atitude será eficaz para melhorar a segurança. Dessa forma o autor acredita que maturidade pode ser mensurada atráves de um progresso ao longo do tempo. Além disso, a maturidade também necessita não só de controles técnicos, mas gerenciais e operacionais. O modelo de Woodhouse (Figura 15) descreve a implementação de nove níveis de maturidade.

Figura 15: *ISMS (IM)-Maturity Model*



Fonte: Woodhouse (2008)

Cada nível mais baixo deste modelo descreve uma cultura corporativa que garante riscos não só à organização, mas também a parceiros e fornecedores:

- Nível 5: Estratégico – A organização possui um processo de melhoria contínua usando um ciclo de avaliação PDCA. Ele usa sistemas para identificar e corrigir falhas no processo de segurança. Neste nível programas de treinamento de segurança para usuários, gerenciamento e profissionais são fornecidos de forma contínua (WOODHOUSE, 2008);
- Nível 4: Gerenciado – A organização revisa as melhores práticas num período definido. O investimento em segurança da informação aumenta conforme necessário. A organização gerencia bem as organizações, mas ainda precisam mudar a cultura corporativa para uma cultura de segurança da informação (WOODHOUSE, 2008);
- Nível 3: Operacional – A organização consegue analisar a política e o procedimento de segurança conforme necessário. O planejamento estratégico de segurança da informação é estabelecido (WOODHOUSE, 2008);
- Nível 2: Técnico – Na organização não existe uma política global de segurança da informação e as operações são realizadas de forma *ad hoc*. Existe investimento nos controles técnicos da segurança da informação. Não existe segregação de funções dentro da organização (WOODHOUSE, 2008);
- Nível 1: Funcional – A organização não está focada e está mal gerenciada. Não existe uma política de segurança abrangente ou procedimentos definidos (WOODHOUSE, 2008);
- Nível 0: Negligente - As unidades de negócio dentro da organização são capazes de proteger seus ativos de informação, através de esforços individuais. Geralmente as organizações desse nível atuam de forma a evitar que esses esforços sejam bem sucedidos (WOODHOUSE, 2008);
- Nível -1: Obstrutivo – O gerenciamento dentro dessas organizações insiste em processos complexos envolvendo soluções técnicas e documentações inadequadas. A participação ativa no processo de segurança da informação é desencorajada. Organizações obstrutivas representam um maior risco de segurança não só para seus próprios ativos de informação, mas também para os ativos de informações de outras organizações com as quais eles interagem ou fazem negócios (WOODHOUSE, 2008);
- Nível -2: Arrogante – As organizações nesse nível não levam em consideração as práticas de segurança. A cultura corporativa nessas organizações inclui um completo

desrespeito e quase total rejeição de qualquer esforço para modificar ou melhorar as práticas de segurança da informação. A Administração acredita firmemente que seus esforços de segurança da informação são as únicas opções corretas e qualquer desacordo é imediatamente esmagado (WOODHOUSE, 2008);

- Nível -3: Subversivo – Neste nível a organização busca ativamente desacreditar e perturbar outras organizações. As organizações de nível -3 tentam garantir que todas as outras organizações sejam (ou sejam percebidas) como pior do que ela própria, comprometendo e prejudicando deliberadamente os concorrentes. Qualquer fraqueza percebida nas organizações parceiras é explorada voluntária e metodicamente. O risco para os ativos de informações dentro das organizações de nível -3 está em seu nível máximo, enquanto o risco para organizações de terceiros é extremo (WOODHOUSE, 2008).

O modelo *An ISMS (im)-Maturity Capability Model* desenvolvido por Woodhouse (2008) destaca a avaliação do papel crítico que a cultura organizacional desempenha nos processos de segurança da informação. Neste modelo cada nível de maturidade está relacionado a cada processo de segurança que pode fornecer indicações de melhorias do estado atual de cada processo e orientar a organização através de estágios de maturidade.

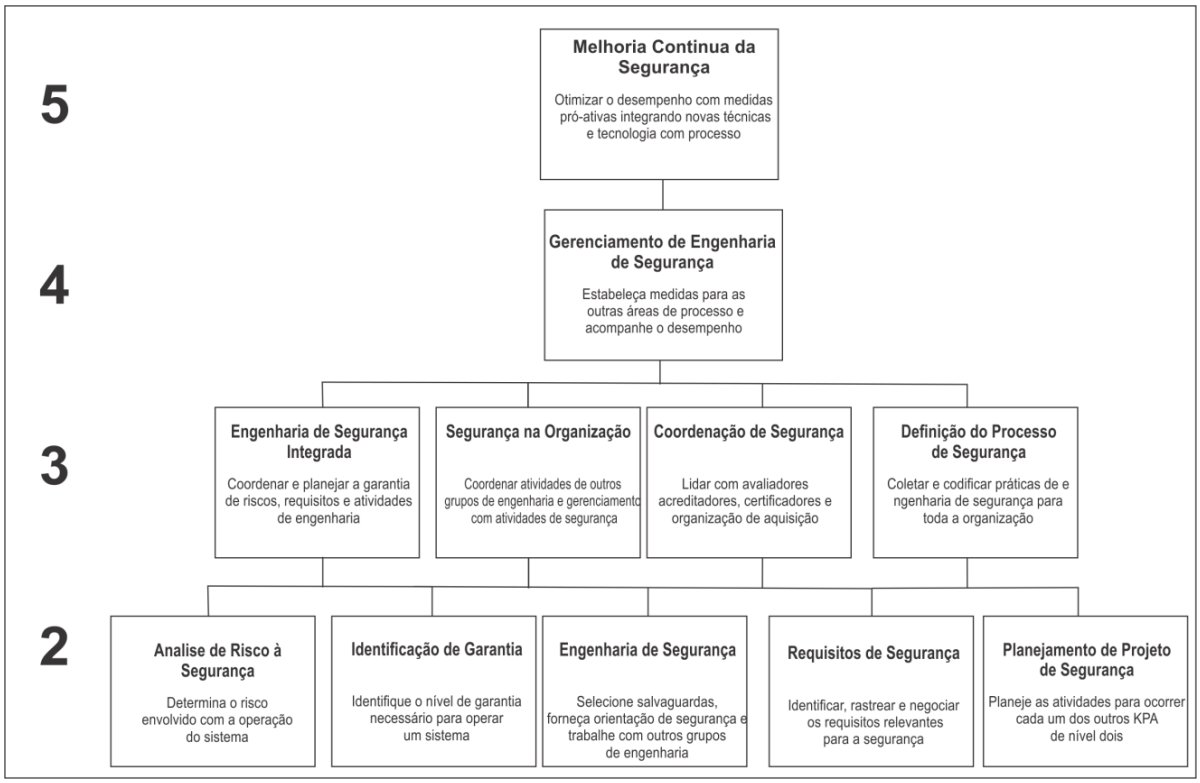
Esta proposta deixa um ponto a ser questionado: o número excessivo de níveis de maturidade pode ocasionar num processo de avaliação longo e demorado. Sendo assim, é possível afirmar que, por exemplo, os níveis -3 subversivo, -2 arrogante e -1 Obstrutivo possam se tornar um único nível, deixando o processo mais ágil e otimizado.

5.2.2. A Security Engineering Capability Maturity Model, Regulwar et al. (2010)

No trabalho proposto por Regulwar et al. (2010) é apresentada uma estrutura de engenharia de segurança que levam as organizações a um melhor, mais barato e mais rápido processo de desenvolvimento de sistemas e produtos seguros. Esta estrutura trata de um modelo de maturidade de capacidade para engenharia de segurança (SE CMM), que tem por objetivo orientar e melhorar os processos na prática da engenharia de segurança. Além disso, é proposta uma cultura organizacional de melhoria de processos. O modelo baseia-se e adota grande parte da estrutura do SEI CMM (SEI, 2010). Ele visa aspectos de gerenciamento das organizações, além de ser direcionado para organizações de engenharia de segurança, que para fins deste modelo, é definida como o grupo de pessoas, tanto os gerentes quanto o pessoal técnico, que tem a responsabilidade de implementar o processo de engenharia de segurança (REGULWAR et al. 2010). Neste modelo, cada nível de maturidade é composto por um conjunto de práticas (KPA)

que, quando executadas, atingem um conjunto de metas (Figura 16). Para construir este modelo, foram identificadas práticas tradicionais de engenharia de segurança.

Figura 16: *Security Engineering Maturity Model* (SE CMM)



Fonte: Regulwar et al. (2010)

A seguir são destacados níveis de maturidade propostos por Regulwar et al. (2010):

- Nível 1 - Inicial: As práticas não estão definidas e precisam ser reinventadas para cada projeto. Os projetos são imprevisíveis devido à programação *ad hoc*, orçamentos, funcionalidade e qualidade do produto. Não existe KPA para este nível (REGULWAR et al. 2010);
- Nível 2 – Repetível: As atividades de garantia são melhoradas porque as práticas são bem definidas e repetíveis. Conforme o autor as KPAs neste nível cobrem a maioria das práticas de engenharia de segurança. Eles são: Planejamento de Segurança, Análise de Risco de Segurança, Identificação de Garantia, Engenharia de Segurança e Requisitos de Segurança (REGULWAR et al. 2010);
- Nível 3 – Definido: Um nível de segurança ainda maior pode ser extraído das práticas, pois todas as áreas de processos necessárias são usadas em cada projeto. As KPAs de nível três incluem a Engenharia de Segurança Integrada, Organização de Segurança, Coordenação de Segurança e Definições de Processo de Segurança (REGULWAR et al. 2010);

- Nível 4 – Gerenciado: Caracteriza uma organização de engenharia de segurança que possui visão de gerenciamento do processo de engenharia de segurança e sua interação com outras disciplinas de engenharia. A KPA utilizada é Gerenciamento de Engenharia de Segurança. (REGULWAR et al. 2010);
- Nível 5 - Otimização: A organização de engenharia de segurança continua identificando áreas de melhoria através da medição, identificação da causa dos problemas e modificação dos processos. A KPA neste nível integra novas técnicas de segurança e aperfeiçoa os desempenhos (REGULWAR et al. 2010).

O trabalho intitulado *A Security Engineering Capability Maturity Model* desenvolvido por Regulwar, Gulhane e Jawandhiya (2010), trata de processos de segurança na organização, pois os níveis são detalhados conforme as práticas que são implantadas dentro da organização. Entretanto, é importante salientar que neste trabalho pode haver uma limitação apenas para uso na área de segurança de engenharia para desenvolvimento de software, podendo surgir dificuldades para a replicação para outras áreas da organização.

5.3. Gerenciamento da Segurança da Informação

Um modelo de maturidade de segurança da informação pode fornecer a uma organização estruturas de segurança da informação distintas. As organizações que se adequam a estes modelos são suscetíveis a perseguir satisfatoriamente a segurança da informação. Além disso, o uso de modelos de maturidade de segurança promove o uso de padrões de melhores práticas que geralmente levam a governança de segurança da informação adequada (LESSING, 2008). Esta seção apresenta quatro trabalhos que tem como aspecto gerenciamento da segurança da informação.

5.3.1. Assessment Methodology on Maturity Level of ISMS, Leem et.al (2005)

No trabalho proposto por Leem, Kim e Lee (2005), os autores sugerem uma metodologia de avaliação do SGSI (Sistemas de Gerenciamento de Segurança da Informação) considerando os aspectos técnicos, gerenciais e operacionais da segurança da informação. Esta metodologia inclui os índices de avaliação, processo e modelo de maturidade.

A metodologia proposta fornece o modelo de maturidade de cinco estágios para o SGSI, incluindo nível de planejamento, nível do ambiente, nível de suporte e nível tecnológico. A metodologia proposta por Leem, Kim e Lee (2005) sugere níveis de maturidade com ponto de vista sintético do SGSI. As definições dos níveis de maturidade são as seguintes:

- Estratégico: A operação do SGSI cria novas oportunidades de negócios e valor das empresas.
- Gerenciamento Ativo: As melhores práticas sobre o SGSI são revistas periodicamente. A monitorização da devida diligência e da conformidade é bem realizada.
- Gerenciamento Passivo: A separação do dever e o posicionamento do oficial de segurança, do administrador e do auditor são concluídos. O planejamento estratégico de segurança da informação é estabelecido.
- Técnico: Os controles técnicos para a segurança do perímetro são introduzidos. No entanto, a política de segurança, procedimentos e diretrizes não são estabelecidos.
- Funcional: Proprietários de informações e sistemas executam controles de segurança, incluindo protetor de tela, vacina antivírus, utilitário de compactação ativado por senha e assim por diante.

Iniciativas no trabalho *Assessment Methodology on Maturity Level of ISMS* proposto por Leem, Kim e Lee (2005) atendem a possibilidade de serem avaliados vários aspectos como: técnicos, gerenciais e operacionais da segurança da informação, dentro do tema de SGSI (Sistema de Gestão de Segurança da Informação).

5.3.2. Best Practices Show the Way to Information Security, Lessing (2008)

No trabalho proposto por Lessing (2008) é desenvolvido um modelo de maturidade extraindo características de vários modelos de maturidade de segurança da indústria e desenvolvendo um modelo genérico de maturidade de segurança. O modelo de Lessing (2008) é orientado para as melhores práticas de segurança da informação.

Os documentos de melhores práticas que foram mapeados contêm as práticas estabelecidas por líderes disciplinares. Eles disponibilizaram esses documentos para controlar com êxito o ambiente de segurança da informação. Segundo Lessing (2008), este trabalho não tem intenção de criar mais um modelo de maturidade de segurança, mas sim um modelo de condução de boas práticas pode ser classificado como um modelo de maturidade.

No Quadro 7 é apresentado o modelo com as melhores práticas proposto por Lessing.

Quadro 7: Modelo Genérico de Maturidade Proposto por Lessing

Níveis	Boas Práticas
Nível 1	Gestão de ativos, gestão de segurança, segurança física e ambiental, medição de desempenho e gestão de segurança.
Nível 2	Necessidades e objetivos de controle, aplicações críticas de negócios, gerenciamento de continuidade de negócios, organização / gestão da segurança da informação, medição do desempenho, gestão da segurança, gestão da segurança do pessoal, desenvolvimento de sistemas de informação e requerimentos legais.
Nível 3	Gerenciamento de segurança, desenvolvimento de sistemas de informação, gerenciamento de segurança e gerenciamento de conformidade.
Nível 4	Gerenciamento de segurança, gerenciamento de riscos, gerenciamento de conformidade.
Nível 5	Continuidade de negócios, gerenciamento de conformidade, aplicações críticas de negócios, medição de desempenho, gerenciamento de segurança e responsabilidade corporativa e criminal.

Fonte: Lessing (2008)

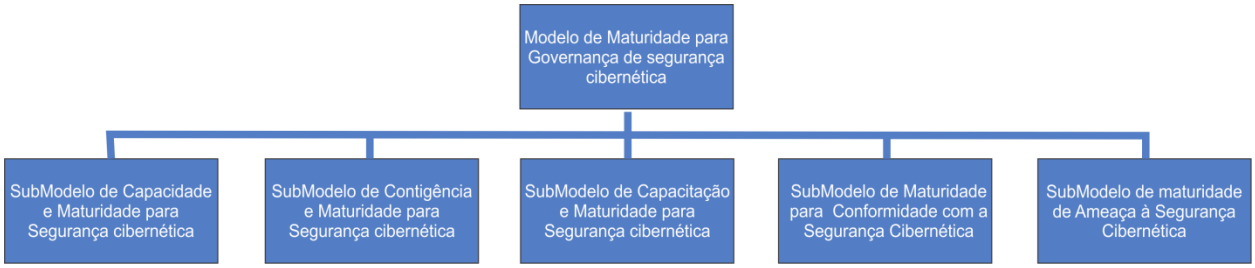
O modelo *Best Practices Show the Way to Information Security*, proposto por Lessing (2008) reforça que é preciso preencher a lacuna de trabalhos que utilizem boas práticas para modelos de maturidade. Desta forma, acredita-se que o modelo de Lessing torna-se relevante para contribuir com a metodologia proposta neste trabalho, pois ambos os modelos tem as práticas de segurança como premissas para avaliar a maturidade da organização.

5.3.3. Modelling Cyber Security Governance Maturity, De Bruin e Von Solms (2016)

No trabalho proposto por De Bruin e Von Solms (2016) é apresentado um modelo que tem como objetivo determinar a maturidade da segurança da informação em uma organização. O modelo é composto por vários modelos de maturidade constituintes que, em conjunto, visam determinar a maturidade do que se denomina *Cyber Security Governance* (De Bruin e Von Solms ,2016).

O modelo proposto por De Bruin e Von Solms (2016) consiste em cinco componenentes ou submodelos (Figura 17) que são apresentados a seguir. Cada submodelo relaciona conteúdos específicos dentro da segurança da informação, podendo ser avaliada a maturidade de forma individual.

Figura 17: Proposta de componentes ou submodelos



Fonte: De Bruin, Von Solms (2016)

Para se chegar ao resultado final são atribuídos pesos a cada nível de maturidade. Em seguida pode-se comparar o número total de práticas "verificadas" com o número total de práticas disponíveis e inserir o resultado final no "*Cyber Security Governance Maturity Dashboard*", atribuindo um número inteiro ao número decimal que será produzido como resultado. A fórmula usada por De Bruin, Von Solms (2016) é apresentada a seguir:

$$Resultado = \frac{(C1 * 1) + (C2 * 2) + (C3 * 3) + (C4 * 4)}{(T1 * 1) + (T2 * 2) + (T3 * 3) + (T4 * 4)}$$

Na fórmula apresentada acima é atribuído um peso para cada nível de maturidade:

- Nível 1 foi atribuído peso 1;
- Nível 2 foi atribuído peso 2;
- Nível 3 foi atribuído peso 3;
- Nível 4 foi atribuído peso 4.

As variáveis C1, C2, C3 e C4 denotam o número total de práticas "verificadas" dentro do nível de maturidade específico. As variáveis T1, T2, T3 e T4, denotam o número total de práticas disponíveis. Uma vez que a fórmula retornará a um valor decimal entre 0,00 e 1,00, é usada cada quadrante como seu respectivo nível (ou seja, 0,00 - 0,24 é atribuído ao Nível 1, 0,25 - 0,49 é atribuído ao Nível 2, 0,50 - 0,74 é atribuído ao Nível 3 e 0,75 - 1,00 são atribuídos ao Nível 4) (De Bruin e Von Solms, 2016).

Sendo assim, os valores serão obtidos após a avaliação. O "*Cyber Security Governance Maturity Dashboard"* (Quadro 8) é preenchido com o apontamento dos níveis de maturidade.

Quadro 8: *Cyber Security Governance Maturity Dashboard* de De Bruin e Von Solms

	Nível 1	Nível 2	Nível 3	Nível 4
Cybersecurity Capability		*		
Cybersecurity Contingency		*		
Cybersecurity Capacity Building				*
Cybersecurity Conformance				*
Cybersecurity Threat	*			

Fonte: De Bruin, Von Solms (2016).

O ponto forte do trabalho desenvolvido por DeBruin e Von Solms (2016) é destacar que cada submodelo ou componente possa ser avaliado individualmente. Desta forma, as avaliações de maturidade podem ser realizadas de forma flexível, ocorrendo o mesmo com as avaliações das dimensões desenvolvidas nesta dissertação.

5.3.4. Security Metrics Maturity Model for Operational Security, Muthukrishnan e Palaniappan (2016)

No trabalho proposto por Muthukrishnan e Palaniappan (2016), são exploradas identificações de elementos de qualidade de segurança para determinar métricas para um ambiente de segurança operacional. Como contribuição, a classificação é realizada através da qualidade de uma métrica de um *scorecard*, que fornece a pontuação. Por fim é divulgado um índice da maturidade de segurança com as métricas que foram utilizadas. Desta forma os autores entendem que é possível quantificar a confiança da empresa, além de utilizar uma classificação com base em taxonomia para ajudar na compreensão dos resultados. O trabalho proposto por Muthukrishnan e Palaniappan (2016) utiliza as seguintes métricas operacionais:

- Gerenciamento de Patch;
- Gerenciamento de Vulnerabilidades;
- Métricas Financeiras;
- Segurança de Aplicativos;
- Gestão da Mudança;
- Gerenciamento de Configurações;
- Gerenciamento de Incidentes.

A avaliação dessas métricas é realizada a partir das análises quantitativa e qualitativa com base em dois níveis de avaliação denominadas *Quantitative Matured Metrics* (QtMM) e *Qualitatives Matured Metrics* (QlMM). O QtMM e QlMM são compostos da seguinte forma:

Quantificável (QtMM1), Facilmente Disponível (QtMM2), Repetitiva (QtMM3), números cardinais ou porcentagem como uma unidade de medida (QtMM4); Correção (QlMM1) Sensibilidade (QlMM2), Significância (QlMM3). Essas métricas produzem a maturidade final, através do cálculo:

- $QtMM = QtMM^1 + QtMM^2 + QtMM^3 + QtMM^4$
- $QlMM = QlMM^1 + QlMM^2 + QlMM^3$
- QMM = QtMM + QlMM

Para a qualificação de métricas, cada propriedade recebe três valores para estabelecer uma qualidade ou a intensidade das propriedades. Os valores são: 0,0 – não cumpridos, 0,5 – parcialmente cumpridos e 1,0 – totalmente cumpridos. Por exemplo:

a) Os dados estão disponíveis prontamente, um só tem que executar algum *script* para recuperar e produzir métricas. Isso proporcionará uma pontuação total de 1.0.
b) Os dados devem ser compilados a partir de um questionário distribuído e adicionado aos dados do sistema existentes. Existe uma intervenção humana nisso, que pode invocar alguns erros, portanto, na discrepância de dados. Portanto, talvez seja atribuída uma pontuação de 0,5.
c) Os dados não estão prontamente disponíveis; é elaborado um processo ou intervenção *ad hoc* para reunir os dados. Isso resultará em 0.0 na pontuação.

- Métricas maduras = 3.0 < QtMM / QlMM
- Métricas em evolução = 2.0 < QtMM / QlMM < 3.0
- Métricas infantis = QtMM / QlMM < 2.0

Finalmente, a média é deduzida do total e fornecida com o SM-Mi (*Security Metrics Maturity Index*). O quadro 9 mostra o índice com base na maturidade métrica média.

Quadro 9: *Cyber Security Governance Maturity Dashboard* de Muthukrishnan e Palaniappan

SM-Mi	Range in Percentage (%)
1	0-20
2	21-40
3	41-70
4	71-90
5	91-100

Fonte: Muthukrishnan e Palaniappan (2016)

A maturidade da organização é definida por uma pontuação em porcentagem que os autores chamam de *Security Metrics Maturity Index* SM-Mi (Quadro 9). Em seguida é

apresentada a escala de maturidade (Figura 18) proposta pelos autores Muthukrishnan e Palaniappan (2016). Essa escala de maturidade indica que, quanto maior o nível, as medidas utilizadas se tornam mais confiáveis e com maior qualidade. Como por exemplo, o Índice 5 significa que a organização possui um modelo de maturidade válido e as métricas são confiáveis. (MUTHUKRISHNAN E PALANIAPPAN , 2016).

Figura 18: Escala de Maturidade SM-Mi

Fonte: Muthukrishnan e Palaniappan (2016)

O trabalho *Security Metrics Maturity Model for Operational Security*, proposto por Muthukrishnan e Palaniappan (2016), tornou-se relevante para este trabalho, pois além da avaliação estar relacionada com aspectos quantitativos, é utilizado uma pontuação com porcentagem para definir a escala de maturidade.

5.4. Análise Comparativa

Nesta seção é apresentada uma análise comparativa entre os trabalhos relacionados. Como forma de analisar os mesmos, foram estabelecidos critérios que são apresentados a seguir.

5.4.1. Critérios para Avaliação dos Trabalhos

Modelos de maturidade de segurança podem envolver aspectos gerenciais, técnicos e operacionais. Após uma revisão da literatura, não foi identicado nenhum trabalho que abordasse modelos de maturidade para configurações de servidores. Entretanto nos trabalhos relacionados presentes nas seções 5.2 e 5.3, foram encontrados fatores relevantes que servem como parâmetros para avaliar os modelos de maturidade propostos neste capítulo comparados com este trabalho. A seguir são apresentadas as características que foram utilizadas para avaliação dos trabalhos.

- **Critério 1 (C1) – Modelo Teórico.** Avalia se o modelo de maturidade consiste de uma generalização a partir de padrões existentes de modelos de maturidade. Dos trabalhos relacionados, apenas a proposta desta dissertação e o trabalho *Security Metrics Maturity Model for Operational Security,* Muthukrishnan e Palaniappan (2016), não partem de uma generalização de algum modelo de maturidade existente;
- **Critério 2 (C2) – Abordagem Quantitativa.** Indica se a avaliação está relacionada com aspectos quantitativos, utilizando pontuações ou porcentagens para definir a escala de maturidade. Neste critério, apenas a proposta desta dissertação e os trabalhos *An ISMS (im)-Maturity Capability Model*, Woodhouse (2008) e Security Metrics Maturity Model for Operational Security, Muthukrishnan e Palaniappan (2016)**.**
- **Critério 3 (C3) – Abordagem Qualitativa.** Indica se a avaliação considera de alguma forma, as motivações, opiniões, comportamentos e expectativas de um indivíduo ou grupos. Neste critério, apenas a proposta desta dissertação e os trabalhos *An ISMS (im)-Maturity Capability Model,* Woodhouse (2008) e *A Security Engineering Capability Maturity Model***,** Regulwar et al. (2010).
- **Critério 4 (C4) – Aspectos Gerenciais.** Indica se a avaliação envolve até o mais alto nível hierárquico da organização. Todos os trabalhos atendem a este critério.
- **Critério 5 (C5) – Aspectos Técnicos.** Indica se a avaliação envolve execução de conhecimentos técnicos, obedecendo a um conjunto de regras e normas. Apenas os trabalhos, *An ISMS (im)-Maturity Capability Model*, Woodhouse (2008), *A Security Engineering Capability Maturity Model*, Regulwar et al. (2010) e *Best Practices Show the Way to Information Security,* Lessing (2008) não atendem a este critério.
- **Critério 6 (C6) – Aspectos Operacionais.** Indica se a avaliação está relacionada com operações de segurança na organização. Apenas o trabalho *An ISMS (im)-Maturity Capability Model,* Woodhouse (2008) não atende a este critério.
- **Critério 7 (C7) – Uso Real ou Simulação do Modelo.** Indica se o modelo foi avaliado em um estudo real ou numa simulação. Apenas os trabalhos *An ISMS (im)-Maturity*

Capability Model, Woodhouse (2008), *A Security Engineering Capability Maturity Model*, Regulwar et al. (2010) e *Best Practices Show the Way to Information Security*, Lessing (2008) não atendem a este critério.

5.4.2. Comparativo entre os Modelos de Maturidade de Segurança

O Quadro 10 apresenta um comparativo entre os modelos de maturidade de segurança apresentados neste capítulo. A primeira coluna exibe o nome do trabalho relacionado e as demais colunas exibem os critérios citados na seção anterior. A marcação "+" indica que o trabalho relacionado atende ao critério estabelecido, enquanto a marcação "-" indica que não foi atendido o critério.

Quadro 10: Comparativo entre os Trabalhos Relacionados

Modelos de Maturidade	C1	C2	C3	C4	C5	C6	C7
An ISMS (im)-Maturity Capability Model	+	-	+	+	-	-	-
A Security Engineering Capability Maturity Model	+	-	+	+	-	+	-
Best Practices Show the Way to Information Security	+	-	-	+	-	+	-
Modelling Cyber Security Governance Maturity	+	+	-	+	+	+	+
Assessment Methodology on Maturity Level of ISMS	+	-	-	+	+	+	+
Security Metrics Maturity Model for Operational Security	-	+	-	+	+	+	+
Proposta desta dissertação	-	+	+	+	+	+	+

Fonte: Elaborado pelo autor

Conforme apresentado no Quadro 10, seis trabalhos foram analisados e comparados. De modo geral, apenas um trabalho (além da proposta desta dissertação) não foi desenvolvido com base na generalização de outros modelos de maturidade de segurança. Uma limitação relevante foi identificada nos trabalhos propostos por Woodhouse (2008), Regulwar et al. (2010) e Lessing (2008). Esses trabalhos apresentam apenas o modelo de maturidade de segurança de forma conceitual, não existindo qualquer simulação ou uso real dos modelos. Desta forma não é possível saber a efetividade e viabilidade do uso desses modelos de maturidade de segurança.

Outro ponto a ser citado é que a maioria dos modelos tem foco em práticas bastante semelhantes, por exemplo, os trabalhos de De Bruin, Von Solms (2016) e Muthukrishnan e Palaniappan (2016), além de desenvolverem o *dashboard* com o nome e escala de maturidade similar.

5.5. Considerações Finais

Neste capítulo foram apresentados trabalhos relacionados que abordam modelos de maturidade de segurança da informação entre o ano de 2005 a 2016, descrevendo as principais contribuições de cada trabalho. Para atender a necessidade da pesquisa uma busca manual baseada em revisão sistemática da literatura foi realizada.

Este capítulo também apresentou uma análise comparativa através da avaliação dos modelos de maturidade de segurança da informação encontrados na literatura. Em seguida foi realizada uma consolidação de características mais relevantes para avaliar cada modelo de maturidade descrevendo os pontos e suas limitações que apoiaram o desenvolvimento desta dissertação.

6. CONCLUSÕES E TRABALHOS FUTUROS

6.1. Conclusões

Este trabalho propôs uma metodologia para apoiar políticas de segurança do *data center* das organizações, independente do sistema operacional utilizado, serviços e versões. Em outras palavras, este trabalho permitiu a avaliação e melhoria da maturidade das configurações de segurança do servidor em ambientes de *data center*. Com esta metodologia também foi possível avaliar as políticas de segurança existentes em normas internacionais voltadas para configurações e fornecer diretrizes para avaliar a maturidade de segurança das organizações.

Desta forma, a contribuição principal foi a proposição desta metodologia que consiste nas três atividades a seguir:

1. Análise dos Controles de Segurança - consiste na seleção das Dimensões, que são conjuntos de controles de segurança que foram extraídos das normas ISO 27002 e NIST SP 800-53;
2. Avaliação da Maturidade – consiste na realização da avaliação de maturidade através de três abordagens: A análise tradicional que segue apenas os controles de segurança e considera o mesmo nível de importância a todos eles. A análise ponderada é comparativamente mais complexa, pois adota mais de uma norma de segurança. A análise contextual é semelhante à análise ponderada, mas também considera a opinião da organização sobre o nível de importância de cada controle de segurança.
3. Geração de Resultados – Esta atividade consiste na entrega de relatórios, reportando o nível de maturidade e as melhorias necessárias para a segurança do ambiente do *data center*.

Outra contribuição relevante é a utilização de três abordagens de avaliação contidas na segunda atividade. Os procedimentos tradicionais, por exemplo, realizam a avaliação da maturidade com base em uma única norma e sem levar em consideração o contexto da organização avaliada.. Cada norma define um conjunto de controles de segurança. A análise tradicional procura evidências de que a configuração de segurança do servidor respeite os controles de segurança recomendados geralmente por uma única norma internacional. Podendo assim limitar a generalidade dos resultados. Desta forma, esta metodologia inclui duas novas abordagens de avaliação:

- A análise ponderada que adota duas ou mais normas de segurança para avaliar a maturidade das configurações de segurança do servidor; Os controles recomendados simultaneamente nas normas de segurança obtêm maior nível de importância; O nível de maturidade capta o senso comum entre diferentes normas;
- A análise contextual é semelhante à análise ponderada; No entanto, também leva em consideração a opinião da organização para determinar o nível de importância de cada controle de segurança. Aqui, o nível de maturidade introduz a perspectiva da empresa sobre o conceito de segurança.

Para avaliar o uso da metodologia foram realizados dois estudos de caso. No primeiro estudo, os resultados permitem demonstrar que a análise tradicional pode ser ineficaz para capturar o nível real de maturidade de segurança no *data center* da empresa. Por exemplo, quando ponderamos os controles de segurança, os resultados foram diferentes na maioria das avaliações. Houve acréscimos significativos na porcentagem e escala de maturidade. Esse resultado indica que o *data center* analisado estava em conformidade com os controles de segurança com peso maior. Por sua vez, a terceira abordagem de avaliação (análise contextual) enriqueceu a análise ponderada com a perspectiva da empresa. Ela trouxe opiniões dos membros da organização sobre cada controle de segurança e permitiu a captura de conhecimento interno de negócios sobre os parâmetros de segurança no procedimento de avaliação. Portanto, foi possível identificar o alinhamento entre as recomendações de normas de segurança e a realidade de cada empresa. Além disso, a análise contextual demonstrou que a organização está priorizando os aspectos de segurança que realmente acredita.

No segundo estudo de caso quando introduzimos a perspectiva da empresa, o *data center* obteve novamente resultados diferentes na escala de maturidade. Eventualmente, a metodologia permitiu identificar erros e omissões nas configurações de segurança. Tais informações são úteis para propor políticas para melhorar os parâmetros de segurança do *data center*.

No final de cada estudo de caso foi solicitado aos participantes que preenchessem um relatório para avaliar os benefícios da metodologia. As respostas atestam que a metodologia foi útil para, tanto compreender o contexto real de segurança do ambiente de *data center*, como para definir políticas para melhorar a segurança.

Após toda a avaliação foram identificados os impactos técnicos e no negócio, levando as respectivas organizações a refletirem sobre suas atividades que entraram em conflito com as recomendações das normas internacionais de segurança. Portanto, as duas organizações começaram a analisar possíveis mudanças na sua equipe técnica, contratos e modelos de negócio.

Por fim, entende-se que o uso da metodologia é viável em qualquer contexto em que o *data center* esteja inserida. Desta forma, esta metodologia não se limita ao tipo de negócio da empresa, qual o fabricante do servidor ou serviços que estão em uso.

6.2. Trabalhos Futuros

Para dar continuidade a este trabalho, são apresentadas as seguintes sugestões de trabalhos futuros.

- **Estender esse trabalho a *data centers* maiores e mais complexos**. Foi avaliado neste trabalho dois estudos de caso relevantes, mas que tinham o *data centers* de médio porte. A análise envolvendo cenários maiores e mais complexos poderá gerar mais resultados que ateste não apenas a importância da metodologia proposta neste trabalho, mas principalmente a importância da adoção de medidas de segurança neste tipo de ambiente;
- **Desenvolver abordagens de avaliação para analisar a maturidade da segurança de outros dispositivos no ambiente do *data center:*** Nesta metodologia foram avaliados apenas servidores, existindo assim a necessidade de avaliar a maturidade de outros dispositivos no ambiente de *data center*, por exemplo, configurações de segurança dos dispositivos de camada 2 e 3 da rede;
- **Agregar a metodologia outras normas internacionais de segurança:** Nesta metodologia foram utilizadas as normas de segurança da informação ISO/IEC 27002 e NIST SP 800-53. Desta forma, acredita-se que a inserção de novas normas, por exemplo, *Shared Assessments Agreed Upon Procedures* (AUP) e *Open Web Application Security Project* (OWASP), possam enriquecer ainda mais a estrutura de controles de segurança;
- **Desenvolver outros modelos de maturidade de segurança para avaliar as demais áreas técnicas nas empresas:** Esta metodologia avaliou apenas configurações de segurança de servidores em ambiente de *data center*. Desta forma, acredita-se que seja possível desenvolver um modelo de maturidade de segurança que envolva as áreas técnicas da organização;
- **Realizar a automação das configurações de segurança de servidores com base nas políticas de segurança e atividades desta metodologia:** Durante o desenvolvimento deste trabalho foi identificada a possibilidade de se automatizar vários controles de segurança com aspecto unicamente técnico. Desta forma, pode ser possível acelerar o

processo de configuração de segurança no sistema operacional e nos arquivos de configuração dos softwares utilizados no servidor.

REFERÊNCIAS

BANGHART, J.; JOHNSON, C. **The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1** . 0 Recommendations of the National Institute of Standards and Technology. Nist Special Publication, 2011.

BARKER, L. K.; NELSON, L. D. **Security Standards- Government and Commercial**. AT&T Technical Journal, v. 67, n. 3, p. 9–18, 1988.

BAYUK, J. L. **The Utility of Security Standards**. Proceedings - International Carnahan Conference on Security Technology, p. 1–6, 2010.

BREAUX, T. D. et al. **Mapping Legal Requirements to IT Controls.** 6th International Workshop on Requirements Engineering and Law, RELAW 2013 - Proceedings, p. 11–20, 2013.

CHATZIPOULIDIS, A.; MAVRIDIS, I. **An Ict Security Management Framework**. Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on. Anais, 2010.

CHRISTOPHER ALBERTS, A. D. **Managing Information Security Risk**. Nist Special Publication, n. March, p. 320, 2011.

CISCO SYSTEMS. **Data Center - Technology Design Guide.** Cisco Validated Design. 2014.

D'AVILA, R. **Data Centers são Novos Alvos dos Ataques Virtuais**. Disponível em: <http://www.linuxmagazine.com.br/lm/noticia/data_centers_saeo_novos_alvos_dos_ataques_virtuais>.

DE BRUIN, R.; VON SOLMS, S. H. **Modelling Cyber Security Governance Maturity**. International Symposium on Technology and Society, Proceedings, v. March, p. 1–8, 2016.

DIGITAL, C. **Data Centers são Os Alvos de Ataques DDoS**. Disponível em: <http://www.linuxmagazine.com.br/lm/noticia/data_centers_e_servicos_na_nuvem_saeo_os_alvos_principais_dos_ataques_ddos>.

FULLER, J. et al. **Fedora 18 Security Guide - A Guide to Securing Fedora Linux**. 2013.

GREENBERG, A. et al. **VL2: A Scalable and Flexible Data Center Network.** ACM SIGCOMM Conference on Data Communication, p. 51–62, 2009.

HERTZOG, R.; MAS, R. **The Debian Administrator's Handbook**. Freexian SARL, 2013.

HOLIK, F. et al. **Methods of Deploying Security Standards in a Business Environment**. Proceedings of 25th International Conference Radioelektronika, RADIOELEKTRONIKA, p.

411–414, 2015.

ISACA. **COBIT 5: Governança e Gestão de TI da Organização**. ISACA, 2013.

ISO/IEC. **ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management**. Disponível em: <https://www.iso.org/standard/56742.html>. Acesso em: 15 out. 2016.

ISO/IEC. **ISO/IEC 27004 - Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation**. Disponível em: <https://www.iso.org/standard/64120.html>. Acesso em: 15 out. 2016.

ISO/IEC 27000. ISO/IEC 27000 **Information technology — Security techniques — Information security management systems — Overview and vocabulary.** October, v. 3, p. 38, 2014.

ISO/IEC 27002. ISO/IEC 27002:2013. **Information technology — Security techniques — Code of practice for information security controls**, second edition ed. p. 1–112, 2013.

ISO 27001. **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos**. 2013.

JACOBS, P.; ARNAB, A.; IRWIN, B. **Classification of security operation centers**. Information Security for South Africa - Proceedings of the ISSA 2013 Conference, 2013.

JANSEN, W. **Directions in Security Metrics Research**, NISTIR 7564. National Institute of Standards and Technology, v. April, p. 1–26, 2009.

JANSSEN, L. A. **Instrumento de Avaliação de Maturidade em Processos de Segurança da Informação: Estudo de Caso em Instituições Hospitalares**. p. 1–166, 2008.

JAYASWAL, K. **Administering Data Centers: Servers, Storage, and Voice over IP**. 2006.

JOHNSON, **A. Guide for Security-Focused Configuration Management of Information Systems**. Nist, n. August, p. 1–88, 2011.

KELLER, S.; SMID, M. **Modes of Operation Validation System (MOVS): Requirements and Procedures**. NIST Special Publication, n. 800–17, p. 1–153, 1998.

KITCHENHAM, B. et al. **Systematic literature reviews in software engineering-A tertiary study**. **I**nformation and Software Technology, v. 52, n. 8, p. 792–805, 2010.

KRÁTKÝ, R. et al. **Red Hat Enterprise Linux 6.8 Security Guide**. 2016.

LEEM, C. S.; KIM, S.; LEE, H. J. **Assessment Methodology on Maturity Level of ISMS**. Proceedings of the 9th International Conference on KnowledgeBased Intelligent Information and

Engineering Systems, v. 3683, p. 609–615, 2005.

LESSING, M. M. **Best practices show the way to Information Security Maturity.** 6th National Conference on Process Establishment, Assessment and Improvement in Information Technology (ImproveIT 2008), p. 1–9, 2008.

LEWIS, M.; FRIEDMAN, M. **IBM Data Center Networking: Planning for Virtualization and Cloud Computing**. Contract, 2011.

LI, Y. **Network-Aware Job Placement in Datacenter Environments**. Department of Computer Science - University of Calbary, 2014.

LIKERT, R. **A technique for the measurement of attitudes**. Archives of Psychology, v. 22 140, p. 55, 1932.

MADAN, S.; MADAN, S. **Security standards perspective to fortify web database applications from code injection attacks**. ISMS 2010 - UKSim/AMSS 1st International Conference on Intelligent Systems, Modelling and Simulation, p. 226–230, 2010.

MAP, D. C. **Colocation USA**. Disponível em: <http://www.datacentermap.com/usa/>.

MIANI, R. S.; ZARPELÃO, B. B.; MENDES, L. S. **Um estudo empírico sobre o uso de métricas de segurança em ambientes reais**. p. 699–710, 2014.

MICROSOFT. **Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)**. Disponível em: <https://www.microsoft.com/en-us/download/details.aspx?id=7558>.

MONTESINO, R.; FENZ, S. **Automation possibilities in information security management**. Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011, p. 259–262, 2011.

MUTHUKRISHNAN, S. M.; PALANIAPPAN, S. **Security metrics maturity model for operational security**. ISCAIE 2016 - 2016 IEEE Symposium on Computer Applications and Industrial Electronics, p. 101–106, 2016.

NASH, K. **The Global State of Information Security 2008 - Our annual survey finds respondents throwing technology at the problem. Which is a beginning, but only a beginning.** Disponível em: <http://www.csoonline.com/article/2123345/data-protection/the-global-state-of-information-security-2008.html>.

NIEKERK, VAN B.; JACOBS, P. **Toward a Secure Data Center Model.** ISACA Journal, v. 3, n. 1, p. 1–10, 2015.

NIST. **Security and Privacy Controls for Federal Information Systems and Organizations.**

SP-800-53 Ar4. 2014.

NIST. NIST SP 800-53A, R4: **Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans**. NIST Special Publication 800-53A, Revision 4, n. December 2014, p. 1–487, 2014b.

NWAFOR, C. I. et al. **A COBIT and NIST-Based Conceptual Framework for Enterprise User Account Lifecycle Management**. World Congress on Internet Security (WorldCIS-2012) A, 2012.

OWASP. **OWASP - The Open Web Application Security Project**. Disponível em: <https://www.owasp.org/index.php/Main_Page>. Acesso em: 6 abr. 2017.

OWASP, P. et al. **OWASP Top 10 - 2013: Os dez riscos de segurança mais críticos em aplicações web**. 2013.

REGULWAR, G. B.; GULHANE, V. S.; JAWANDHIYA, P. M. **A Security Engineering Capability Maturity Model. 2010** International Conference on Educational and Information Technology, n. Iceit, p. 306–311, 2010a.

RELEASE, P. **CISCO CYBERSECURITY REPORT: CSOS REVEAL TRUE COST OF BREACHES**. Disponível em: <http://www.datacenterjournal.com/cisco-cybersecurity-report-csos-reveal-true-cost-breaches/>.

RIGON, E. A.; WESTPHALL, C. **M. Modelo De Avaliação Da Maturidade Da Segurança Da Informação Information.** Revista Eletrônica de Sistemas de Informaçao, p. 93–104, 2013.

SCARFONE, K.; JANSEN, W.; TRACY, M. Guide to General Server Security Recommendations of the National Institute of Standards and Technology. **Special Publication 800-123**, 2008.

SEI, S. E. I. **CMMI for Development, Version 1.3**. Carnegie Mellon University, n. November, p. 482, 2010.

SERVICES, F. et al. **TG-19, Part 1: Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures**. Test, 1999.

SHIEH, A. et al. **Sharing the Data Center Network**. Nsdi, 2011.

SMITH, H. M. **Red Hat Enterprise Linux Deployment Guide**. 2007.

SPIESS, J. et al. **Business Continuity and Security in Datacenter Interconnection**. Bell Labs Technical Journal, v. 18, n. 4, p. 3–17, 2014.

SWANSON, M.; GUTTMAN, B. **NIST Special Publication 800-14. Generally Accepted**

Principles and Practices for Securing Information Technology Systems. 1996.

TAUBENBERGER, S.; JÜRJENS, J. **IT Security Risk Analysis based on Business Process Models enhanced with Security Requirements**. p. 1–10, 2008.

TIA. TIA Standard ANSI/TIA-942-2005 **Telecommunications Infrastructure Standard for Data Center**. n. April, p. 148, 2005.

UWIZEYEMUNGU, S.; POBA-NZAOU, P. **Understanding Information Technology Security Standards Diffusion**. 2012.

VAULT, C. **Security Hardening Guide for IBM WebSphere Portal**. 2016.

WINOGRAD, T.; TRACY, M.; JANSEN, W. **Guidelines on Securing Public Web Servers Recommendations of the National Institute of Standards and Technology.** NIST Special Publication 800-44, n. 800–44 Version 2, 2007.

WOODHOUSE, S. **An ISMS (im)-maturity capability model**. Proceedings - 8th IEEE International Conference on Computer and Information Technology Workshops, CIT Workshops 2008, n. Im, p. 242–247, 2008.

Quadro 11: Detalhes da Dimensão Server Business Compliance - SBC

Família	Controles	Propósito	Guia de Implementação	ISO/IEC 27002	NIST SP 800-53
SBC 1 - Orientações acerca da Configuração do *Data Center* e o Negócio	SBC 1.1 - Estratégia para Configuração da Segurança do *Data Center*	O proposito do controle Estratégia para Configuração de Segurança do Datacenter é criar um conjunto de políticas de segurança da informação para atender os requisitos entre o *data center* e o negócio.	Convém que este documento seja definido e aprovado pela direção, sendo publicado e comunicado para os gestores de segurança e partes externas relevantes (como por exemplo, provedores de serviço. É importante que o alto nível da organização tenha conhecimento da definição da política de configuração de segurança do *data center*, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança do *data center*. Desta forma atendendo os seguintes requisitos: a) estratégia do negócio; - Quais as informações serão armazenadas no servidor; - Quais as categorias informações serão processadas ou transmitidas através do servidor; - Qual o sistema Operacional adequeado para o datacenter na organização; - Quais são os requisitos de segurança para esta informação; - Será que alguma informação ser lidos ou armazenados em outro host; - Que outro serviço(s) será fornecido pelo servidor; - Quais são os requisitos de segurança para estes serviços adicionais; - Onde na rede o servidor será localizado; b) de regulamentações, legislação e contratos; c) atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança do datacenter para	**A.5.1.1**	**PM-1, SI-1**

			os papéis definidos;		
	SBC 1.2 - Análise Crítica das Políticas para Configuração de Segurança do *Data Center*	O proposíto do controle Análise Crítica das Políticas para Configuração de Segurança do Datacenter é analisar criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia do *data center*.	Convém que a política de segurança do datacenter tenha um gestor de segurança que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação das políticas de segurança do datacenter. Convém que a análise crítica inclua a avaliação de oportunidades para melhoria da política de segurança do datacenter tendo como objetivo responder às mudanças ao ambiente organizacional, às circunstâncias do negócio, às condições legais, ou ao ambiente de tecnologia.	**A. 5.1.2**	**PM-1, SI-1**
	SBC 1.3 - Documentação do Sistema Utilizado no *Data Center*	O proposíto do controle Documentação do Sistema Utilizado no *Data Center* é obter a documentação oficial do sistema utilizado no *data center*, ou	Convém que a documentação a incluam os seguintes requisitos: a) Configuração de Segurança, instalação e operação do sistema, componente ou serviços; b) A utilização eficaz e manutenção das funções / mecanismos de segurança; e	**Nulo**	**SA-5**

		componentes do sistema ou serviço de sistema.	c) Vulnerabilidades conhecidas sobre configurações e uso de funções administrativas do sistema;		
SBC 2 - Conformidade com os Requisitos Legais e Contratuais	SBC 2.1 - Identificação da Legislação e conformidades contratuais	O proposito do controle Identificação da Legislação e conformidades contratuais é Identificar toda a legislação aplicável à organização, para atender aos requisitos relativos ao seu tipo de negócio em conformidade com o uso do servidor.	Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes para uso do servidor, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização. Caso a organização realize tenha implantado servidor (es) em outros país(es) convém que os gestores considerem a conformidade em todos esses países.	**A.18.1.1**	**PM-1, SI-1**
	SBC 2.2 - Direitos de Propriedade Intelectual	O proposito do controle Direitos de Propriedade Intelectual é criar procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de software proprietários.	Convém que sejam Identificada de toda legislação aplicácel ao datacenter como propriedade intelectual: I) O uso legal de produtos de software e de informação; II) Conscientização das políticas para proteger os direitos de propriedade intelectual; III) Controles para assegurar que o número máximo de usuários permitidos, dentro da licença concedida, não está excedido; IV) Somente produtos de software autorizados e licenciados sejam instalados; V) O uso de documentação associada à proteção de licenças quanto à utilização de cópias.	**A.18.1.2**	**CM-10**

	SBC 2.3 - Privacidade nas Informações Pessoais	O proposíto do controle Privacidade nas Informações Pessoais é proteger as informações e identificação pessoal no servidor conforme requerido por legislação e regulamentação pertinente, quando aplicável.	Convém aplicar controles de privacidade consistentes com quaisquer excepções e isenções específicas, incluídas no legislação, ordens executivas, diretrizes, políticas e regulamentos (por exemplo, a aplicação da lei ou considerações de segurança nacional.Política de dados da organização para proteção e privacidade da informação de identificação pessoal, seja desenvolvida e implementada que constarão nos registros do servidor. Esta política deve ser comunicada a todas as pessoas envolvidas no processamento de informação de identificação pessoal, ou até na contratação de funcionário.	**A.18.1.3**	**Nulo**
	SBC 2.4 - Controles de Criptografia	O proposíto do controle Controles de Criptografia é desenvolver uma documentação que garanta a conformidade com as legislações e regulamentações vigentes quanto ao uso de criptografia.	Convêm que os controles de criptografia devam ser usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes. Este deve estar em conformidade com leis e legislações para: I - Restrições à importação e/ou exportação de hardware e software do servidor para execução de funções criptográficas; II) Restrições à importação e/ou exportação de hardware e software de computador que foi projetado para ter funções criptográficas embutidas; III) Restrições no uso de criptografia; IV) Métodos mandatórios ou discricionários de acesso pelas autoridades dos países à informação cifrada por hardware ou software para fornecer confidencialidade ao conteúdo. Criptografia pode ser utilizada para suportar uma variedade de soluções de segurança incluindo, por exemplo, a protecção das informações, assinaturas digitais, geração de números aleatórios e de hash.	**A. 18.1.4**	**IA - 7, SC-13**

SBC 3 - Contratação de Profissionais	SBC 3.1 - Seleção dos Profissionais	O proposíto do controle Seleção dos Profissionais é garantir que os profissionais que irão desempenhar as atividades nas configurações do *data center* tenham capacidade suficiente para atender as atividades de configuração do datacenter desde o nível básico ao mais complexo.	Convém que verificações do histórico sejam realizadas para todos os candidatos a emprego ou convocação, de acordo com a ética, regulamentações e leis relevantes, seja proporcional aos requisitos do negócio, e atenda a demanda e complexidade das atividades nas configurações de segurança do *data center*, incluam os seguintes itens: a) disponibilidade de referências de caráter satisfatórias, por exemplo, uma profissional e uma pessoal; b) uma verificação (da exatidão e completeza) das informações do curriculum vitae do candidato; c) confirmação das qualificações acadêmicas e profissionais; d) verificação independente da identidade (passaporte ou documento similar); e) verificações mais detalhadas, tais como verificações financeiras (de crédito) ou verificações de registros criminais. f) o profissional possui certificação equivalente com as atividades	**A. 7.1.1**	**PS - 3, SA-21**

	SBC 3.2 - Termos e Condições de Contrato	O Proposíto do controle Termos e Condições de Contrato é garantir que as obrigações contratuais com funcionários e partes externas, foram declaradas conforme as suas responsabilidades para atender a organização e a segurança do *data center*.	Convém que as obrigações contratuais para funcionários e partes externas, reflitam as políticas para segurança da informação do *data center*, esclarecendo e declarando:a) que todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis do *data center* assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento do datacenter;b) as responsabilidades legais e direitos dos funcionários e partes externas, e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais e legislação de proteção de dados;c) as responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização, associados com a informação, com os recursos de processamento da informação e com os serviços de informação conduzidos pelos funcionários, fornecedores ou partes externas;d) as responsabilidades dos funcionários ou partes externas, pelo tratamento da informação recebida de outras companhias ou partes interessadas;e) ações a serem tomadas no caso de o funcionário ou partes externas, desrespeitar os requisitos de segurança da informação da organização	**A. 7.1.2**	**PL-4, PS-6**
SBC 4 - Conscientização, e Treinamento para Configuração de Segurança do *Data Center*	SBC 4.1 - Sanções Disciplinares	O proposíto do controle Sanções Disciplinares é criar um processo disciplinar formal que assegura um tratamento justo e correto aos funcionários que são suspeitos de cometer violações de segurança no	Convém que na organização deva existir um processo formal bem definido para tormar ações contra funcionários que tenham cometido violações segurança do *data center*. Importante que o processo disciplinar formal apresente uma resposta de forma gradual, que leve em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio, se este é ou não o primeiro delito, se o infrator foi ou não adequadamente treinado, as legislações relevantes, os contratos do negócio e outros fatores conforme	**A. 7.2.3**	**PS- 8**

		data center.	requerido. Sanções da organização refletem as leis federais, ordens executivas, diretrizes, regulamentos, políticas, normas e Orientações. Processos sanções são descritas em acordos de acesso e pode ser incluído como parte de políticas e procedimentos gerais de pessoal para as organizações.		
	SBC 4.2 - Treinamento em Segurança do *Data Center*	O proposíto do controle Treinamento em Segurança do *Data Center* é o profissional a entender os objetivos da segurança do *data center* e o impacto potencial, positivo e negativo, do seu próprio comportamento na organização, deixando-o consciente e conduzido-o em colaboração com outras atividades de treinamento geral em TI ou treinamento geral em segurança. A organização fornecera treinamento básico de conscientização de segurança aos profissionais que terão contato com o datacenter (incluindo gerentes, executivos seniores, e contratados).	Convém que um programa de treinamento em configuração da segurança do datacenter seja estabelecido alinhado com as políticas e procedimentos relevantes de segurança do datacenter, levando em consideração as informações da organização a serem protegidas e os controles a serem implementados para proteger a informação. O treinamento para segurança do *data center* comteplará: a) Declaração do comprometimento do profissional com a segurança da informação no *data center*; b) A necessidade de tornar conhecido e estar em conformidade com as obrigações e regras para a segurança do datacenter, conforme definido nas políticas, normas, leis, regulamentações, contratos e acordos. c) responsabilidade pessoal por seus próprios atos e omissões, e compromissos gerais para manter seguro ou para proteger a informação que pertença à organização e partes externas. d) procedimentos de segurança da informação básicos (tais como, notificação de incidente no *data center*) e controles básicos (tais como, segurança da senha,	**A. 7.2.2**	**AT-2, AT-3, CP-3, IR-2, PM-13**

			controles contra códigos maliciosos e política de mesa limpa e tela limpa). e) pontos de contato e recursos para informações adicionais e orientações sobre questões de segurança do *data center*, incluindo materiais de treinamento. f) exercícios práticos: podem incluir, por exemplo, engenharia social para coletar as informações, obteção de acesso não autorizado, ou simular o impacto adverso da abertura de anexos de e-mail maliciosos ou através de ataques de spear phishing, links maliciosos.		
SBC 5 - Requisitos do Negócio para Controle de Acesso	SBC 5.1 - Políticas de Controle de Acesso	O proposíto do controle Políticas de Controle de Acesso é determinar regras apropriadas do controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem suas informações no datacenter direta ou indiretamente, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança do *data center*.	Convém que uma declaração nítida dos requisitos do negócio a serem atendidos pelo controle de acesso, seja fornecida aos usuários e provedores de serviços. Este controle aborda o estabelecimento de políticas e procedimentos para o implementação efetiva dos controles de segurança selecionados e melhorias de controle de acesso as informações do datacenter. Este documento inclui:a) requisitos de segurança de aplicações de negócios individuais;b) política para disseminação e autorização da informação, por exemplo, o princípio "necessidade de conhecer" e níveis de segurança e a classificação das informações.c) consistência entre os direitos de acesso e as políticas de classificação da informação em diferentes sistemas e redes;d) legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços;e) gerenciamento de direitos de acesso em um ambiente distribuído e	**A. 9.1.1**	**AC-1**

			conectado à rede que reconhece todos os tipos de conexões disponíveis;f) segregação de funções de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso;g) requisitos para autorização formal de pedidos de acesso.h) requisitos para análise crítica periódica de direitos de acesso.i) remoção de direitos de acesso.j) arquivo dos registros de todos os eventos significantes, relativos ao uso e gerenciamento das identidades do usuário e da informação de autenticação secreta;k) regras para o acesso privilegiado.		
SBC 6 - Classificação da Informação no *Data Center*	SBC 6.1 - Classificação da Informação	O proposíto do controle Classificação da Informação é garantir limites de autorização bem definidas para constitui um pré-requisito para a efetivas decisões de categorização de segurança do datacenter. Descrever os possíveis impactos adversos para as operações do datacenter e indivíduos que utilizarão as informações.	Convêm que as informações do *data center* sejam classificadas em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. Convém que as classficações levem e conta a conformidade com o negócio para compartilhar ou restringir acesso. Importante estabelecer critérios para análise crítica da classificação, e serem avaliados por meio da confidencialidade, integridade e disponibilidade: I - Categoriza informações do datacenter de acordo com a legislação federal aplicável leis, ordens executivas, diretrizes, políticas, regulamentos, normas e orientação; II - Documenta os resultados de categorização de segurança do *data center* (incluindo a justificação de apoio) na segurança planejar para o sistema de informação; III - Garante que o agente responsável pela autorização aprova a decisão de categorização de segurança.	**A. 8.2.1**	**RA-2**

	SBC 6.2 - Rótulos e Tratamento da Informação	O proposíto do controle Rótulos e tratamento da informação é aplicar e uso dos atributos legíveis no que diz respeito a estruturas dos dados internos do *data center*.	Convém que as informações sejam marcadas para definir as limitações da informação. Esta marcação pode não ser necessária em casos em que o *data center* mantenha informações de domínio público. Entretanto, pode se utilizar para realizar marcações para informações públicas, indicando que a informação é de domínio público.	**A. 8.2.2**	**MP-3**
SBC 7 - Documentação dos Procedimentos de Segurança	SBC 7.1 - Responsabilidades e Procedimentos Operacionais	O proposíto do controle Responsabilidades e Procedimentos Operacionais é instânciar um documento que estejam descritos todos os procedimentos de configuração de segurança.	Convém que todo o procedimento de configuração do datacenter seja documentados e disponibilizados aos profissionais/usuários do *data center*. Os procedimentos de configuração incluem: a) a instalação e configuração de sistemas; b) processamento e tratamento da informação, tanto automática como manual; c) cópias de segurança (*backup*); d) requisitos de agendamento, incluindo interdependências com outros sistemas, a primeira hora para início da tarefa e a última hora para o término da tarefa; e) instruções para tratamento de erros ou outras condições excepcionais, que possam ocorrer durante a execução de uma tarefa, incluindo restrições de uso dos utilitários do sistema; h) procedimento para o reinício e recuperação em caso de falha do sistema; i) gerenciamento de trilhas de auditoria e informações de registros (*logs*) de sistemas j) procedimentos de monitoramento.	**A. 12.1.1**	**SA-5**
	SBC 7.2 - Políticas e Procedimentos de Manutenção do *Data Center*	O propósito do controle Políticas e Procedimentos de manutenção do *Data Center* é abordar o estabelecimento de	Convém que sejam criados políticas e procedimentos que refletem as leis federais, ordens executivas, diretrizes, regulamentos, políticas, normas e orientações. A política do *data center* pode ser incluída como parte da política geral de segurança da	**Nulo**	**MA -1**

		políticas e procedimentos para o implementação efetiva dos controles de segurança do *data center*.	informação nas organizações ou, inversamente, pode ser representado por várias políticas que reflitam a natureza complexa de certas organizações.		
	SBC 7.3 - Políticas e Procedimentos de Avaliação de Risco de Configuração do *Data Center*	O propósito do controle Políticas e Procedimentos de Avaliação de Risco do *Data Center* é desenvolver um documento e divulgar abordando os riscos das configurações de segurança do *data center*.	Convém que sejam criadas políticas de avaliação de risco que aborda finalidade, o escopo, papéis, responsabilidades, compromisso de gestão, a coordenação entre as entidades organizacionais e de conformidade para apoiar as configurações do *data center*.	**5.1.1, 5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2**	**RA-1**
SBC 8 - Informação da Arquitetura de Segurança do *Data Center*	SBC 8.1 - Informação da Arquitetura de Segurança do *Data Center*	O propósito do controle Informação da Arquitetura de Segurança do *Data Center* é desenvolver uma arquitetura de configuração do segurança do *data center* e divulgar abordando os riscos das configurações de segurança do *data center*.	Convém que a arquitetura descreva a filosofia geral, os requisitos e abordagem em relação à proteção da confidencialidade, integridade e disponibilidade da informação do *data center*: a) Descreve como a arquitetura de segurança do *data center* é integrado e suporta a arquitetura empresarial; e b) Descreve quaisquer suposições de segurança da *data center* sobre, e dependências em diante, serviços externos; c). Revisões e atualizações da arquitetura de segurança do *data center* para refletir alterações na arquitetura da empresa;	**Nulo**	**PL-8**

Fonte: Elaborado pelo autor. Controles extraídos das normas ISO/IEC 27002 (2013), NIST (2014).

Quadro 12: Detalhes Dimensão Server Operating System Security - SOS

Família	Controles	Proposito	Guia de Implementação	ISO/I	NIST

				EC 27002	SP 800-53
SOS 1 - Segurança no Deploy do Sistema Operacional	SOS 1.1 - Configuração da Partição do Sistema de Arquivos	O proposito do controle Configuração do Sistema de Arquivos é particionar o disco e colocar os principais diretórios em particões separadas, proporcionando uma maior segurança quanto à integridade do Sistema Operacional.	Convém que um sistema de controle de configuração seja utilizado para manter controle da implementação do sistema operacional para proteger a integridade dos dados	**Nulo**	**SC-2**
	SOS 1.2 - Segurança no Bootloader do Sistema Operacional	O proposito do controle Segurança no Bootloader do Sistema Operacional é implementar verificação da integridade com a garantia de que apenas códigos confiáveis são executados durante o processo de inicialização.	Convém implementar técnicas para assegurar a integridade dos processos de inicialização do Sistema Operacional.	**Nulo**	**SI-7**
	SOS 1.3 - Segurança dos Dispositivos de Entrada e Saída do *Data Center*	O proposíto do controle Segurança dos Dispositivos de Entrada e Saída do *Data Center* é Bloquear dispositivos de entrada/saída (I/O) em todos os sistemas que controlam ou armazenam conteúdo, com exceção dos sistemas utilizados para conteúdo I/O.	Convém restringir a instalação e/ou utilização de gravadores de mídia e outros dispositivos com capacidade de saída para sistemas específicos de I/O usados para a saída de conteúdo para mídias físicas.	**A.8.2.3, A.8.3.1, A.11.2.9**	**AC-19, MP-2**
	SOS 1.4 - Restauração do Sistema Operacional	O proposíto do controle Restauração do Sistema Operacional é criar um ponto de restauração para retornar as configurações antigas.	Convém que uma estratégia de retorno às condições anteriores seja disponibilizada antes que mudanças sejam implementadas no sistema.	**A.12.5.1 (e)**	**Nulo**
	SOS 1.5 - Segurança na Memória do Sistema Operacional	O proposíto do controle Segurança na Memória do Sistema Operacional é implementar uma proteção para a memória contra códigos maliciosos.	Convém garantir a segurança para proteger a memória incluindo, por exemplo, a prevenção de execução de dados e espaço de endereços randomizados. Prevenção de execução de dados pode ser imposta por hardware ou com	**Nulo**	**SI-16**

			hardware fornecendo a maior força do mecanismo reforçado por software.		
SOS 2 - Atualização de Patches do Sistema Operacional	SOS 2.1 - Execução por Profissionais Treinados	O proposito do controle Execução por Profissionais Treinados é garantir que toda a atualização do Sistema Operacional seja executada por um profissional treinado ou certificado. Ver (SBC 3.1)	Convém que as atualizações do sistema operacional, aplicativos e bibliotecas de programas sejam executados por administradores treinados e com autorização gerencial apropriada.	**A.12.5 .1 (a)**	**CM-11**
	SOS 2.2 - Teste de Atualização do Sistema Operacional	O proposíto do controle Teste de Atualização do Sistema Operacional para atualizar regularmente os sistemas com patches/atualizações que remediam vulnerabilidades de segurança.	Convém testar os patches em ambiente separado antes da implantação no servidor. Convém verificar se as atualizações estão suas versões estáveis.	**A.12.5 .1 (c)**	**NULL**
	SOS 2.3 - Atualização no Sistema Operacional	O proposíto do controle Atualização no Sistema Operacional é implementar um processo para atualizar regularmente os sistemas (por exemplo, sistemas de transferência de arquivos, sistemas operacionais, bancos de dados, aplicativos, dispositivos de rede) com patches/atualizações que remediam vulnerabilidades de segurança.	Convém que sempre que possível, seja implementar uma ferramenta de gestão de patch centralizada para implantar automaticamente patches para todos os sistemas. Procurar patches de fornecedores e outros terceiros, testar os patches antes da implantação, implementar um processo de exceção e controles de compensação para casos em que haja um caso legítimo de negócios para sistemas sem patch.	**A.12.5 .1**	**CM-5(3)**
SOS 3 - Segurança do Sistema Operacional	SOS 3.1 - Remoção e Desativação de Serviços e Protocolos desnecessários	O proposíto do controle Desinstalação de Serviços Desnecessários e Aplicações é desinstalar os serviços desnecessários e aplicações devem ser desinstaladas de servidores.	Convém que em todos os servidores seja desativado ou desinstalado qualquer serviço, aplicativo ou aplicativo de inicialização que não seja necessário. Convém instalar a configuração mínima do Sistema Operacional, em seguida, adicionar, remover ou desabilitar serviços, aplicações e protocolos de rede conforme necessário.	**NULL**	**CM-1, CM-2**

	SOS 3.2 - Criptografia no Sistema de Arquivo	O proposito do controle Criptografia do Sistema de Arquivo/Unidade de Disco é criptografar conteúdo em sistema de arquivo utilizado pelo sistema operacional.	Convém usar criptografia baseada em um mínimo AES de 128 bits por meio de criptografia baseada em sistema de arquivo.	**A.10.1 .1, 14.1.3**	**SC-13**
	SOS 3.3 - Envio de Chave de Decodificação	O proposito do controle Envio de Chave de Decodificação é enviar chaves ou senhas de decodificação usando um protocolo de comunicação fora da unidade.	Convém enviar chaves ou senhas de decodificação utilizando um método diferente do que aquele que foi utilizado para a transferência do conteúdo. Verificar para garantir que os principais nomes e senhas não estejam relacionados ao projeto ou conteúdo.	**A.10.1 .2**	**SC-12**
SOS 4 - Controle de Acesso	SOS 4.1 - Registro e remoção de usuários	O proposíto do controle Resgistro e Remoção de Usuário é implementar um processo formal de registro e cancelamento de usuários	Convém que o processo para gerenciar o identificador de usuário (ID de usuário) inclua: a) o uso de um ID de usuário único, para permitir relacionar os usuários com suas responsabilidadese ações; o uso compartilhado de ID de usuário somente será permitido, onde eles são necessáriospor razões operacionais ou de negócios e convém que seja aprovado e documentado; b) a imediata remoção ou desabilitação do ID de usuário que tenha deixado à organização; c) a remoção e identificação, de forma periódica, ou a desabilitação de usuários redundantes com ID; d) a garantia de que o ID de usuário redundante não é emitido para outros usuários;	**A.9.2. 1**	**AC-2, IA-2, IA-4, IA-5, IA-8**
	SOS 4.2 - Atribuir Credenciais do Usuário	O proposíto do controle Atribuir Credenciais do Usuário é atribuir credenciais exclusivas com base na necessidade de saber usando os princípios de privilégio mínimo	Convém implementar credenciais com base na necessidade para os seguintes sistemas de informação, no mínimo: a) Sistemas de produção; b) Ferramentas de gerenciamento de conteúdos; c) Ferramentas de transferência de conteúdos;	**A.9.2. 2, A.9.2. 3**	**AC-2, AC-6, IA-4**

			d) Serviços de rede; e) Sistemas de registro e monitoramento; f) Portal web do cliente; g) Sistemas de gestão de contas.		
	SOS 4.3 - Criação de Grupos de Usuário	O proposíto do controle Criação de Grupos de Usuários é implementar as contas do sistema do sistema conforme, funções organizacionais / empresariais.	Convém implementar grupos de usuários do sistema conforme a organização do negócio. (ver SBC-1.1).	**A.9.2.2**	**AC-2**
	SOS 4.4 - Renomear as Contas de administrador	O proposíto do controle Renomear as contas de administrador padrão e limitar o uso dessas contas a situações especiais que requerem essas credenciais.	Convém consultar a documentação de todo o hardware e software para identificar todas as contas padrão, nisto incluem: a) Mudar a senha de todas as contas padrão b) Sempre que possível, mudar o nome de usuário de cada conta. c) Desativar contas de administrador quando não estiverem em uso.	**A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5,**	**AC-2, PE-1**
	SOS 4.5 - Limitação de Acesso nas Estações de Trabalho	O proposíto do controle Limitação de Acesso nas Estações de Trabalho é proibir acesso dos usuários como administradores da rede/servidor em suas próprias estações de trabalho	Convém verificar se a conta de usuário utilizada para acessar a estação de trabalho não tem privilégios de administrador do sistema/rede.	**9.2.1**	**AC-5, SC-2**
	SOS 4.6 - Remoção de Contas Padrão do Sistema	O proposíto do controle Remoção de Contas Padrão do Sistema é desativar ou remover contas locais em sistemas onde tecnicamente é viável.	Convém implementar um serviço centralizado de gerenciamento de contas (ou seja, o servidor de diretório como o LDAP/OpenLDAP ou Active Directory) para autenticar o acesso do usuário aos sistemas de informação.	**A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5,**	**AC-2, PE-2**

				A.9.2.6	
SOS 5 - Autenticação do Usuiário do Sistema Operacional	SOS 5.1 - Senhas Sólidas	O proposíto do controle Senhas Sólidas é implementar senhas com que possam dificultar quaisquer ataques.	Convém implementar controle de senha: a) Extensão mínima de senha de 8 caracteres b) Mínimo de três dos seguintes parâmetros: maiúsculas, minúsculas, números e caracteres especiais c) Duração máxima da senha de 90 dias d) Duração mínima da senha de 1 dia e) Máximo de tentativas inválidas de login de entre 3 e 5 tentativas f) Histórico de senha de dez senhas anteriores	**9.2.4**	**IA-5**
	SOS 5.2 - Usuários e Senhas Exclusivas	O proposíto do controle Usuários e Senhas Exclusivas é reforçar o uso de nomes de usuário e senhas exclusivos para acessar os sistemas do datacenter.	Convém que seja implementado o uso de nomes de usuários e senhas exclusivos para todos os sistemas do datacenter. Convém configurar os sistemas de informação para exigirem autenticação, usando nomes de usuário e senhas exclusivos a um nível mínimo conforme SOS 5.1.	**A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3**	**IA-2, IA-5**
	SOS 5.3 - Criação de Senha de Dois Fatores	O proposíto do controle Criação de Senha de Dois Fatores é implementar senha de dois fatores para acesso remoto na rede.	Convém que seja implementado dois dos seguintes itens para acesso remoto: a) Informação que o indivíduo sabe (por exemplo, a senha, número do PIN); b) Um item físico exclusivo que o indivíduo possui (por exemplo, *token* ou cartão de acesso; c) Uma qualidade física exclusiva do indivíduo (por exemplo, impressão digital, retina).	**A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2**	**AC-17**
	SOS 5.4 - Bloqueio de	O proposíto do controle Bloqueio de Tela por Inatividade é bloquear a tela	Convém configurar servidores e estações de trabalho manualmente ou através de uma	**A.11.2.8,**	**AC-11**

	Tela por Inatividade	após periodo de inatividade.	política para ativar um protetor de tela protegido por senha após um máximo de 5 minutos de inatividade	**A.11.2.9**	
SOS 6 - Segurança de Redes no Sistema Operacional	SOS 6.1 - Responsabilidades Operacionais	O proposíto do controle Responsabilidades Operacionais é implementar um controle para proteger as informações nos sistemas e aplicações	Convém que responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede sejam estabelecidos;	**A.13.1.1(a)**	**AC-20**
	SOS 6.2 - Gerenciamento dos Serviços de Rede	O proposíto do controle Gerenciamento dos Serviços de Rede é implementar um controle para proteger as informações nos sistemas e aplicações.	Convém que atividades de gerenciamento sejam coordenadas para otimizar os serviços para a organização e assegurar que os controles estão aplicados de forma consistente sobre toda a infraestrutura de processamento da informação;	**A.13.1.1(e)**	**AC-17**
	SOS 6.3 - Conexão sobre Sistemas à Rede	O proposíto do controle Controles de Redes-Conexões Sobre Sistemas à Rede é implementar um controle para restringir as conexões de rede do servidor.	Convém que a conexão de sistemas à rede seja restrita.	**A.13.1.1(g)**	**SC-15**
	SOS 6.4 - Registro de Atividades da Rede	O proposíto do controle Controles de Redes-Registro de Atividades Sistemas à Rede é implementar um controle para registrar das conexões da rede.	Convém que sejam aplicados mecanismos apropriados de registro e monitoração para habilitar a gravação e detecção de ações que possam afetar, ou ser relevante para a segurança da informação.	**A.13.1.1(d)**	**AC-3, AC-17**
	SOS 6.6 - Remoção de Conteúdo	O proposíto do controle Remoção de Conteúdo é remover o conteúdo de dispositivos de transferência de conteúdo logo após a transmissão/recepção bem sucedida.	Implementar um processo de remoção de conteúdo dos dispositivos de transferência quando aplicável, remover o acesso de clientes às ferramentas de transferência imediatamente após a conclusão do projeto, confirmar que a conexão está encerrada após o término da sessão.	**A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7**	**MP-6**

	SOS 6.7- Segurança de Serviço de Redes	O proposíto do controle Segurança de Serviço de Redes é implementar mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede, sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.	Convém implementar serviços de rede que incluem o fornecimento de conexões, serviços de rede privados, redes de valor agregado e soluções de segurança de rede gerenciadas como firewalls e sistemas de detecção/prevenção de intrusão.	**A.13.1 .2(d)**	**SC-7(5)**
	SOS 6.8 - Transferência das Informações	O proposíto do controle Transferência das Informações é implementar técnicas de criptografia para transferência das informações.	Convém usar técnicas de criptografia para, por exemplo, proteger a confidencialidade, a integridade e a autenticidade das informações, proteger a informação transferida contra interceptação, cópia, modificação, desvio e destruição, detectar e proteger contra código malicioso que pode ser transmitido através do uso de recursos eletrônicos de comunicação.	**A.13.2 .1**	**CA-3, SA-9**
	SOS 6.9 - Segurança na Resolução de Nomes (Autoritativo)	O proposíto do controle Segurança na Resolução de Nomes (Autoritativo) é fornecer autenticação e verificação de integridade dos artefatos de origem e dados adicionais junto com os dados de resolução de nomes com autoridade. O sistema retorna em resposta ao nome externo as consultas; e fornece os meios para indicar o status de segurança das zonas e permite a verificação de uma cadeia de confiança entre os domínios pai e filho.	Convém que este controle permita que os clientes externos, incluindo, por exemplo, clientes de Internet, para obter garantias de autenticação, origem e verificação de integridade para o nome de host / serviço para informações de resolução de endereço de rede obtida através do serviço. Sistemas de informação que fornecem o nome e endereço resolução serviços incluem, por exemplo, servidores sistema de nome de domínio (DNS). Artefatos adicionais incluem, por exemplo, DNS de segurança (DNSSEC) com assinaturas digitais e chaves criptográficas.	**Nulo**	**SC-20**

	SOS 6.10 - Segurança na Resolução de Nomes (Recursivo)	O proposíto do controle Segurança na Resolução de Nomes (Recursivo) é executar a verificação da integridade de dados de origem e autenticação dos dados sobre as respostas de resolução de nome / endereço do sistema recebendo de fontes autorizadas.	Convém que o servidor tenha autenticado canais para provedores de validação confiáveis. Sistemas de informação que fornecem o nome e endereço resolução serviços para clientes locais incluem, por exemplo, DNS Reverso ou servidores do sistema de nomes de domínio (DNS caching). Resolvedores cliente DNS quer executar a validação de assinaturas DNSSEC, ou clientes usam canais autenticados para resolvedores recursiva que efectuar as validações.	**Nulo**	**SC-21**

Fonte: Elaborado pelo autor. Controles extraídos das normas ISO/IEC 27002 (2013), NIST (2014).

Quadro 13: Detalhes da Dimensão Server Aplication Security - SAS

Família	Controles	Propósito	Guia de Implementação	ISO/IEC 27002	NIST SP 800-53
SAS 1 - Instalação Segura dos Softwares	SAS 1.1 - Política e Procedimento para Aquisição de Software ou Serviço	O propósito do controle Política e Procedimento para Aquisição de Software ou Serviço é facilitar a aquisição do software utilizado *data center*.	Convém que uma política ou procedimento seja implementado para a aquisição do software utilizado no *data center*.	**A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2**	**SA-1**
	SAS 1.2 - Desinstalação de Softwares Desnecessários	O propósito do controle Desinstalação de Serviços Desnecessários e Aplicações é desinstalar os serviços desnecessários e aplicações que devem ser desinstaladas de servidores.	Convém revisar a lista de serviços instalados em todos os servidores de transferência de conteúdo e desinstale ou desative qualquer um que não seja necessário.	**Nulo**	**CM-1, CM-2**
	SAS 1.3 - Atualização dos Softwares e Aplicativos	O proposíto do controle Atualização dos Softwares e Aplicativos é implementar um processo para atualizar regularmente os sistemas.	Convém que sempre que possível, seja implementado uma ferramenta de gestão de patch centralizada para implantar automaticamente patches para todos os sistemas. Procurar patches de fornecedores e terceiros.	**A.12.5.1**	**CM-5, CM-7(4), CM-7(5), CM-11**
	SAS 1.4 - Limite de Privilégio na Operacionalização dos Softwares	O proposíto do controle Limite de Privilégio na Operacionalização dos Softwares é limitar o uso dos softwares no *data center*.	Convém implementar privilégios de acesso para operacionalização dos softwares em uso no *data center*.	**A.12.5.1, A.9.2.3**	**CM 5 (5)**

	SAS 1.5 - Configuração de Software em Ambiente de Teste	O proposíto do controle Configuração de Software em Ambiente de Teste é configurar servidores em ambiente de não produção. Na prática, geralmente há inconsistências entre os ambientes de teste e de produção, que pode resultar em vulnerabilidades.	Convém que os Sofftwares aplicativos somente sejam implementados após testes extensivos e bem sucedidos; é recomendável que os testes incluam testes sobre uso, segurança, efeitos sobre outros sistemas como também sobre uso amigável, e sejam realizados em sistemas separados; Convém que seja assegurado que todas as bibliotecas de código fonte dos programas correspondentes tenham sido atualizadas;	**A.12.5.1**	**CM-5, CM-7(4), CM-7(5), CM-11**
	SAS 1.6 - Execução de Códigos	O proposíto do controle Execução de Códigos é controlar a execução de códigos no sistema operacional do *data center*.	Convém que os sistemas operacionais somente contenham código executável e aprovado, e não contenham códigos em desenvolvimento ou compiladores.	**A.12.5.1**	**CM-5, CM-7(4), CM-7(5), CM-11**
	SAS 1.7 - Contigência dos Softwares	O proposíto do controle Contigência dos Softwares é manter as versões anteriores dos softwares no *data center*.	Convém que versões anteriores dos softwares aplicativos sejam mantidas como medida de contingência.	**A.12.5.1**	**CM-5, CM-7(4), CM-7(5), CM-11**
	SAS 1.8 - Arquivamento dos Softwares	O proposíto do controle Arquivamento dos Softwares é arquivar os softwares anteriores dos softwares no *data center*.	Convém que versões antigas de software sejam arquivadas, junto com todas as informações e parâmetros requeridos, Procedimentos, detalhes de configurações, e software de suporte durante um prazo igual ao prazo de retenção dos dados.	**A.12.5.1**	**CM-5, CM-7(4), CM-7(5), CM-11**
SAS 2 - Restrições aos Recursos do Servidor	SAS 2.1 - Configuração da Partição do Sistema de Arquivos de	O proposito do controle Configuração do Sistema de Arquivos de Software é particionar o disco e colocar os principais diretórios em partições separadas,	Convém que um sistema de controle de configuração seja utilizado para manter controle de tamanho apropriado para utilização de arquivos dos softwares.	**Nulo**	**SC-2**

	Softwares	proporcionando uma maior segurança quanto à integridade do sistema operacional.			
	SAS 2.2 - Controle de Acesso Concorrente	O proposito do controle Controle de Acesso Concorrente é definir um número máximo de acessos simultâneos.	Convém que as organizações limitem o número de sessões simultâneas para administradores de sistema ou indivíduos que trabalham no servidor ou aplicações de missão crítica. Este controle aborda sessões simultâneas para contas do sistema de informação.	**Nulo**	**AC-10**
SAS 3 - Controle de Acesso do Software	SAS 3.1 - Restrições de acesso à informação	O propósito do controle Restrições de acesso à informação é restringir o acesso à informação e funções das aplicações.	Convém que os seguintes controles sejam considerados de forma a apoiar os requisitos de restrição de acesso:a) fornecer menus para controlar o acesso às funções dos sistemas de aplicação;b) controlar quais dados podem ser acessados por um usuário em particular;c) controlar os direitos de acesso dos usuários, por exemplo, ler, escrever, excluir e executar;d) controlar os direitos de acesso de outras aplicações;e) limitar a informação contidas nas saídas;f) prover controles de acesso lógico ou fisico para o isolamento de aplicações sensíveis, dados de aplicação ou sistemas.	**A.9.4.1**	**AC-3, AC-24**
	SAS 3.2 - Segurança no Login do Software	O propósito do controle Segurança no Login do Software é implementar e controlar uma política de acesso à aplicações por um procedimento seguro de login.	Convém que o procedimento de entrada (login) revele o mínimo de informações sobre a aplicação, de forma a evitar o fornecimento de informações, desnecessárias a um usuário não autorizado. Convém que uma técnica de autenticação adequada seja escolhida para validar a identificação alegada de um usuário. Convém que um bom procedimento de	**A.9.4.2**	**AC-7, AC-8, AC-9, IA-6**

			entrada no software: a) não mostre identificadores de sistema ou de aplicação até que o processo tenha sido concluído com sucesso; b) mostre um aviso geral informando que o computador seja acessado somente por usuários autorizados; c) não forneça mensagens de ajuda durante o procedimento de entrada (log-on) que poderiam auxiliar um usuário não autorizado; d) valide informações de entrada no sistema somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não indique qual parte do dado de entrada está correto ou incorreto; e) proteja contra tentativas forçadas de entrada no sistema (*login*); f) registre tentativas de acesso ao sistema, sem sucesso e bem sucedida; g) comunique um evento de segurança caso uma tentativa potencial ou uma violação bem sucedida de entrada no sistema (*login*), seja detectada; h) mostre as seguintes informações quando o procedimento de entrada no sistema (*login*) finalizar com sucesso: 1) data e hora da última entrada no sistema (*login*) com sucesso; 2) detalhes de qualquer tentativa sem sucesso de entrada no sistema (log-on)		

			desde o último acesso com sucesso; i) não mostre a senha que está sendo informada; j) não transmita senhas em texto claro pela rede; k) encerre sessões inativas após um período definido de inatividade, especialmente em locais de alto risco, tais como, locais públicos, ou àreas externas ao gerenciamento de segurança da organização ou quando do uso de dispositivos móveis; l) restrinja os tempos de conexão para fornecer segurança adicional nas aplicações de alto risco e reduzir a janela de oportunidade para acesso não autorizado.		
	SAS 3.3 - Software de Gerenciamento de Senha	O propósito do controle Software de Gerenciamento de Senha é assegurar que senhas sejam de qualidade.	Convém que o sistema de gerenciamento de senha: a) obrigue o uso individual de ID de usuário e senha para manter responsabilidades; b) permita que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros; c) obrigue a escolha de senhas de qualidade; d) obrigue os usuários a mudarem as suas senhas temporárias no primeiro acesso ao sistema; e) force as mudanças de senha a intervalos regulares, conforme necessário; f) mantenha um registro das senhas anteriores utilizadas e bloquei a reutilização; g) não mostre as senhas na tela quando	**A.9.4.3**	**IA-5**

			forem digitadas; h) armazene os arquivos de senha separadamente dos dados do sistema da aplicação; i) armazene e transmita as senhas de forma protegida.		
	SAS 3.4 - Software Utilitários Privilegiados	O propósito do controle Software Utilitários Privilegiados é utilizar programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações sejam restrito e estritamente controlado.	Convém que as seguintes diretrizes para o uso de utilitários de programa que possam ser capazes de sobrepor os controles dos sistemas e as aplicações, sejam consideradas: a) uso de procedimentos de identificação, autenticação e autorização para programas utilitários desistema; b) segregação de programas utilitários dos softwares de aplicação; c) limitação do uso de programas utilitários a um número mínimo de usuários confiáveis e autorizados; d) autorização para uso de programas utilitários não previstos; e) limitação da disponibilidade dos programas utilitários, por exemplo, para a duração de uma modificação autorizada; f) registro de todo o uso de programas utilitários;g) definição e documentação dos níveis de autorização para os programas utilitários; h) remoção ou desabilitação de todos os	**A.9.4.4**	**AC-3, AC-6**

			programas utilitários desnecessários; i) não deixar programas utilitários disponíveis para usuários que têm acesso às aplicações nos sistemas onde a segregação de funções é requerida.		
	SAS 3.5 - Controle ao Código Fonte dos Softwares	O propósito do controle Controle ao Código Fonte dos Softwares é controlar o acesso ao código fonte dos programas e itens associados.	Convém que o acesso ao código-fonte de programas e de itens associados sejam estritamente controlados. Para os códigos-fonte de programas, este controle pode ser obtido com a guarda centralizada do código, de preferência utilizando bibliotecas de programa-fonte. É conveniente que as seguintes orientações sejam consideradas: a) quando possível, convém que seja evitado manter as bibliotecas de programa-fonte no mesmo ambiente dos sistemas operacionais. b) convém que seja implementado o controle do código-fonte de programa e das bibliotecas de programa- fonte, conforme procedimentos estabelecidos; c) convém que o pessoal de suporte não tenha acesso irrestrito às bibliotecas de programa-fonte; d) convém que a atualização das bibliotecas de programa-fonte e itens associados, e a	**A.9.4.5**	**AC-3, AC-6, CM-5**

			entrega de fontes de programas a programadores seja apenas efetuada após o recebimento da autorização pertinente; e) As listagens dos programas sejam mantidas num ambiente seguro; f) convém que seja mantido um registro de auditoria de todos os acessos a código-fonte de programas; g) convém que a manutenção e a cópia das bibliotecas de programa-fonte estejam sujeitas a procedimentos estritos de controles de mudanças.		
SAS 4 - Segurança em Softwares de Transferência de Arquivos	SAS 4.1 - Critografia na Transferência dos Dados	O propósito do controle Criptografia na Transferência dos Dados é implementar uma criptografia para os softwares que utilizam transferência de Arquivos.	Convém implementar nas ferramentas de transferência que usam controles de acesso, um mínimo de criptografia deAES de 128 bits e de autenticação sólida para sessões de transferência de conteúdo.	**A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3**	**IA-5, SC-13**
SAS 5 - Instalação e Configuração de Controles de Segurança Adicionais	SAS 5.1 - Instalação de Software Antivírus	O proposíto do controle Instalação de Software Antivírus é proteger o sistema operacional de possíveis malwares, códigos maliciosos, worms, trojans, spyware e virus que possam incapacitar a funcionalidade do servidor ou colete infromações.	Convém Instalar uma solução corporativa de antivírus com um console de gerenciamento centralizado.	**A.12.2.1**	**SI-3**
	SAS 5.2- Atualização de Software Antivírus	O proposíto do controle Atualização de Software Antivírus é atualizar definições diárias de antivírus.	Convém configurar o console de gerenciamento centralizado de antivírus para baixar e enviar atualizações de definição, pelo menos uma vez por dia.	**A.12.2.1**	**SI-3**
	SAS 5.3 - Execução de Software	O proposíto do controle Execução de Software Antivírus é executar verificações de vírus para permitir a	Convém executar o software antivírus para realizar uma verificação completa do sistema com base na estratégia de antivírus e	**A.12.2.1**	**SI-3**

	Antivírus	verificação/ativação das verificações completas do sistema de vírus para servidores.	onfigurar o software antivírus para executar durante os períodos ociosos.		
	SAS 5.4 - Notificação de falha da Segurança no Software	O proposíto do controle Notificação de falha da Segurança no Software é implementar ou executar verificações dos softwares.	Convém executar notificações previstas pelos sistemas de informação incluem, por exemplo, alertas eletrônicos para administradores de sistema, mensagens para consoles de computador local, e / ou indicações de hardware, como luzes	**Nulo**	**SI-6(1)**
	SAS 5.5 - Verificação Automatizada da Segurança	O proposíto do controle Verificação Automatizada da Segurança é implementar ou executar verificações automatizadas e distribuídas de segurança do sistema operacional.	Convém que o sistema implemente de forma automatizada mecanismos de apoio à gestão de testes de segurança distribuída.	**Nulo**	**SI-6(2)**
	SAS 5.6 - Relatório da Segurança	O proposíto do controle Relatório de Segurança é disponibilizar relatórios de segurança do *data center*.	Convém que sejam emitidos relatórios de segurança para verificação dos resultados junto a, por exemplo, a alta direção da organização.	**Nulo**	**SI-6(3)**

Fonte: Elaborado pelo autor. Controles extraídos das normas ISO/IEC 27002 (2013), NIST (2014).

Quadro 14: Detalhes da Dimensão Server Security Preserving - SSP

Família	Controles	Proposito	Guia de Implementação	ISO/IEC 27002	NIST SP 800-53
SSP 1 - Gestão de Incidente de Segurança do *Data Center*	SSP 1.1 - Responsabilidades e Procedimentos no *Data Center*	O propósito do controle Responsabilidades e Procedimentos do *Data Center* é fornecer a organização com um roteiro para a implementação da sua capacidade de resposta a incidentes no *data center*, descrever a estrutura e organização da capacidade de resposta a incidentes, abordar em alto nível para a forma como a capacidade de resposta a incidentes se encaixa na organização geral. Atende aos requisitos exclusivos da organização quanto o *data center*, que se relacionam com a missão, o tamanho, estrutura e funções, definir os incidentes reportados, e definir o suporte de recursos e de gestão necessárias para efetivamente manter e amadurecer uma capacidade de resposta a incidentes.	Convém que as organizações a desenvolvam e implementem uma abordagem de resposta a incidentes, missões organizacionais, funções de negócio, estratégias, metas e objetivos para resposta a incidentes que ajudam a determinar a estrutura das capacidades de resposta a incidentes. As responsabilidades pelo gerenciamento serão estabelecidas para assegurar que os seguintes procedimentos são desenvolvidos e comunicados, de forma adequada: a) responsabilidades pelo gerenciamento sejam estabelecidas para assegurar que os seguintes procedimentos são desenvolvidos e comunicados, de forma adequada, dentro da organização: 1) procedimentos para preparação e planejamento a respostas a incidentes; 2) procedimentos para monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação; 3) procedimentos pra registros das atividades de gerenciamento de incidentes; 4) procedimentos para tratamento para evidências forenses; 5) procedimentos para avaliação e decisão dos eventos de segurança da informação e avaliação de fragilidades de segurança da	**A. 16.1.1**	**IR-8**

			informação; 6) procedimentos para resposta, incluindo aquelas relativas a escalação, recuperação controlada de um incidente e comunicação as pessoas ou organizações relevantes, internas e externas. b) procedimentos estabelecidos assegurem que: 1) pessoal competente trata as questões relativas a incidentes de segurança dentro da organização; 2) um ponto de contato para notificação e detecção de incidentes de segurança está implementado; 3) contatos apropriados são mantidos com autoridades, grupos de interesses externos ou fóruns que tratam de questões relativas a incidentes de segurança da informação. c) convém que procedimentos de notificação incluam: 1) preparação de formulários de notificação de evento de segurança da informação para apoiar as ações de notificação e ajudar a pessoa que está notificando, lembrando de todas as ações necessárias no caso de um evento de segurança da informação; 2) o procedimento a ser realizado no caso de um evento de segurança da informação, por exemplo relatar todos os detalhes (tipo de não conformidade ou violação, mau funcionamento, mensagens na tela, comportamento estranho) imediatamente; e não		

			tomar nenhuma ação sozinho, porém notificar imediatamente ao ponto de contato, tomando apenas ações coordenadas; 3) referência a um processo disciplinar formal estabelecido para tratar com funcionários que cometam violações de segurança da informação; 4) processo de realimentação adequado para assegurar que aquelas pessoas que notificaram um evento de segurança da informação são informadas dos resultados após o assunto ter sido tratado e encerrado.		
	SSP 1.2 - Notificação de fragilidade do Sistema do *Data Center*	O propósito do controle Notificação de fragilidade do Sistema do *Data Center* é identificar no datacenter, falhas de software, incluindo vulnerabilidades potenciais resultantes dessas falhas, e relatar essa informação ao gestor de segurança responsável. Atualizações de software relevantes para a segurança incluem, por exemplo, *pacthes*, *services packes*, *packages*, *hot fixes* e *antivírus*. As organizações também podem tratar falhas descobertas durante as avaliações de segurança.	Convém que os funcionários e partes externas que usam os sistemas e serviços do datacenter na organização, precisam ser instruídos a registrar e notificar quaisquer fragilidades de segurança da informação suspeita ou observada, nos sistemas ou serviços. Este controle também atribui: a) Identificação, relatórios e correção de falhas de sistemas no *data center*; b) Testes de software e atualizações de firmware. c) Instalação de softwares de segurança relevantes e atualizações de firmware no prazo de liberação das atualizações.	**A. 16.1.3**	**SI - 2**

	SBC 1.3 - Avaliação e Decisão dos Eventos de Segurança do *Data Center*	O propósito do controle Avaliação e Decisão dos Eventos de Segurança do *Data Center* é auditar, análisar e relatar informações de auditoria relacionadas à segurança realizada por organizações, incluindo, por exemplo, a auditoria que resulta num monitoramento do uso da conta, acesso remoto e definições de configuração.	Convém a gestão de segurança avaliar cada evento de segurança da informação usando uma escala de classificação de incidentes e eventos de segurança da informação no *data center*, para decidir se é recomendado que o evento seja classificado como um incidente de segurança da informação. A priorização e a classificação de incidentes podem ajudar a identificar o impacto e a abrangência de um incidente. É necessário que os resultados na analise sejam registradas, a fim de obter uma melhor verificação e referência futura. Como resultados podem ser comunicados às entidades organizacionais que incluem, por exemplo, a equipe de resposta a incidentes, *help desk*, grupo de segurança da informação/departamento. Se a organização está proibida de revisar e anslisar as informações, auditar ou é incapaz de realizar tais atividades, a revisão/análise pode ser realizada por outras organizações que tenham capacidade e competência.	**A. 16.1.4**	**AU-6, IR-4**
	SSP 1.4 - Resposta aos incidentes de segurança do *Data Center*	O propósito do controle Resposta aos Incidentes de Segurança do *Data Center* é estabelecer uma comunicação com pessoas relevantes na organização para responder aos incidentes de segurança no *data center*.	Convém que os incidentes de segurança da informação no *data center* sejam reportados para um ponto de contato definido e outras pessoas relevantes da organização, ou ainda, partes externas.Convém que a notificação inclua os seguintes itens: a) coleta de evidências, tão rápido quanto possível, logo após a ocorrência; b) realização de análise forense de segurança da informação, conforme requerido c) escalação, conforme requerido;	**A. 16.1.5**	**IR-4**

			d) garantia de que todas as atividades de respostas envolvidas são adequadamente registradas paraanálise futura; e) comunicação da existência de incidente de segurança da informação ou qualquer detalhe relevantepara pessoas internas ou externas, ou organizações que precisam tomar conhecimento; f) tratamento com as fragilidades de segurança da informação encontradas que causem oucontribuam para o incidente; g) uma vez que o incidente foi, de forma bem sucedida, formalmente tratado, encerrar o incidente e registrá-lo.		
SSP 2 - Registro e Monitoramento	SSP 2.1 - Sistemas de Relatórios e Registros em Tempo Real	O propósito do controle Sistemas de Relatórios e Registros em Tempo Real é implementar sistemas de relatórios e registros em tempo real para registrar e relatar os eventos de Segurança.	Convém que os registros (logs) de eventos incluam, quando relevante: a) identificação dos usuários (ID); b) atividades do sistema; c) datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (log-on) e saída (log-off) no sistema; d) identidade do dispositivo ou sua localização quando possível e o identificador do sistema; e) registros das tentativas de acesso ao sistema, aceitas e rejeitadas; f) registros das tentativas de acesso a outros recursos e dados, aceitos e rejeitados; g) alterações na configuração do sistema; h) uso de privilégios; i) Uso de aplicações e utilitários do sistema; j) arquivos acessados e o tipo de acesso; k) endereços e protocolos de rede; l) alarmes provocados pelo sistema de controle	**A.12.4.1**	**AU-3, AU-6, AU-11, AU-12, AU-14**

			de acesso; m) ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção de intrusos; n) registros de transações executadas pelos usuários nas aplicações.		
	SSP 2.2 - Proteção da Informação Auditada	O propósito do controle Proteção da Informação Auditada é proteger as informações dos registros de eventos (log) e seus recursos contra acesso não autorizado e adulteração.	Convém que os controles implementados objetivem a proteção contra codificações não autorizadas às informações dos (logs) e problemas operacionais com os recursos dos registros (log), tais como: - Alterações dos tipos de mensagens que são gravadas; - Arquivos de registros (log) sendo editados ou excluídos; - Capacidade de armazenamento da mídia magnética do arquivo de registros (log) excedida, resultando em falhas no registro de eventos ou sobreposição do registro de evento anterior.	**A.12.4.2**	**AU-9**
	SSP 2.3 - Registro dos Administradores e Operadores do *Data Center*.	O propósito do controle Registro dos Administradores e Operadores do *Data Center* registrar as atividades privilegiadas.	Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares.	**A.12.4.3**	**AU-9, AU-12**
	SSP 2.4 -	O propósito do controle Retenção	Convém Armazenar os registros de conteúdo	**A.12.4.1,**	**AU-11**

	Retenção de Registros	de Registros é armazenar conteúdo de um servidor por um período específico.	em um servidor centralizado que possa ser acessado somente por usuários específicos.	**A.16.1.7**	
	SSP 2.5 - Sincronização do Relógio	O propósito do controle Sincronização do Relógio é gerar registros de tempo para apoiar auditoria de sistemas.	Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa. O ajuste correto dos relógios dos computadores é importante para garantir a exatidão dos registros (log) de auditoria, que podem ser requeridos para investigações ou como evidências em casos legais ou disciplinares. Registros (log) de auditoria incorretos podem dificultar tais investigações e causar danos à credibilidade dessas evidências. Um relógio interno ligado ao relógio atômico nacional via transmissão de rádio pode ser utilizado como relógio principal para os sistemas de registros (logging). O protocolo de hora da rede pode ser utilizado para sincronizar todos os relógios dos servidores com o relógio principal	**A.12.4.1**	**AU-8**
SSP 3- Auditoria	SSP 3.1 - Capacidade de Auditoria	O propósito do controle Capacidade de Auditoria é verificar se se a organização é capaz de auditar os eventos de segurança do *Data Center*.	Convém que as organizações identifiquem eventos de auditoria como àqueles que são significativos e relevantes para a segurança do sistema do datacenter, suas configurações e os ambientes em que esses sistemas operam de forma a atender às necessidades específicas de auditoria e em curso. Eventos de auditoria podem incluir, por exemplo, alterações de senha, não logons, ou não acessa relacionada aos sistemas de informação, de uso administrativo privilégio, de uso de	**Nulo**	**AU-2**

			credenciais, ou uso de credenciais de terceiros. Ao determinar o conjunto de eventos auditáveis, as organizações consideram a adequada auditoria para cada um dos controles de segurança a serem implementadas.		
	SSP 3.2 - Auditoria e Geração de Relatórios Otimizados	O propósito do controle Auditoria e Geração de Relatórios Otimizados é implementar uma forma de resumo dos artefatos (simplicar) auditados.	Convém que o *data center* gere informações de auditoria recolhidas e organizadas em um formato resumido que é mais significativo para os analistas. Esta capacidade de reduzir a geração destes relatórios nem sempre vêm do mesmo sistema de informação ou junto das mesmas entidades organizacionais que realizam atividades de auditoria. Capacidade de redução de auditoria pode incluir, por exemplo, modernas técnicas de mineração de dados com filtros avançados de dados para identificar o comportamento anômalo em registros.	**Nulo**	**AU-7**
	SSP 3.3 - Auditoria Alternativa	O propósito do controle Auditoria Alternativa é o datacenter ter a capacidade de auditar por meios alternativos em caso de falha.	Convém que seja implementado uma capacidade de auditoria alternativa de curto prazo, até a falha no recurso de auditoria principal seja corrigida. As organizações podem determinar que a capacidade de auditoria alternativa só precise fornecer um subconjunto da funcionalidade de auditoria primário que é impactado pela falha.	**Nulo**	**AU-13**
SSP 4 - Backup	SSP 4.1 - Cópias de Segurança - Completude e Exatidão das Cópias	O propósito do controle Cópias de Segurança - Completude e Exatidão das Cópias é o gerar cópias completas e exatas das informações do *data center*.	Convém que os registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação, os quais convêm que sejam produzidos.	**A. 12.3.1(a)**	**CP-9**

	SSP 4.2 - Cópias de Segurança - Abrangência e Frequência	O propósito do controle Abrangência e Frequência é o de gerar cópias com abragência e frequência regular das informações do *data center*.	Convém que a frequência da geração das cópias de segurança do datacenter reflitam os requisitos de negócio da organização, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização;	**A. 12.3.1(b)**	**CP-9**
	SSP 4.3 - Cópias de Segurança - Armazenamento Remoto	O propósito do controle Cópias de Segurança - Armazenamento Remoto é o gerar cópias em local remoto.	Convém que as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal.	**A. 12.3.1(c)**	**CP-9(3)**
	SSP 4.4 - Cópias de Segurança - Criptografia	O propósito do controle Cópias de Segurança - Criptografia é criptografar as cópias geradas.	Convém que em situações onde a confidencialidade seja importante, convém que cópias de segurança sejam protegidas através de encriptação.	**A. 12.3.1(d)**	**CP-9**
SSP 5 - Redundância	SSP 5.1 - Disponibilidade dos Recursos de Configuração do *Data Center*	O propósito do controle Disponibilidade dos Recursos de Configuração do *Data Center* é assegurar a disponibilidade dos recursos de processamento da informação no *data center*.	Convém que os recursos de processamento da informação no *data center* sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade nas configurações.	**A. 17.2.1**	**CP-2,CP-6, CP-7**
SSP 6 - Teste de Segurança do *Data Center*	SSP - 6.1 - Autorização para Ambiente de Teste	O proposíto do controle Autorização para Ambiente de Teste é estabelecer autorização para uso da cópia da informação *data center*	Convém que seja obtida autorização cada vez que for utilizada uma cópia da informação operacional para uso em ambiente de teste.	**A.14.3.1(b)**	**Nulo**
	SSP - 6.2- Exclusão dos Dados no Ambiente de Teste	O proposíto do controle Exclusão dos Dados no Ambiente de Teste é excluir as informações utilizadas no ambiente de teste.	Convém que a informação operacional seja apagada do ambiente de teste, imediatamente após finalizar os testes.	**A.14.3.1(c)**	**Nulo**
	SSP - 6.3 - Registro do Uso dos Dados no	O proposíto do controle Registro do Uso dos Dados no Ambiente de Teste é registrar todo o uso das	Convém que a cópia e o uso de informação operacional sejam registrados de forma a prover uma trilha para auditoria;	**A.14.3.1(d)**	**Nulo**

	Ambiente de Teste	informaçãos no Ambiente de Teste.			
	SSP 6.4 - Scanning de Vulnerabilidades	O proposíto do controle Scanning de Vulnerabilidades é verifica a existência de vulnerabilidades no sistema do *Data Center* e aplicações hospedadas.	Convém que sejam implementadas ferramentas e técnicas que facilitam a interoperabilidade entre as ferramentas e automatize partes do processo de gerenciamento de vulnerabilidades usando padrões de varredura.	**Nulo**	**RA -5**
	SSP 6.5 - Teste de Penetração	O proposíto do controle Teste de Penetração é analisar e verificar vulnerabilidades exploradas por atacantes.	Convém simular as ações dos potenciais atacantes na realização de ataques cibernéticos hostis contra organizações e fornece uma análise mais aprofundada das fraquezas / deficiências relacionadas à segurança. As organizações também podem usar os resultados das análises de vulnerabilidade para apoiar as atividades de teste de penetração. Os testes de penetração podem ser realizados sobre os componentes de hardware, software ou firmware de um sistema de informação e pode exercer ambos os controles de segurança física e técnica.	**Nulo**	**CA- 8**

Fonte: Elaborado pelo autor. Controles extraídos das normas ISO/IEC 27002 (2013), NIST (2014).

APÊNDICE B. PONTUAÇÕES OBTIDAS

Apêndice B.1. Pontuações Obtidas no Estudo de Caso 1

Quadro 15: Pontuações Obtidas no Estudo de Caso 1 - Dimensão Server Business Compliance

Família	Controles	EV	Evidência	CW	OW
SBC 1 - Orientações acerca da Configuração do *Data Center* e o Negócio	SBC 1.1 - Estratégia para Configuração da Segurança do *Data Center*	1	Existem apenas regras estabelecidas pela detentora da franquia quanto o tipo de servidor.	2	5
	SBC 1.2 - Análise Crítica das Políticas para Configuração de Segurança do *Data Center*	0	Inexistente	2	4
	SBC 1.3 - Documentação do Sistema Utilizado no *Data Center*	4	Toda a documentação do Windows Server 2012 R2 está de posse da organização.	1	4
SBC 2 - Conformidade com os Requisitos Legais e Contratuais	SBC 2.1 - Identificação da Legislação e conformidades contratuais	2	Só existe a configuração de hardware e alguns softwares	2	5
	SBC 2.2 - Direitos de Propriedade Intelectual	4	Todos os softwares e o sistema operacionais são originais e contém suas devidas docuemtnações.	2	5
	SBC 2.3 - Privacidade nas Informações Pessoais	0	Inexistente	1	4
	SBC 2.4 - Controles de Criptografia	0	Inexistente	2	5
SBC 3 - Contratação de Profissionais	SBC 3.1 - Seleção dos Profissionais	1	O profissional possui algumas certificações, porém estão vencidas.	2	4
	SBC 3.2 - Termos e Condições de Contrato	0	Inexistente.	2	5
SBC 4 - Conscientização, e Treinamento para Configuração de Segurança do *Data Center*	SBC 4.1 - Sanções Disciplinares	0	Inexistente	2	5
	SBC 4.2 - Treinamento em Segurança do *Data Center*	0	Inexistente	2	5
SBC 5 - Requisitos do Negócio para Controle de	SBC 5.1 - Políticas de Controle de Acesso	0	Inexistente	2	5

Acesso					
SBC 6 - Classificação da Informação no *Data Center*	SBC 6.1 - Classificação da Informação	0	Inexistentte	2	5
	SBC 6.2 - Rótulos e tratamento da informação	1	Existe um software para realização de rotulamento, porém não foi implatando.	2	4
SBC 7 - Documentação dos Procedimentos de Segurança	SBC 7.1 - Responsabilidades e Procedimentos Operacionais	0	Inexistente	2	4
	SBC 7.2 - Políticas e Procedimentos de Manutenção do *Data Center*	0	Inexistente	1	5
	SBC 7.3 - Políticas e Procedimentos de Avaliação de Risco de Configuração do *Data Center*	0	Inexistente	2	5
SBC 8 - Informação da Arquitetura de Segurança do *Data Center*	SBC 8.1 - Informação da Arquitetura de Segurança do *Data Center*	0	Inexistente	1	5

Fonte: Elaborado pelo autor.

Quadro 16: Pontuações Obtidas no Estudo de Caso 1 - Dimensão Server Security Operating System

Família	Controles	EV	Evidence	CW	OW
SOS 1 - Segurança no Deploy do Sistema Operacional	SOS 1.1 - Configuração da Partição do Sistema de Arquivos	4	Existe um disco exclusivo para o sistema de arquivos, e outro para os aplicativos.	1	5
	SOS 1.2 - Segurança no Bootloader do Sistema Operacional	0	Inexistentte	1	4
	SOS 1.3 - Segurança dos Dispositivos de Entrada e Saída do *Data Center*	0	Inexistentte	2	3
	SOS 1.4 - Restauração do Sistema Operacional	0	Inexistentte	1	4
	SOS 1.5 - Segurança na Memória do Sistema Operacional	0	Inexistentte	1	3
SOS 2 - Atualização de	SOS 2.1 - Execução por Profissionais Treinados	0	Inexistentte	2	5

Patches do Sistema Operacional	SOS 2.2 - Teste de Atualização do Sistema Operacional	0	Inexistentte	1	4
	SOS 2.3 - Atualização no Sistema Operacional	4	É utilizado o Windows Update frenquentemente.	2	4
SOS 3 - Segurança do Sistema Operacional	SOS 3.1 - Remoção e Desativação de Serviços e Protocolos desnecessários	4	Serviços desnecessários foram removidos do servidor.	1	5
	SOS 3.2 - Criptografia no Sistema de Arquivo	0	Inexistentte	2	3
	SOS 3.3 - Envio de Chave de Decodificação	0	Inexistentte	2	3
SOS 4 - Controle de Acesso	SOS 4.1 - Registro e Remoção de Usuários	2	Existe um registro formal, porém realizado pela empresa NSR, que é contratada pela detentora da franquia.	2	5
	SOS 4.2 - Atribuir Credenciais do Usuário	0	Inexistentte	2	5
	SOS 4.3 - Criação de Grupos de Usuário	0	Inexistentte	2	5
	SOS 4.4 - Renomear as contas de administrador	0	Inexistentte	2	4
	SOS 4.5 - Limitação de Acesso nas Estações de Trabalho	2	Os usuários acessam apenas os softwares de frente de loja. Entretanto o terminal permite conexão de dispositivos via USB.	2	5
	SOS 4.6 - Remoção de Contas Padrão do Sistema	0	Inexistentte	2	5
SOS 5 - Autenticação do Usuiário do Sistema Operacional	SOS 5.1 - Senhas Sólidas	0	Inexistentte	2	5
	SOS 5.2 - Usuários e Senhas Exclusivas	0	Inexistentte	2	4
	SOS 5.3 - Criação de Senha de Dois Fatores	0	Inexistentte	2	1
	SOS 5.4 - Bloqueio de Tela por Inatividade	4	Já vem por padrão no Windows Server 2012.	2	4
SOS 6 - Segurança de Redes no Sistema Operacional	SOS 6.1 - Responsabilidades Operacionais	0	Inexistentte	2	4
	SOS 6.2 - Gerenciamento dos Serviços de Rede	0	Inexistentte	2	4

	SOS 6.3 - Conexão sobre Sistemas à Rede	4	Todos os serviços de rede são através de VPN com login e senha.	2	5
	SOS 6.4 - Registro de Atividades da Rede	2	Existe apenas o software padrão do Windows Server 2012 R2, Event Viewer.	2	5
	SOS 6.6 - Remoção de Conteúdo	0	Inexistentte	2	5
	SOS 6.7- Segurança de Serviço de Redes	0	Inexistentte	2	5
	SOS 6.8 - Transferência das Informações	0	Inexistentte	2	3
	SOS 6.9 - Segurança na Resolução de Nomes (Autoritativo)	0	Inexistentte	1	3
	SOS 6.10 - Segurança na Resolução de Nomes (Recursivo)	0	Inexistentte	1	3

Fonte: Elaborado pelo autor.

Quadro 17: Pontuações Obtidas no Estudo de Caso 1 - Dimensão Server Application Security

Família	Controles	EV	Evidencia	CW	OW
SAS 1 - Instalação Segura dos Softwares	SAS 1.1 - Política e Procedimento para Aquisição de Software ou Serviço	3	A detentora da franquia PIZZA HUT utiliza uma Política de softwares homologados. Esta documentação é padrão em todas as lojas no brasil. Nenhum software pode ser adiquirido sem esse procedimento. Um problema foi encontrado, pois não é possível adquirir outros softwares de mesma qualidade ou superior.	2	4
	SAS 1.2 - Desinstalação de Softwares Desnecessários	4	Todos os softwares são utilizados pelo servidor. Não foi encontrado algum software que não estivesse sendo utilizado.	1	5
	SAS 1.3 - Atualização dos Softwares e Aplicativos	2	Existe uma gestão de atualização de patches, mas de forma em que o gerente de TI não tem respostas das atualizações por parte dos fornecedores.	2	5
	SAS 1.4 - Limite de Privilégio na Operacionalização dos Softwares	0	Inexistente.	2	5
	SAS 1.5 - Configuração de Software em Ambiente de Teste	0	Inexistente.	2	5
	SAS 1.6 - Execução de Códigos	4	Todos os softwares são homologados.	2	5
	SAS 1.7 - Contigência dos Softwares	0	Inexistente.	2	4
	SAS 1.8 - Arquivamento dos Softwares	1	Só existe arquivamento do Windows Server 2012 R2.	2	3

SAS 2 - Restrições aos Recursos do Servidor	SAS 2.1 - Configuração da Partição do Sistema de Arquivos de Softwares	4	Existem dois HD´s. Um exclusivo para o sistema e outro para o sistema operacional.	1	5
	SAS 2.2 - Controle de Acesso Concorrente	0	Inexistente.	1	4
SAS 3 - Controle de Acesso do Software	SAS 3.1 - Restrições de acesso à informação	0	Inexistente.	2	4
	SAS 3.2 - Segurança no Login do Software	1	Existência algumas medidas, porém são realizdaas de maneira trivial.	2	3
	SAS 3.3 - Software de Gerenciamento de Senha	0	Inexistente.	2	5
	SAS 3.4 - Software Utilitários Privilegiados	4	Existe uma partição para os softwares utilitários	2	4
	SAS 3.5 - Controle ao Código Fonte dos Softwares	4	Todos os softwares são homologados e descritos em contrato com a detentora da franquia. obs: o ponto f) não é utilizado para esta avaliação.	2	5
SAS 4 - Segurança em Softwares de Transferência de Arquivos	SAS 4.1 - Critografia na Transferência dos Dados	4	Toda a transação no servidor é via VPN. Essas medidas estão inclusos no protocolo da detentora da franquia.	2	5
SAS 5 - Instalação e Configuração de Controles de Segurança Adicionais	SAS 5.1 - Instalação de Software Antivírus	0	Inexistente	2	5
	SAS 5.2- Atualização de Software Antivírus	0	Inexistente	2	5
	SAS 5.3 - Execução de Software Antivírus	0	Inexistente	2	5

	SAS 5.4 - Notificação de falha da Segurança no Software	0	Inexistente	1	5
	SAS 5.5 - Verificação Automatizada da Segurança	0	Inexistente	1	3
	SAS 5.6 - Relatório da Segurança	0	Inexistente	1	5

Fonte: Elaborado pelo autor.

Quadro 18: Pontuações Obtidas no Estudo de Caso 1 - Dimensão Server Security Preserving

Família	Controles	EV	Evidencia	CW	OW
SSP 1 - Gestão de Incidente de Segurança do *Data Center*	SSP 1.1 - Responsabilidades e Procedimentos no *Data Center*	0	Inexistente.	2	5
	SSP 1.2 - Notificação de fragilidade do Sistema do *Data Center*	0	Inexistente.	2	5
	SBC 1.3 - Avaliação e Decisão dos Eventos de segurança do *Data Center*	0	Inexistente.	2	5
	SSP 1.4 - Resposta aos Incidentes de Segurança do *Data Center*	3	Alguns incidentes são reportados para a detentora da franquia, porém não se obteve resposta ou o andamento do processo.	2	5
SSP 2 - Registro e Monitoramento	SSP 2.1 - Sistemas de Relatórios e Registros em Tempo Real	1	Inexistente.	2	5
	SSP 2.2 - Proteção da Informação Auditada	1	Inexistente.	2	5
	SSP 2.3 -Registro dos Administradores e Operadores do *Data Center*.	3	O Windows Server já registra todos os acessos dos administradores.	2	5

	SSP 2.4 - Retenção de Registros	0	Inexistente.	2	5
	SSP 2.5 - Sincronização do Relógio	4	Por padrão o Windows Server já utilizado um servidor NTP padrão da Microsoft.	2	5
SSP 3- Auditoria	SSP 3.1 - Capacidade de Auditoria	3	É possível auditar eventos quando está relacionado com o próprio usuário. Entretando com os usuários fornecedores isso não é possivel	1	5
	SSP 3.2 - Auditoria e Geração de Relatórios Otimizados	0	Inexistente.	1	5
	SSP 3.3 - Auditoria Alternativa	0	Inexistente.	1	5
SSP 4 - Backup	SSP 4.1 - Cópias de Segurança - Completude e Exatidão das Cópias	4	Toda a base de backup é em nuvem, por recomendação da detentora da franquia.	2	5
	SSP 4.2 - Cópias de Segurança - Abrangência e Frequência	4	Todos os backups são diários.	2	5
	SSP 4.3 - Cópias de Segurança - Armazenamento Remoto	4	Toda a base de backup é em nuvem, por recomendação da detentora da franquia.	2	5
	SSP 4.4 - Cópias de Segurança - Criptografia	3	Há um grau de inconsistência no artefato, faltam informações precisas de onde é gerado o backup.	2	4
SSP 5 - Redundância	SSP 5.1 - Disponibilidade dos Recursos de Configuração do *Data Center*	0	Inexistente.	2	5

SSP 6 - Teste de Segurança do Datacenter	SSP - 6.1 - Autorização para Ambiente de Teste	1	Inexistente.	1	5
	SSP - 6.2- Exclusão dos Dados no Ambiente de Teste	1	Inexistente.	1	4
	SSP - 6.3 - Registro do Uso dos Dados no Ambiente de Teste	0	Inexistente.	1	5
	SSP 6.4 - Scanning de Vulnerabilidades	0	Inexistente.	1	5
	SSP 6.5 - Teste de Penetração	0	Inexistente.	1	5

Fonte: Elaborado pelo autor.

Apêndice B.2. Pontuações Obtidas no Estudo de Caso 2

Quadro 19: Pontuações Obtidas no Estudo de Caso 2 - Dimensão Server Business Compliance

Família	Controles	EV	Evidência	CW	OW
SBC 1 - Orientações acerca da Configuração do Datacenter e o Negócio	SBC 1.1 - Estratégia para Configuração da Segurança do *Data Center*	1	O openredu apenas recebeu da ATI informações sobre qual o sistema operacional, quantidade de armazenamento e memória disponíveis.	2	3
	SBC 1.2 - Análise Crítica das Políticas para Configuração de Segurança do *Data Center*	0	Inexistente	2	4
	SBC 1.3 - Documentação do Sistema Utilizado no *Data Center*	3	O openredu tem disponível pela empresa Canonical todos os detalhes do Ubuntu.	1	5
SBC 2 - Conformidade com os Requisitos Legais e Contratuais	SBC 2.1 - Identificação da Legislação e conformidades contratuais	3	Tanto o Sistema Operacional, como as aplicações tem licença de uso GLP2.	2	4
	SBC 2.2 - Direitos de Propriedade Intelectual	4	Tanto o Sistema Operacional, como as aplicações tem licença de uso GLP2.	2	1
	SBC 2.3 - Privacidade nas Informações Pessoais	0	Inexistente	1	3

	SBC 2.4 - Controles de Criptografia	0	Inexistente	2	4
SBC 3 - Contratação de Profissionais	SBC 3.1 - Seleção dos Profissionais	0	Inexistente	2	5
	SBC 3.2 - Termos e Condições de Contrato	0	Inexistente	2	5
SBC 4 - Conscientização, e Treinamento para Configuração de Segurança do *Data Center*	SBC 4.1 - Sanções Disciplinares	0	Inexistente	2	4
	SBC 4.2 - Treinamento em Segurança do *Data Center*	0	Inexistente	2	5
SBC 5 - Requisitos do Negócio para Controle de Acesso	SBC 5.1 - Políticas de Controle de Acesso	0	Inexistente	2	3
SBC 6 - Classificação da Informação no Datacenter	SBC 6.1 - Classificação da Informação	0	Inexistente	2	3
	SBC 6.2 - Marcação da Informação	0	Inexistente	2	4
SBC 7 - Documentação dos Procedimentos de Segurança	SBC 7.1 - Responsabilidades e Procedimentos Operacionais	0	Inexistente	2	5
	SBC 7.2 - Políticas e Procedimentos de Manutenção do *Data Center*	0	Inexistente	1	3
	SBC 7.3 - Políticas e Procedimentos de Avaliação de Risco de Configuração do *Data Center*	0	Inexistente	2	3
SBC 8 - Informação da Arquitetura de Segurança do *Data Center*	SBC 8.1 - Informação da Arquitetura de Segurança do *Data Center*	0	Inexistente	1	4

Fonte: Elaborado pelo autor.

Quadro 20: Pontuações Obtidas no Estudo de Caso 2 - Dimensão Server Security Operating System

Família	Controles	EV	Evidence	CW	OW
SOS 1 - Segurança no Deploy do Sistema Operacional	SOS 1.1 - Configuração da Partição do Sistema de Arquivos	4	Os diretórios do sistema de arquivos, /var/ /dev/ /boot /tmp /mnt /var /usr foram particionados de maneira correta.	1	4

	SOS 1.2 - Segurança no Bootloader do Sistema Operacional	4	A ATI mantém um ambiente seguro quanto ao Bootloader no Ubuntu server, por utilizar um gerenciador seguro de maquinas virtuais. Além disso o Bootloader GRUB foi configurado corretamente.	1	3
	SOS 1.3 - Segurança dos Dispositivos de Entrada e Saída do *Data Center*	4	A ATI mantém um ambiente seguro quanto ao Bootloader no Ubuntu server, por utilizar um gerenciador seguro de maquinas virtuais. Além de ser registro o acesso de dispositivo ao data center.	2	3
	SOS 1.4 - Restauração do Sistema Operacional	4	A ATI mantém serviços de SNAPSHOTS no hypervisor. Toda a configuração foi realizada de maneira correta.	1	5
	SOS 1.5 - Segurança na Memória do Sistema Operacional	4	A ATI mantém um controle do uso da memória do servidor. Além disso, é gerenciador o desempenho da memória.	1	3
SOS 2 - Atualização de Patches do Sistema Operacional	SOS 2.1 - Execução por Profissionais Treinados	0	Inexistente	2	4
	SOS 2.2 - Teste de Atualização do Sistema Operacional	0	Inexistente	1	3
	SOS 2.3 - Atualização no Sistema Operacional	0	Inexistente	2	4
SOS 3 - Segurança do Sistema Operacional	SOS 3.1 - Remoção e Desativação de Serviços e Protocolos desnecessários	3	Foi identificado o serviço *collect_d* que não está sendo utilizado. Desta forma é possível que aumentem as chances de ataques ao serviço, além de consumir recursos do servidor de forma desnecessária.	1	5
	SOS 3.2 - Criptografia no Sistema de Arquivo	0	Inexistente	2	3
	SOS 3.3 - Envio de Chave de Decodificação	0	Inexistente	2	3
SOS 4 - Controle de Acesso	SOS 4.1 - Registro e remoção de usuários	4	Existe uma documentação, no servidor (constando o ID), como na própria ATI, que mantem uma documentação dos usuários que acessam o servidor.	2	4
	SOS 4.2 - Atribuir Credenciais do Usuário	4	Existe uma documentação, no servidor (constando o ID), como na própria ATI, que	2	4

			mantem uma documentação dos usuários que acessam o servidor.		
	SOS 4.3 - Criação de Grupos de Usuário	2	Foi identificado que existem usuários no grupo adm, porém existem 4 usuarios sem grupo específico.	2	3
	SOS 4.4 - Renomear as contas de administrador	4	Existe uma documentação, no servidor (constando o ID), como na própria ATI, que mantem uma documentação dos usuários que acessam o servidor. As contas do administrador do sistema são alteradas.	2	5
	SOS 4.5 - Limitação de Acesso nas Estações de Trabalho	4	O acesso do servidor só realizado após acesso a VPN da ATI e utilização via SSH (Secure Shell).	2	5
	SOS 4.6 - Remoção de Contas Padrão do Sistema	4	Existe uma documentação, no servidor (constanto o ID), como na própria ATI, que mantem uma documentação dos usuários que acessam o servidor. As contas padrão do sistema foram removidas.	2	4
SOS 5 - Autenticação do Usuiário do Sistema Operacional	SOS 5.1 - Senhas Sólidas	2	As senhas são alteradas, porém passaram 90 dias e não houve alteração.	2	4
	SOS 5.2 - Usuários e Senhas Exclusivas	3	Todas as senhas de usuários são exclusivas. Porém os usuários encontrados em /etc/passwd que não são usados, não se tem informações precisas.	2	4
	SOS 5.3 - Criação de Senha de Dois Fatores	4	O acesso ao servidor só é possível através de uma VPN, acesso SSH e Login do Sistema Operacional.	2	5
	SOS 5.4 - Bloqueio de Tela por Inatividade	0	O keepAlive do serviço SSH está como ***YES***, portanto não existe a implementação deste conjtrole.	2	4
SOS 6 - Segurança de Redes no Sistema Operacional	SOS 6.1 - Responsabilidades Operacionais	0	Inexistente	2	5
	SOS 6.2 - Gerenciamento dos Serviços de Rede	4	A ATI conta com gerenciador dos serviços de rede e gerenciador das maquinas virtuais.	2	5

	SOS 6.3 - Conexão sobre Sistemas à Rede	4	A ATI conta com gerenciador dos serviços de rede e gerenciador das maquinas virtuais.	2	5
	SOS 6.4 - Registro de Atividades da Rede	4	A ATI conta com gerenciador dos serviços de rede e gerenciador das maquinas virtuais.	2	5
	SOS 6.6 - Remoção de Conteúdo	0	Inexistente	2	5
	SOS 6.7 - Segurança de Serviço de Redes	0	Inexistente	2	5
	SOS 6.8 - Transferência das Informações	4	Foi identificado o uso de criptografias adequadas no serviço de rede. VPN, SSH.	2	5
	SOS 6.9 - Segurança na Resolução de Nomes (Autoritativo)	0	Inexistente	1	5
	SOS 6.10 - Segurança na Resolução de Nomes (Recursivo)	0	Inexistente	1	5

Fonte: Elaborado pelo autor.

Quadro 21: Pontuações Obtidas no Estudo de Caso 2 - Dimensão Server Application Security

Família	Controles	EV	Evidencia	CW	OW
SAS 1 - Instalação Segura dos Softwares	SAS 1.1 - Política e Procedimento para Aquisição de Software ou Serviço	0	Não existente	2	5
	SAS 1.2 - Desinstalação de Softwares Desnecessários	1	Alguns softwares foram desinstalados, porém há indicios de alguns softwares que não são utilizados.	1	4
	SAS 1.3 - Atualização dos Softwares e Aplicativos	0	Não existente	2	4
	SAS 1.4 - Limite de Privilégio na Operacionalização dos Softwares	1	O Usuário Deploy tem acesso semelhante ao Root. Nenhum usuário pode ter acesso total igual ao usuário root.	2	5
	SAS 1.5 - Configuração de Software em Ambiente de Teste	4	Toda a configuração acontece previamente numa estância denominada *stage.openredu*.	2	5

	SAS 1.6 - Execução de Códigos	4	Toda a execução e controle dos códigos ruby on rails, e scripts de deploy acontecem previamente numa estância denominada *stage.openredu*.	2	5
	SAS 1.7 - Contigência dos Softwares	4	Todas as versões antesriores dos softwares são mantidas de forma adequada em outras estâncias ou em arquivos do openredu.	2	5
	SAS 1.8 - Arquivamento dos Softwares	1	Todas as versões antesriores dos softwares são arquivadas, porém devido a um número restrito na equipe, não existem uma preocupação em se arquivar um software adequadamente.	2	2
SAS 2 - Restrições aos Recursos do Servidor	SAS 2.1 - Configuração da Partição do Sistema de Arquivos de Softwares	0	Não existente	1	4
	SAS 2.2 - Controle de Acesso Concorrente	0	Não existente	1	4
SAS 3 - Controle de Acesso do Software	SAS 3.1 - Restrições de acesso à informação	4	As informações dos softwares são restritas de maneira adequada conforme configurações no servidor.	2	5
	SAS 3.2 - Segurança no Login do Software	1	No login do openredu, um banner de serviços foi identificado, bem como informações de códigos e parametros ao digitar um path na barra de endereço.	2	5
	SAS 3.3 - Software de Gerenciamento de Senha	0	Não existente	2	3
	SAS 3.4 - Software Utilitários Privilegiados	1	Só exite controles para aplicação do openredu que utiliza o Nginx e o ruby on rail. Nos demais softwares não existem tal controle.	2	3
	SAS 3.5 - Controle ao Código Fonte dos Softwares	4	Por se tratar de comunidade de opensource todo o código desenvolvido é verificado e testado.	2	4

SAS 4 - Segurança em Softwares de Transferência de Arquivos	SAS 4.1 - Critografia na Transferência dos Dados	1	Embora exista o uso do serviço SSH, o serviço web NGINX não tem o serviço SSL implementado no servidor.	2	4
SAS 5 - Instalação e Configuração de Controles de Segurança Adicionais	SAS 5.1 - Instalação de Software Antivírus	0	Não existente	2	4
	SAS 5.2- Atualização de Software Antivírus	0	Não existente	2	3
	SAS 5.3 - Execução de Software Antivírus	0	Não existente	2	4
	SAS 5.4 - Notificação de falha da Segurança no Software	4	É usado o *MONIT*, monitorando o unicorn, nginx, mysql.	1	5
	SAS 5.5 - Verificação Automatizada da Segurança	4	É usado o MONIT, são monitorados o unicorn, nginx, mysql.	1	5
	SAS 5.6 - Relatório da Segurança	0	Não existente	1	4

Fonte: Elaborado pelo autor.

Quadro 22: Pontuações Obtidas no Estudo de Caso 2 - Dimensão Server Security Preserving

SERVER SECURITY PRESERVING					
Família	**Controles**	**EV**	**Evidencia**	**CW**	**OW**
SSP 1 - Gestão de Incidente de Segurança do *Data Center*	SSP 1.1 - Responsabilidades e Procedimentos no *Data Center*	0	Inexistente	2	4
	SSP 1.2 - Notificação de fragilidade do Sistema do *Data Center*	4	Foram realizadas atividades com as ferramentas de notificação de fragilidade, como por exemplo: Sqlmap, Owasp Zap, Unicast.	2	5
	SSP 1.3 - Avaliação e Decisão dos Eventos	0	Inexistente.	2	4

	de segurança do *Data Center*				
	SSP 1.4 - Resposta aos incidentes de segurança do *Data Center*	1	Existe uma parte externa que é reportada e um contato definido para serem reportados. Porém o tempo de resposta é lento.	2	5
SSP 2 - Registro e Monitoramento	SSP 2.1 - Sistemas de Relatórios e Registros em Tempo Real	2	Existe registro dos logs, porém não é utilizada uma ferramenta centralizada.	2	5
	SSP 2.2 - Proteção da Informação Auditada	0	Inexistente	2	5
	SSP 2.3 - Registro dos Administradores e Operadores do *Data Center*.	4	Os logs são verificados a intervalos regulares no arquivo /var/log/auth	2	5
	SSP 2.4 - Retenção de Registros	1	Os logs da aplicação Openredu são retidos, porém não há um controle para a retenção dos registros do servidor.	2	5
	SSP 2.5 - Sincronização do Relógio	4	Neste servidor está instalado o servidor NTP de forma adequada.	2	5
SSP 3- Auditoria	SSP 3.1 - Capacidade de Auditoria	0	Inexistente	1	4
	SSP 3.2 - Auditoria e Geração de Relatórios Otimizados	0	Inexistente	1	4
	SSP 3.3 - Auditoria Alternativa	0	Inexistente	1	4
SSP 4 - Backup	SSP 4.1 - Cópias de Segurança - Completude e Exatidão das Cópias	2	São realizados backups apenas do banco MYSQL.	2	5
	SSP 4.2 - Cópias de Segurança - Abrangência e Frequência	1	É realizada de maneira aleatória.	2	5
	SSP 4.3 - Cópias de Segurança - Armazenamento Remoto	2	São realizados backups apenas do banco MYSQL.	2	5
	SSP 4.4 - Cópias de Segurança - Criptografia	0	Inexistente	2	3
SSP 5 - Redundância	SSP 5.1 - Disponibilidade dos Recursos de Configuração do *Data Center*	0	Inexistente	2	5

SSP 6 - Teste de Segurança do *Data Center*	SSP - 6.1 - Autorização para Ambiente de Teste	0	Inexistente	1	4
	SSP - 6.2- Exclusão dos Dados no Ambiente de Teste	0	Inexistente	1	4
	SSP - 6.3 - Registro do Uso dos Dados no Ambiente de Teste	0	Inexistente	1	3
	SSP 6.4 - Scanning de Vulnerabilidades	0	Inexistente	1	4
	SSP 6.5 - Teste de Penetração	4	Testes de penetração estão sendo realizados de forma periódica no servidor.	1	5

Fonte: Elaborado pelo autor.

APÊNDICE C. RESULTADO DO PROGRAMA DE MELHORIAS

Neste apêndice estão relacionados todas as recomendações dos fatos críticos ou pontos relevantes que precisam ser implementados nas duas organizações avaliadas. Cada proposta de melhoria é classificada por um número identificador (Id). Este apêndice está separado entre os estudos de casos 1 e 2 respectivamente.

Apêndice C.1. Programa de Melhoria do Estudo de Caso 1

Quadro 23: Programa de Melhoria - Estudo de Caso 1

Id 1	Convém que a organização tenha a documentação conforme o controle SSP 1.1.
Id 2	Convém que os funcionários e partes externas que usam os sistemas e serviços do *data center* na organização, precisam ser instruídos a registrar e notificar quaisquer fragilidades de segurança da informação suspeita ou observada, nos sistemas ou serviços, conforme SSP 1.2.
Id 3	Convém que a gestão de segurança avalie cada evento de segurança da informação usando uma escala de classificação de incidentes e eventos de segurança da informação no *data center*, conforme SSP 1.3.
Id 4	Convém que os incidentes de segurança da informação no data center sejam reportados para um ponto de contato definido e outras pessoas relevantes da organização, ou ainda, partes externas (detentora da franquia ou fornecedores), conforme SSP 1.4.
Id 5	Sugere-se a utilização precisa e detalhada da ferramenta da *Microsoft Event Viewer*, OSSEC e similares.
Id 6	Convém a criação de GPO's para definir o tamanho dos logs e a utilização de usuários legítimos. Sugere-se a leitura do documento *Microsoft Knowledge Base* para mais esclarecimentos.
Id 7	Convém procurar orientação de um consultor jurídico para determinar os requisitos regulamentares para a retenção de registros.
Id 8	Convém procurar orientação de um consultor jurídico para determinar os requisitos regulamentares para a retenção de registros.
Id 9	Convém usar auditoria, por exemplo, nas alterações de senha, não-*logons*, ou não acesso relacionada aos sistemas de informação, de uso administrativo privilegiado, de uso de credenciais, ou uso de credenciais de terceiros.

Id 10	Convém que o *data center* gere informações de auditoria recolhidas e organizadas em um formato resumido que é mais significativo para os analistas. Recomenda-se utilizar as ferramentas de auditoria da Central de Registros.
Id 11	Convém que seja implementado uma capacidade de auditoria alternativa de curto prazo, até que a falha no recurso de auditoria principal seja corrigida, conforme SSP 3.3.
Id 12	Convém que seja revisto o contrato com o fornecedor de serviço de TI referente aos serviços de backup do servidor que são realizados em nuvem. Nesta documentação é importante identificar onde é gerado o backup e qual criptografia utilizada.
Id 13	Convém que seja revisto o contrato com o fornecedor de serviço de TI referente aos serviços de backup do servidor que são realizados em nuvem. Nesta documentação é importante identificar onde é gerado o backup e qual criptografia utilizada.
Id 14	Convém que seja implantada uma redundância de toda a infraestrutura ou de no mínimo dos componentes essenciais para manter a disponibilidade dos sistemas.
Id 15	Convém a autorização para cópia do ambiente como teste, tomando os devidos cuidados com as informações ali contidas.
Id 16	Convém colocar em contrato que toda e qualquer informação contida no ambiente de teste seja apagada ao fim de sua utilização.
Id 17	Convém que seja documentado e salvo todos os registros realizados nos testes, além do efeito causado durante o mesmo, para que posteriormente possa ser analisado.
Id 18	Convém a utilização da ferramenta Nessus ou similar, para varredura e vulnerabilidades, gerando informações detalhadas dos possíveis pontos fracos do *data center*.
Id 19	Convém utilizar técnicas para verificar o estado das informações, simulando um ataque real ao *data center* utilizando as técnicas: 1 - Coletar Informações, 2 - Mapeamento de Rede, 3 - Enumeração de Serviços, 4 - Busca de Vulnerabilidade, 5 - Exploração das Vulnerabilidades, 6 - Implantação de *Backdoors* e *Rootkits*, 7 - Eliminação de Vestígios.
Id 20	Convém realizar uma análise individual, verificando os requisitos de cada franqueado. Dando a possibilidade de escolher qual o software se adapta a sua realidade.
Id 21	Convém à implementação de um sistema de *helpdesk* (GLPI, OTRS, OSTICKET) onde possam ser centralizadas todas as requisições de atualização de software.
Id 22	Convém que seja instalado o *Active Directory* no servidor e que sejam criadas GPOS para restrição de acesso aos softwares.
Id 23	Convém que seja implementado um servidor de homologação de softwares em que

	sejam realizados testes em no mínimo três dias em ambiente de não produção.
Id 24	Convém que versões de softwares anteriores sejam mantidas, como, por exemplo, em backup, caso haja alguma falha ou erro da aplicação, sendo possível realizar uma reinstalação.
Id 25	Convém que a organização tenha um armário, por exemplo, para que sejam arquivadas as mídias dos softwares utilizados no servidor e o acesso dessas mídias sejam controladas pelo responsável técnico do servidor.
Id 26	Convém criar GPO's que controlem o número máximo de acessos simultâneos.
Id 27	Convém criar GPO's para gerenciar os acessos às informações.
Id 28	Convém que o procedimento de entrada (login) revele o mínimo de informações sobre a aplicação, de forma a evitar o fornecimento de informações, desnecessárias a um usuário não autorizado, conforme SAS 3.2.
Id 29	Convém utilizar o *Active Directory* para o armazenamento centralizado das senhas e GPO's com requisitos mínimos.
Id 30	Convém implementar solução de antivírus e centralizar os incidentes gerados na organização e manter o antivírus atualizado, criando uma rotina de checagem.
Id 31	Convém implementar servidores IDS/IPS como apoio a segurança automatizando as checagens e gerando relatórios automáticos, como por exemplo as ferramentas Snort, OSSEC, Nessus).
Id 32	Convém realizar periodicamente relatórios de segurança do *data center*, podendo ser realizado através da contratação de especialistas para realizar periodicamente relatórios de segurança do *data center*.
Id 33	Convém que seja investigada a documentação do *Windows Server* 2012 quanto o *bootloader* NTLDR e suas configurações de segurança. Ver http://support.microsoft.com.
Id 34	Convém restringir a instalação e/ou utilização de gravadores de mídia e outros dispositivos com capacidade de saída para sistemas específicos de I/O usados para a saída de conteúdo para mídias físicas. Podem ser utilizadas GPO's para realizar esta tarefa.
Id 35	Convém que sejam realizadas criações de restaurações do sistema periodicamente utilizando ferramentas do próprio Windows Server 2012. Ver http://support.microsoft.com.
Id 36	Convém a utilização do *Control Flow Guard*. ver: http://support.microsoft.com, conforme SOS 1.5.

Id 37	Convém a utilização do *Active Directory* e GPO's para controlar a criação e remoção de usuários, para atribuir credenciais e limitar acesso desses usuários e renomear contas do administrador.
Id 38	Convém implementar uma política de segurança para remoção de contas padrão do sistema e que sejam alteradas por exemplo, usuário administrador. Implementar senha e troca de senha por período.
Id 39	Convém a utilização do *Active Directory* e GPO's para o gerenciamento de nível de complexidade de senha.
Id 40	Convém que sejam criadas políticas de responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede.
Id 41	Convém que seja implementado um servidor *Proxy*, por exemplo: *squid*, onde as conexões seriam concentradas e logadas a fim de auditoria, além de softwares como o *zabbix* para monitoramento do tráfego de rede, possibilitando a detecção de anomalias.
Id 42	Convém implementar um processo de remoção de conteúdo dos dispositivos de transferência quando aplicável, remover o acesso de clientes às ferramentas de transferência imediatamente após a conclusão do projeto, confirmar que a conexão está encerrada após o término da sessão.
Id 43	Convém que os serviços de rede sejam implementados com segurança, por exemplo: FTPS, HTTPS, IPSEC, DNSSEC entre outras. Além disso, a implementação de *firewall* para controle de acesso aos serviços.
Id 44	Convém a criação de uma política de criptografia de dados onde qualquer dado confidencial trocado com clientes e fornecedores, sejam criptografados para garantir a confidencialidade e integridade dessas informações.
Id 45	Convém inplementar servidor confiável de resolução de nomes e atribuir protocolos de seguranças adicionais DNS e DNSSEC.
Id 46	Convém configurar o DNS reverso a fim de garantir a identidade do domínio, permitindo a verificação do mesmo.
Id 47	Convém que este documento seja definido e aprovado pela direção, sendo publicado e comunicado para os gestores de segurança e partes externas relevantes (como por exemplo, provedores de serviço. É importante que o alto nível da organização tenha conhecimento da definição da política de configuração de segurança do *data center*, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança do *data center*.
Id 48	Convém que a política de segurança do *data center* tenha um gestor de segurança que

	tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação das políticas de segurança do *data center*. Convém que a análise crítica inclua a avaliação de oportunidades para melhoria da política de segurança do *data center* tendo como objetivo responder às mudanças ao ambiente organizacional, às circunstâncias do negócio, às condições legais, ou ao ambiente de tecnologia.
Id 49	Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes para uso do servidor, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização. Caso a organização tenha implantado servidor(es) em outro(s) país(es) convém que os gestores considerem a conformidade em todo (s) esse(s) país(es).
Id 50	Convém aplicar controles de privacidade consistentes com quaisquer exceções e isenções específicas, incluídas na legislação, ordens executivas, diretrizes, políticas e regulamentos (por exemplo, a aplicação da lei ou considerações de segurança nacional). Uma política de dados da organização para proteção e privacidade da informação de identificação pessoal, seja desenvolvida e implementada que constarão nos registros do servidor. Esta política deve ser comunicada a todas as pessoas envolvidas no processamento de informação de identificação pessoal, ou até na contratação de funcionário.
Id 51	Convém que os controles de criptografia deverão ser usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes. Este deve estar em conformidade com leis e legislações para: • Restrições à importação e/ou exportação de hardware e software do servidor para execução de funções criptográficas; • Restrições à importação e/ou exportação de hardware e software de computador que foi projetado para ter funções criptográficas embutidas; • Restrições no uso de criptografia; • Métodos mandatórios ou discricionários de acesso pelas autoridades dos países à informação cifrada por hardware ou software para fornecer confidencialidade ao conteúdo.
Id 52	Criptografia pode ser utilizada para suportar uma variedade de soluções de segurança incluindo, por exemplo, a proteção das informações, assinaturas digitais, geração de números aleatórios e de *hash*.
Id 53	Convém que verificações do histórico sejam realizadas para todos os candidatos a emprego ou convocação, de acordo com a ética, regulamentações e leis relevantes, seja

	proporcional aos requisitos do negócio, e atenda a demanda e complexidade das atividades nas configurações de segurança do *data center*, incluam os seguintes itens: • Disponibilidade de referências de caráter satisfatórias, por exemplo, uma profissional e uma pessoal; • Uma verificação (da exatidão e completude) das informações do curriculum vitae do candidato; • Confirmação das qualificações acadêmicas e profissionais; • Verificação independente da identidade (passaporte ou documento similar); • Verificações mais detalhadas, tais como verificações financeiras (de crédito) ou verificações de registros criminais; • O profissional deve possuir certificação equivalente com as atividades.
Id 54	Convém que as obrigações contratuais para funcionários e partes externas, reflitam as políticas para segurança da informação do *data center*, esclarecendo e declarando: • Que todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis do *data center* assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento do *data center*; • As responsabilidades legais e direitos dos funcionários e partes externas, e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais e legislação de proteção de dados; • As responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização, associados com a informação, com os recursos de processamento da informação e com os serviços de informação conduzidos pelos funcionários, fornecedores ou partes externas; • As responsabilidades dos funcionários ou partes externas, pelo tratamento da informação recebida de outras companhias ou partes interessadas; • Ações a serem tomadas no caso de o funcionário ou partes externas, desrespeitar os requisitos de segurança da informação da organização.
Id 55	Convém que na organização deva existir um processo formal bem definido para adotar ações contra funcionários que tenham cometido violações contra o *data center*. Importante que o processo disciplinar formal apresente uma resposta de forma gradual, que leve em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio, se este é ou não o primeiro delito, se o infrator foi ou não

	adequadamente treinado às legislações relevantes, aos contratos do negócio e outros fatores conforme requerido. Sanções da organização refletem as leis federais, ordens executivas, diretrizes, regulamentos, políticas, normas e orientações. Processos e sanções são descritos em acordos de acesso e pode ser incluído como parte de políticas e procedimentos gerais de pessoal para as organizações.
Id 56	Convém que um programa de treinamento em configuração da segurança do *data center* seja estabelecido alinhado com as políticas e procedimentos relevantes de segurança do *data center*, levando em consideração as informações da organização a serem protegidas e os controles a serem implementados para proteger a informação. • Declaração do comprometimento do profissional com a segurança da informação no *data center*; • A necessidade de tornar conhecido e estar em conformidade com as obrigações e regras para a segurança do *data center*, conforme definido nas políticas, normas, leis, regulamentações, contratos e acordos; • Responsabilidade pessoal por seus próprios atos e omissões, e compromissos gerais para manter seguro ou para proteger a informação que pertença à organização e partes externas. • Procedimentos de segurança da informação básicos (tais como, notificação de incidente no *data center*) e controles básicos (tais como, segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa). • Pontos de contato e recursos para informações adicionais e orientações sobre questões de segurança do *data center*, incluindo materiais de treinamento. • Exercícios práticos: podem incluir, por exemplo, engenharia social para coletar as informações, obtenção de acesso não autorizado, ou simular o impacto adverso da abertura de anexos de e-mail maliciosos ou através de ataques de *spear phishing*, links maliciosos.
Id 57	Convém que uma declaração nítida dos requisitos do negócio a serem atendidos pelo controle de acesso, seja fornecida aos usuários e provedores de serviços. Este controle aborda o estabelecimento de políticas e procedimentos para o implementação efetiva dos controles de segurança selecionados e melhorias de controle de acesso às informações do *data center*. Este documento inclui: • Requisitos de segurança de aplicações de negócios individuais; • Política para disseminação e autorização da informação, por exemplo, o princípio "necessidade de conhecer" e níveis de segurança e a classificação das

	informações; • Consistência entre os direitos de acesso e as políticas de classificação da informação em diferentes sistemas e redes; • Legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços; • Gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis; • Segregação de funções de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso; • Requisitos para autorização formal de pedidos de acesso. • Requisitos para análise crítica periódica de direitos de acesso. • Remoção de direitos de acesso. • Arquivo dos registros de todos os eventos significantes, relativos ao uso e gerenciamento das identidades do usuário e da informação de autenticação secreta; • Regras para o acesso privilegiado.
Id 58	Convém que as informações do *data center* sejam classificadas em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. Convém que as classificações levem em conta a conformidade com o negócio para compartilhar ou restringir acesso. Importante estabelecer critérios para análise crítica da classificação, e serem avaliados por meio da confidencialidade, integridade e disponibilidade: • Categoriza informações do *data center* de acordo com a legislação federal e leis aplicáveis, ordens executivas, diretrizes, políticas, regulamentos, normas e orientação; • Documenta os resultados de categorização de segurança do *data center* (incluindo a justificação de apoio); • Garante que o agente responsável pela autorização aprove a decisão de categorização de segurança.
Id 59	Convém que as informações sejam marcadas para definir as limitações da informação. Esta marcação pode não ser necessária em casos em que o *data center* mantenha informações de domínio público. Entretanto, pode-se utilizar para realizar marcações para informações públicas, indicando que a informação é de domínio público.

Id 60	Convém que todo o procedimento de configuração do *data center* seja documentado e disponibilizado aos profissionais/usuários do *data center*. Os procedimentos de configuração incluem: • A instalação e configuração de sistemas; • Processamento e tratamento da informação, tanto automática como manual; • Cópias de segurança (backup); • Requisitos de agendamento, incluindo interdependências com outros sistemas, a primeira hora para início da tarefa e a última hora para o término da tarefa; • Instruções para tratamento de erros ou outras condições excepcionais, que possam ocorrer durante a execução de uma tarefa, incluindo restrições de uso dos utilitários do sistema; • Procedimento para o reinício e recuperação em caso de falha do sistema; • Gerenciamento de trilhas de auditoria e informações de registros (logs) de sistemas e procedimentos de monitoramento.
Id 61	Convém que sejam criadas políticas e procedimentos que reflitam as leis federais, ordens executivas, diretrizes, regulamentos, políticas, normas e orientações. A política do *data center* pode ser incluída como parte da política geral de segurança da informação nas organizações ou, inversamente, pode ser representado por várias políticas que reflitam a natureza complexa de certas organizações.
Id 62	Convém que sejam criadas políticas de avaliação de risco que abordam finalidade, o escopo, papéis, responsabilidades, compromisso de gestão, a coordenação entre as entidades organizacionais e de conformidade para apoiar as configurações do *data center*.
Id 63	Convém que a arquitetura descreva a filosofia geral, os requisitos e abordagem em relação à proteção da confidencialidade, integridade e disponibilidade da informação do *data center*: • Descreve como a arquitetura de segurança do *data center* é integrado e suporta a arquitetura empresarial; • Descreve quaisquer suposições de segurança da *data center* sobre, e dependências em diante, serviços externos; • Revisões e atualizações da arquitetura de segurança do *data center* para refletir alterações na arquitetura da empresa.

Fonte: Elaborado pelo autor.

Apêndice C.2. Programa de Melhoria do Estudo de Caso 2

Quadro 24: Programa de Melhoria - Estudo de Caso 2

Id 1	Convém que as organizações desenvolvam e implementem uma abordagem de resposta a incidentes, missões organizacionais, funções de negócio, estratégias, metas e objetivos para resposta a incidentes que ajudam a determinar a estrutura das capacidades de resposta a incidentes. As responsabilidades pelo gerenciamento serão estabelecidas para assegurar que os seguintes procedimentos de segurança sejam desenvolvidos e comunicados, de forma adequada conforme controle SSP 1.1.
Id 2	Convém a gestão de segurança avaliar cada evento de segurança da informação usando uma escala de classificação de incidentes e eventos de segurança da informação no *data center*, para decidir se é recomendado que o evento seja classificado como um incidente de segurança da informação. • A priorização e a classificação de incidentes podem ajudar a identificar o impacto e a abrangência de um incidente. É necessário que os resultados na analise sejam registradas, a fim de obter uma melhor verificação e referência futura. • Como resultados podem ser comunicados às entidades organizacionais que incluem, por exemplo, a equipe de resposta a incidentes, *helpdesk*, grupo de segurança da informação / departamento. Se a organização está proibida de revisar e analisar as informações, auditar ou é incapaz de realizar tais atividades, a revisão / análise pode ser realizada por outras organizações que tenham capacidade e competência, conforme controle SSP 1.3.
Id 3	Convém que os incidentes de segurança da informação no *data center* sejam reportados para um ponto de contato definido e outras pessoas relevantes da organização, ou ainda, partes externas, conforme controle SSP 1.4.
Id 4	Convém a utilização de aplicativos que utilizem protocolos SNMP. Sugere-se, por exemplo, o Zabbix e o Nagios para monitoramento do servidor e geração de relatórios em tempo real.
Id 5	Convém que as organizações identifiquem eventos de auditoria como aqueles que são significativos e relevantes para a segurança do sistema do *data center*, suas configurações e os ambientes em que esses sistemas operam de forma a atender às necessidades específicas de auditoria em curso. Eventos de auditoria podem incluir, por exemplo, alterações de senha, não *logins*, ou não acesso relacionada aos sistemas de informação, de uso administrativo, de uso de

	credenciais, ou uso de credenciais de terceiros. Ao determinar o conjunto de eventos auditáveis, as organizações consideram a adequada auditoria para cada um dos controles de segurança a serem implementadas. Para equilibrar requisitos de auditoria com outras necessidades de sistemas de informação, este controle também requer a identificação de que subconjunto de eventos que são auditados em um determinado ponto no tempo. Conforme o controle SSP 3.1, sugere-se o uso do Nessus ou similares.
Id 6	Convém que seja implementado uma capacidade de auditoria alternativa de curto prazo, até que a falha no recurso de auditoria principal seja corrigida. As organizações podem determinar que a capacidade de auditoria alternativa precise apenas fornecer um subconjunto da funcionalidade de auditoria primário que é impactado pela falha. Sugere-se o uso do Nessus ou similares.
Id 7	Convém que os registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação, os quais convêm que sejam produzidos, conforme controle SSP 4.1. Sugere-se o uso do software Bacula ou similares como servidor de backup.
Id 8	Convém que em situações onde a confidencialidade seja importante, cópias de segurança sejam protegidas através de encriptação. Sugere-se a criptografia de todos os dados trafegados entre o servidor e os clientes com ferramentas como: *GPG, OpenSSH, OpenSSL* ou similares.
Id 9	Convém que sejam aplicadas redundâncias de todas as camadas do sistema e serviços, a fim de assegurar a disponibilidade dos serviços.
Id 10	Convém que seja criado um protocolo de autorização para que testes sejam realizados no sistema, a fim de controlar quais informações estarão disponíveis para a auditoria.
Id 11	Convém que a cópia e o uso de informação operacional sejam registrados de forma a prover uma trilha para auditoria.
Id 12	Convém que sejam analisados todos os pontos fracos do sistema, utilizando ferramentas como *Nmap, Nessus, Uniscan* ou similares, para analise e mapeamento das vulnerabilidades.
Id 13	Convém que uma política ou procedimento seja implementado para a aquisição do software utilizado no *data center*.
Id 14	Convém revisar a lista de serviços instalados em todos os servidores de transferência de conteúdo e desinstalar ou desativar qualquer um que não seja necessário.

Id 15	Convém à utilização de pacotes atualizados do próprio repositório do Ubuntu 14.04, alinhando a verificações automáticas em intervalos regulares, e o uso de comandos e criação de scripts com o *CRON*.
Id 16	Convém implementar privilégios de acesso para operacionalização dos softwares em uso no *data center*. Sugere-se o uso do *AppArmor* (por ser nativo em distribuições derivadas do Debian) ou similares.
Id 17	Convém que versões antigas de software sejam arquivadas, junto com todas as informações e parâmetros requeridos, procedimentos, detalhes de configurações, e software de suporte durante um prazo igual ao prazo de retenção dos dados.
Id 18	Convém que um sistema de controle de configuração seja utilizado para manter controle de tamanho apropriado para utilização de arquivos dos softwares. Sugere-se o uso do *Gparted* e *Fdisk* (nativos) ou similares.
Id 19	Convém que as organizações limitem o número de sessões simultâneas para administradores de sistema ou indivíduos que trabalham no servidor ou aplicações de missão crítica. Este controle aborda sessões simultâneas para contas do sistema de informação. Sugere-se configurar o sistema Ubuntu por parte dos serviços podendo ser realizado nos arquivos de configuração. Por exemplo, *nginx, ssh, apache* entre outros.
Id 20	Convém que o procedimento de entrada (login) revele o mínimo de informações sobre a aplicação, de forma a evitar o fornecimento de informações, desnecessárias a um usuário não autorizado. Convém que uma técnica de autenticação adequada seja escolhida para validar a identificação alegada de um usuário. Convém que seja implementado um bom procedimento de entrada no software.
Id 21	Convém que as seguintes diretrizes para o uso de utilitários de programa possam ser capazes de sobrepor os controles dos sistemas e as aplicações. Sugere-se o uso de *SELinux* para atender o controle SAS 3.4.
Id 22	Convém a utilização se ferramentas como *OpenSSL, OpenSSH, GPG, TrueCrypty, SFTP* ou similares para a criptografia dos dados transferidos.
Id 23	Convém a instalação do antivírus *Clamav* ou similar para auxiliar na proteção do sistema operacional. Sugere-se a atualização periódica do software antivírus.
Id 24	Convém configurar o software antivírus para realizar uma verificação completa do sistema com base na estratégia de antivírus e configurar o software antivírus para executar durante os períodos ociosos.
Id 25	Convém gerar relatório por meio de ferramentas de *helpdesk* com os índices de incidentes de segurança da informação a fim de tomar as medidas cabíveis para a

	mitigação dos incidentes.
Id 26	Convém que as atualizações do sistema operacional, aplicativos e bibliotecas de programas sejam executadas por administradores treinados e com autorização gerencial apropriada. Sugere-se que a comunidade atente a profissionais com certificação *LPI 1* no mínimo para *deploy* e configurações de servidores Ubuntu com a aplicação *Openredu*.
Id 27	Convém testar os *patches* em ambiente separado antes da implantação no servidor. Convém verificar se as atualizações estão em suas versões estáveis. Sugere-se o uso de outras estâncias.
Id 28	Convém que sempre que possível, seja implementado uma ferramenta de gestão de *patch* centralizada para implantar automaticamente para todos os sistemas. Procurar *patchs* de fornecedores e outros terceiros, testá-los antes da implantação, implementar um processo de exceção e controles de compensação para casos em que haja um caso legítimo de negócios para sistemas sem patch. Sugere-se um processo que defina os critérios e frequência das atualizações no script de deploy. O comando CRON pode ser utilizado neste script.
Id 29	Convém retirar o serviço *collectd* que não está sendo utilizado.
Id 30	Convém usar criptografia baseada em um mínimo AES de 128 bits por meio de criptografia baseada em sistema de arquivo. Sugere-se o uso do *AppArmor* ou similares como o *SELinux*.
Id 31	Convém enviar chaves ou senhas de decodificação utilizando um método diferente do que aquele que foi utilizado para a transferência do conteúdo. Verificar para garantir que os principais nomes e senhas não estejam relacionados ao projeto ou conteúdo. Sugere-se o uso do *AppArmor* ou similares como o *SELinux*.
Id 32	Convém que os quatros usuários sem grupo definido que foram identificados no arquivo de configuração que está no diretório /etc/passwd, sejam analisados e se possível excluídos do servidor.
Id 33	Convém implementar controle de senha: • Extensão mínima de senha de 8 caracteres; • Mínimo de três dos seguintes parâmetros: maiúsculas, minúsculas, números e caracteres especiais; • Duração máxima da senha de 90 dias; • Duração mínima da senha de 1 dia; • Máximo de tentativas inválidas de login entre 3 e 5 tentativas;

	• Histórico de senha de dez senhas anteriores; • Sugere-se o uso do *SELinux*.
Id 34	Convém que seja implementado o uso de nomes de usuários e senhas exclusivos para todos os sistemas do *data center*. Convém configurar os sistemas de informação para exigirem autenticação, usando nomes de usuário e senhas exclusivos a um nível mínimo conforme SOS 5.1;
Id 35	Convém configurar servidores e estações de trabalho manualmente ou através de uma política para ativar um protetor de tela protegido por senha após um máximo de 5 minutos de inatividade. Sugere-se que o *KeepAlive* do serviço SSH esteja como *NO*.
Id 36	Convém que responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede sejam estabelecidos.
Id 37	Convém implementar uma politica de remoção de conteúdo após terminada as conexões;
Id 38	Convém que os serviços de rede sejam implementados com segurança. Sugere-se criptografar os dados trafegados com o servidor utilizando os protocolos, por exemplo: *ssh, sftp, openvpn, https*.
Id 39	Convém que seja implementado o serviço *DNSSEC*. Sugere-se a utilização de servidores DNS Autoritativo para controle do apontamento da tabela de DNS do seu site.
Id 40	Convém colocar os servidores DNS em computadores diferentes, com configurações e políticas de acesso diferentes; ou utilizando o conceito de *views* (visões ou vistas), por exemplo, no *BIND* 9.
Id 41	Convém que este documento seja definido e aprovado pela direção, sendo publicado e comunicado para os gestores de segurança e partes externas relevantes (como por exemplo, provedores de serviço. É importante que o alto nível da organização tenha conhecimento da definição da política de configuração de segurança do *data center*, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança do *data center*. Desta forma atendendo os seguintes requisitos: a) estratégia do negócio: o Quais as informações serão armazenadas no servidor; o Quais as categorias e informações serão processadas ou transmitidas através do

	servidor; o Qual o sistema operacional adequado para o *data center* na organização; o Quais são os requisitos de segurança para esta informação; o Quais informações serão lidas ou armazenadas em outro host; o Que outro serviço (s) será fornecido pelo servidor; o Quais são os requisitos de segurança para estes serviços adicionais; o Onde na rede o servidor será localizado; b) de regulamentações, legislação e contratos: c) atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança do *data center* para os papéis definidos.
Id 42	Convém que a política de segurança do *data center* tenha um gestor de segurança que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação das políticas de segurança do *data center*. Convém que a análise crítica inclua a avaliação de oportunidades para melhoria da política de segurança do *data center* tendo como objetivo responder às mudanças ao ambiente organizacional, às circunstâncias do negócio, às condições legais, ou ao ambiente de tecnologia.
Id 43	Convém que a documentação inclua os seguintes requisitos: • Configuração de segurança, instalação e operação do sistema, componente ou serviços; • A utilização eficaz e manutenção das funções / mecanismos de segurança; e vulnerabilidades conhecidas sobre configurações e uso de funções administrativas do sistema.
Id 44	Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes para uso do servidor, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização. Caso a organização realize ou tenha implantado servidor(es) em outros país(es) convém que os gestores considerem a conformidade em todos esses países.
Id 45	Convém aplicar controles de privacidade consistentes com quaisquer exceções e isenções específicas, incluídas na legislação, ordens executivas, diretrizes, políticas e regulamentos (por exemplo, a aplicação da lei ou considerações de segurança nacional). Política de dados da organização para proteção e privacidade da informação de identificação pessoal, seja desenvolvida e implementada que constarão nos registros do servidor. Esta política deve ser comunicada a todas as pessoas envolvidas no processamento de informação de identificação pessoal, ou até na contratação de

	funcionário.
Id 46	Convém que os controles de criptografia devam ser usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes. Este deve estar em conformidade com leis e legislações para: • Restrições à importação e/ou exportação de hardware e software do servidor para execução de funções criptográficas; • Restrições à importação e/ou exportação de hardware e software de computador que foi projetado para ter funções criptográficas embutidas; • Restrições no uso de criptografia; • Métodos mandatórios ou discricionários de acesso pelas autoridades dos países à informação cifrada por hardware ou software para fornecer confidencialidade ao conteúdo; • Criptografia pode ser utilizada para suportar uma variedade de soluções de segurança incluindo, por exemplo, a proteção das informações, assinaturas digitais, geração de números aleatórios e de hash.
Id 47	Convém que verificações do histórico sejam realizadas para todos os candidatos a emprego ou convocação, de acordo com a ética, regulamentações e leis relevantes, seja proporcional aos requisitos do negócio, e atenda a demanda e complexidade das atividades nas configurações de segurança do *data center*, e incluam os seguintes itens: • Disponibilidade de referências de caráter satisfatórias, por exemplo, uma profissional e uma pessoal; • Uma verificação (da exatidão e completeza) das informações do curriculum vitae do candidato; • Confirmação das qualificações acadêmicas e profissionais; • Verificação independente da identidade (passaporte ou documento similar); • Verificações mais detalhadas, tais como verificações financeiras (de crédito) ou verificações de registros criminais; • O profissional deve possuir certificação equivalente com as atividades.
Id 48	Convém que as obrigações contratuais para funcionários e partes externas, reflitam as políticas para segurança da informação do *data center*, esclarecendo e declarando: • Todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis do *data center* assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento

	do *data center*; • As responsabilidades legais e direitos dos funcionários e partes externas, e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais e legislação de proteção de dados; • As responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização, associados com a informação, com os recursos de processamento da informação e com os serviços de informação conduzidos pelos funcionários, fornecedores ou partes externas; • As responsabilidades dos funcionários ou partes externas, pelo tratamento da informação recebida de outras companhias ou partes interessadas; • As ações a serem tomadas no caso de o funcionário ou partes externas, desrespeitar os requisitos de segurança da informação da organização.
Id 49	Convém que na organização deva existir um processo formal bem definido para adotar ações contra funcionários que tenham cometido violações contra a segurança do *data center*. Importante que o processo disciplinar formal apresente uma resposta de forma gradual, que leve em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio, se este é ou não o primeiro delito, se o infrator foi ou não adequadamente treinado às legislações relevantes, aos contratos do negócio e outros fatores conforme requerido: • Sanções da organização refletem as leis federais, ordens executivas, diretrizes, regulamentos, políticas, normas e orientações. Processos e sanções são descritas em acordos de acesso e podem ser incluídos como parte de políticas e procedimentos gerais de pessoal para as organizações.
Id 50	Convém que um programa de treinamento em configuração da segurança do *data center* seja estabelecido alinhado com as políticas e procedimentos relevantes de segurança do data center, levando em consideração as informações da organização a serem protegidas e os controles a serem implementados para proteger a informação. O treinamento para segurança do *data center* comtemplará: • Declaração do comprometimento do profissional com a segurança da informação no *data center*; • A necessidade de tornar conhecido e estar em conformidade com as obrigações e regras para a segurança do *data center*, conforme definido nas políticas, normas, leis, regulamentações, contratos e acordos; • Responsabilidade pessoal por seus próprios atos e omissões, e compromissos

	gerais para manter seguro ou para proteger a informação que pertença a organização e partes externas; • Procedimentos de segurança da informação básicos (tais como, notificação de incidente no *data center*) e controles básicos (tais como, segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa). • Pontos de contato e recursos para informações adicionais e orientações sobre questões de segurança do *data center*, incluindo materiais de treinamento. • Exercícios práticos: o Podem incluir, por exemplo, engenharia social para coletar as informações, obtenção de acesso não autorizado, ou simular o impacto adverso da abertura de anexos de e-mail maliciosos ou através de ataques de *spear phishing*, links maliciosos.
Id 51	Convém que uma declaração nítida dos requisitos do negócio a serem atendidos pelo controle de acesso seja fornecida aos usuários e provedores de serviços. Este controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva dos controles de segurança selecionados e melhorias de controle de acesso às informações do *data center*. Este documento inclui: • Requisitos de segurança de aplicações de negócios individuais; • Política para disseminação e autorização da informação, por exemplo, o princípio "necessidade de conhecer" e níveis de segurança e a classificação das informações. • Consistência entre os direitos de acesso e as políticas de classificação da informação em diferentes sistemas e redes; • Legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços; • Gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis; • Segregação de funções de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso; • Requisitos para autorização formal de pedidos de acesso; • Requisitos para análise crítica periódica de direitos de acesso; • Remoção de direitos de acesso; • Arquivo dos registros de todos os eventos significantes, relativos ao uso e

	gerenciamento das identidades do usuário e da informação de autenticação secreta; • Regras para o acesso privilegiado.
Id 52	Convém que sejam criados políticas e procedimentos que refletem as leis federais, ordens executivas, diretrizes, regulamentos, políticas, normas e orientações. A política do *data center* pode ser incluída como parte da política geral de segurança da informação nas organizações ou, inversamente, pode ser representado por várias políticas que reflitam a natureza complexa de certas organizações.
Id 53	Convém que sejam criadas políticas de avaliação de risco que abordam o escopo, papéis, responsabilidades, compromisso de gestão, a coordenação entre as entidades organizacionais e de conformidade para apoiar as configurações do *data center*.
Id 54	Convém que a arquitetura descreva a filosofia geral, os requisitos e abordagem em relação à proteção da confidencialidade, integridade e disponibilidade da informação do *data center:* • Descrever como a arquitetura de segurança do *data center* é integrado e suporta a arquitetura empresarial; • Descrever quaisquer suposições de segurança do *data center* sobre dependências em diante e serviços externos; • Revisões e atualizações da arquitetura de segurança do *data center* para refletir alterações na arquitetura da empresa.