CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior em Tecnologia de Segurança da Informação

Márcio Corrêa Rocha

Aspectos de Segurança em Terceirizações de Serviços de Tecnologia da Informação.

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior em Tecnologia de Segurança da Informação

Márcio Corrêa Rocha

Aspectos de Segurança em Terceirizações de Serviços de Tecnologia da Informação.

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança da Informação, sob a orientação do Prof.(a) Esp. Daniele Junqueira Frosoni

Área de concentração: Segurança da Informação.

Americana, S. P.

2015

Rocha, Márcio Corrêa
R574a Aspectos de segurança em terceirizações de serviços de tecnologia da informação. / Márcio Corrêa Rocha. – Americana: 2015.
52f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Daniele Junqueira Frosoni

1. Segurança em sistemas de informação I. Frosoni, Daniele Junqueira II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Márcio Corrêa Rocha

ASPECTOS DE SEGURANÇA EM TERCEIRIZAÇÕES DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação.

Americana, 08 de dezembro de 2015.

Banca Examinadora:

Daniele Junqueira Frosoni (Presidente)
Especialista
Faculdade de Tecnologia de Americana

Rogério Nunes de Freitas (Membro)
Especialista
Faculdade de Tecnologia de Americana

Luiz Carlos Degrande Júnior (Membro)
Graduado
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a Deus pela força que me deu durante esses anos de estudo, nos quais muitas adversidades quase me tiraram a oportunidade de concluir a graduação, porém sempre me mantive firme no propósito de atingir esse objetivo.

Aos meus amigos de jornada, Rogério, Lucas, Peterson, Andressa, Mayra e Vítor, juntos passamos por muitos desafios, e a ajuda mútua contribuiu para que superássemos a maior parte deles e chegássemos o mais longe que cada um conseguiu.

A minha orientadora, a professora Daniele Frosoni pelo direcionamento e correção da monografia, que possibilitou a conclusão do curso.

A toda minha família e amigos, que apesar de todos os momentos que me tiraram de casa e não me deixavam elaborar a monografia, sempre estavam do meu lado dando apoio moral.

Em especial ao meu amigo, Jeferson Thiago de Almeida Aguiar, que me apoiou desde o início na escolha do curso, me incentivou a me manter firme a cada dificuldade.

RESUMO

A busca pela terceirização de serviços de tecnologia da informação tem sido cada vez mais frequente nas empresas, como forma de implementar as demandas de mercado e obter maior competitividade frente aos concorrentes. Através da análise de solicitações de proposta de terceirização de serviços de TI lançadas no mercado entre 2014 e 2015, este trabalho teve com o objetivo de verificar se os requisitos de segurança da informação recomendados pela Norma ABNT ISO 27.002 estão sendo contemplados nestes documentos. Os resultados mostram que somente alguns requisitos indicados pela norma foram contemplados nestas solicitações, podendo trazer riscos de segurança da informação se contratação do serviço for efetivada.

Palavras Chave: Terceirização de TI, Segurança da informação, NBR ISO/IEC 27002.

ABSTRACT

The outsourcing of information technology services has increased considerably in recent years as a way to implement the market demands and achieve greater competitiveness against competitors. Based on companies' requests for proposal (RFP) of IT outsourcing services between 2014 and 2015, this paper focused on analysis of information security requirements recommended by the ISO 27002 standard in these documents. The results showed that few information security requirements are identified, which can bring security risks to companies businesses.

.

Keywords: *IT Outsourcing, information security, NBR ISO/IEC 27002.*

SUMÁRIO

LISTA DE FIGURAS E DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas.
DVD	*Digital Versatile Disc*, ou Disco Digital Versátil, em português.
EAESP/FGV	Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas.
HD	*High Definition*, ou Alta Definição, em português.
IEC	*International Electrotechnical Commission*, ou Comissão Eletrotécnica Internacional, em português.
ISO	*International Organization for Standardization*, ou Organização Internacional para Padronização, em português.
NBR	Norma Brasileira
RFP	*Request for Proposal*, ou Pedido de Proposta, , em português.
TI	Tecnologia da Informação
USB	*Universal Serial Bus*, ou Barramento Série Universal, em português.
VPN	*Virtual Private Network*, ou Rede Virtual Privada, em português.
VLAN	*Virtual Local Area Network*, ou Área de Rede Local Virtual, em português.

1 INTRODUÇÃO

A constante evolução da tecnologia traz cada vez mais novidades para o mercado mundial, como o armazenamento em nuvem, análise de dados desestruturados, computação cognitiva[1], internet das coisas[2], comércio eletrônico, todas elas estão apoiadas na expansão da conectividade, trazendo para as empresas, dos mais diversos segmentos de atuação, a possibilidade de agregar valor aos produtos e serviços prestados a seus clientes, transformar a cadeia de suprimentos, substituir atividades manuais por processos integrados e eletrônicos, além do levantamento e análise de dados proporcionar maior agilidade na tomada de decisões das operações internas e externas.

Contudo as organizações que possuem atuação em ramos diferentes de TI, e não querem usar recursos próprios para tal atividade optam por contratar uma empresa especializada em prover esses serviços para realizar o trabalho, através do processo denominado terceirização. (LAUDON; LAUDON, 2006).

Como a terceirização é a porta de entrada de recursos externos que irão prestar os serviços para a empresa contratante, tendo acesso a informações e aos ativos da mesma, observa-se a possibilidade de riscos associados a segurança da informação. Com o intuito de esclarecer se as organizações que aderem a esse tipo de serviço observam os parâmetros de segurança da informação, esse estudo propõe analisar se as solicitações de propostas, ou RFPs (*Request for Proposal*), de empresas de ramos distintos observam os aspectos recomendados pela norma da NBR ISO/IEC 27002.

O **objetivo geral** deste trabalho é identificar se os aspectos de segurança da informação recomendados pela norma NBR ISO/IEC 27002 são observados no processo de terceirização de serviços de TI.

---

[1] **Computação Cognitiva** - Termo definido como a transferência para os sistemas computacionais de características humanas para que assim ele possa operar de forma inteligente, tentando imitar as ações registradas. (MITCHELL, 2008)

[2] **Internet das Coisas** – Termo utilizado para definir os dispositivos inteligentes que utilizam a internet de forma autônoma, sem a necessidade de ações humanas para sua execução. (COMER, 2015)

Para isso foram estabelecidos os seguintes os **objetivos específicos**: a) Fazer o levantamento bibliográfico sobre terceirização de TI, conhecendo mais sobre essa prática e como ela se relaciona com a segurança da informação b) Estudar as recomendações de segurança da norma ISO 27.002:2013 c) Realizar um estudo de caso através de solicitações de propostas de terceirização de serviços de TI para identificar quais aspectos de segurança foram observados, tendo como base a norma ABNT NBR ISO/IEC 27002 (2013) d) Discutir formas de introduzir os aspectos de segurança da informação nas solicitações de propostas de serviços de TI.

Como metodologia para o desenvolvimento deste trabalho, foi utilizada uma abordagem qualitativa através do levantamento bibliográfico em monografias, livros e artigos publicados na Internet e em biblioteca, e também, o estudo de caso através da análise de solicitações de propostas, ou RFPs (*Request for Proposal*) de empresas que buscaram terceirização de tecnologia da informação, fazendo uma comparação aos requisitos de segurança recomendados pela ISO 27.002 (2013), para assim diagnosticar se os mesmos foram observados.

O trabalho foi estruturado em seis capítulos, sendo que o primeiro traz a introdução ao tema de estudo proposto, o segundo conceitua o processo de terceirização, o terceiro abrange a segurança da informação, o quarto é sobre a análise crítica dos aspectos apontados na Norma ABNT NBR ISO/IEC 27002 (2013), o quinto é o estudo de caso sobre as RFPs lançadas por empresas que buscavam parceiros prestadores de serviços de TI, e por fim, o sexto e último capítulo traz às considerações finais.

2 TERCEIRIZAÇÃO DE TECNOLOGIA DA INFORMAÇÃO

A terceirização de serviços de tecnologia da informação surgiu como forma das empresas focarem seus esforços em seu ramo principal de negócios, contratando outra empresa com conhecimento técnico, profissionais capacitados e os equipamentos necessários para fazer com que a organização consiga atingir seus objetivos estratégicos, melhorando o valor do produto ou serviço prestado ao seu cliente final. (ABERTIN; SANCHEZ, 2008).

Contudo apesar da idéia de que o serviços serão transferidos para outra empresa, é necessário entender que a responsabilidade pelas ações tomadas durante a execução dos mesmos continuam sendo da empresa contratante, o que se transfere é a mão-de-obra, os recursos, equipamentos, mas não a responsabilidade pelo produto final resultado através da solução (VIDAL, 1993).

2.1 HISTÓRIA TERCEIRIZAÇÃO DE TECNOLOGIA DA INFORMAÇÃO (TI)

A história da terceirização remete a evolução da industrialização, pois apesar de se ter como base de popularização as duas últimas décadas, o surgimento da idéia pode ser considerado, ainda na Segunda Guerra Mundial para a contratação de parceiros que produzissem armamento bélico, ou durante a revolução industrial, onde determinadas atividades já eram transferidas para outros prestadores de serviços, assim ambas seguem o mesmo conceito, por isso pode-se considerar a terceirização como um procedimento reciclado de outros momentos históricos. (GRIFFITHS; REMENYI, p. 61).

A relação do termo terceirização e tecnologia data dos anos 60, onde iniciou-se a utilização dos computadores para fins comerciais, passando para os anos 70 com a escassez de programadores no mercado, o que não supria a necessidade de se desenvolver sistemas operacionais que atendessem as necessidades dos negócios, já nos anos 80 houve a explosão da produção em massa, o que trouxe o aumento de competitividade e a redução dos custos de produção, isso exigiu que a forma de se pensar em gestão de TI começasse a mudar para atender essa nova

demanda. Tal fenômeno foi chamado por Saad (2006, p. 7), como sendo a “Terceirização Operacional”, onde as empresas com dificuldades financeiras para investir em melhorias no seu ambiente tecnológico, contratavam parceiros para desempenhar atividades não estratégicas.

Contudo a grande ascensão desse meio de prestação de serviços, trazida pela globalização causada pela evolução da internet, ocorreu em 1990, onde as empresas realmente deixaram de se preocupar com a autossuficiência mudando o modelo de controle dos recursos, através da busca de terceiros para trabalhar como parceiros na chamada “Terceirização Estratégica”, onde não apenas atividades operacionais eram repassadas, mas também algumas que suportavam a tomada de decisão dos negócios. Seguindo para a década de 2000, veio à terceirização dos serviços de administração, supervisão e controle em banco de dados, redes e dos mecanismos de segurança, mostrando que não somente atividades mecânicas, ou de manutenção estavam sendo repassadas, mas também, em ritmo menor, atividades de planejamento, supervisão e controle, na chamada “Terceirização Revolucionária”. (Saad, 2006, p. 8).

Já hoje é inegável que a terceirização está presente em todos os setores de mercado, e nas mais diversas atividades, incluindo a área de TI. Meirelles (2008) ressalta os resultados da pesquisa da Eaesp/FGV onde constatou-se que em 2007, 98% das empresas do Brasil, já tinham parte de sua TI terceirizada.

2.2 OBJETIVOS ESPERADOS COM TERCEIRIZAÇÃO DE TECNOLOGIA DA INFORMAÇÃO (TI)

Com o aumento desse segmento de negócio, esse assunto se tornou alvo de discussões no mundo todo, e para entender melhor a busca das organizações pelo processo de terceirização é necessário avaliar os fatores que as levam a adotar esse tipo de prática, e que acabam sendo ponto crucial no momento da decisão. Faria (2008), cita os fatores abaixo como sendo os principais:

- Focar os recursos internos no ramo de atuação principal dos negócios, otimizando tempo e qualidade da execução dos serviços.
- Adquirir conhecimento especializado e em constante atualização dos recursos para realização de demandas de serviços específicos.
- Implementar um serviço ou uma solução que é utilizado pelo mercado, mas que não pode ser eficientemente fornecido pela organização, aumentando a competitividade frente aos concorrentes.
- Possibilitar a execução dos serviços em diferentes locais e distâncias, visando a continuidade dos negócios.
- Melhorar o processo de aquisição e manutenção dos equipamentos e serviços através do gerenciamento de capacidade baseado na demanda do negócio para atingir os objetivos da organização.
- Auxiliar no processo de escalabilidade, possibilitando a capacidade de manipular uma porção crescente de trabalho de forma uniforme, ou estar preparado para crescer rapidamente.
- Redução de custos através de melhores investimentos em recursos de tecnologia.

Além dos objetivos citados acima é importante destacar conforme cita Saad (2006, p. 10) que “o relacionamento contratante-provedor se caracteriza por ter alto valor agregado”, e por ter essa característica é esperado que o fornecedor de serviços atue de forma pró-ativa com relação a previsão de necessidades futuras do negócio, antecipando prioridades e tendências de mercado naquele setor, alinhando a estratégia da organização com a evolução de TI, para que isso ocorra ele tem que entender qual é o contexto da empresa, quais são os objetivos, a missão, a visão e os valores, somente assim conseguirá atingir o resultado esperado.

2.3 PROCESSO DE TERCEIRIZAÇÃO DE TI

O processo de terceirização tem início através de um documento chamado RFP[3] (*request for proposal*), onde a empresa especifica todos os requisitos técnicos e comerciais que espera ser atingido com o projeto, assim como o prazo para resposta. De posse deste documento, as prestadoras de serviço tomam conhecimento dos detalhes do projeto, e se candidatam para fornecer tais serviços, iniciando o processo de resposta a solicitação de proposta. A primeira etapa tem como objetivo conseguir das prestadoras uma posição se elas atendem, ou não, a cada requisito listado no documento, por isso é necessário que todos os aspectos sejam considerados no momento da sua elaboração, caso contrário, serão considerados fora do escopo do projeto, podendo trazer impactos futuros.

Albertin e Sanchez (2008), relatam que a elaboração da RFP não é uma tarefa fácil, devido a quantidade de elementos a serem considerados, e a amplitude da análise, sendo ela na maioria das vezes incompleta, para evitar que isso ocorra eles defendem que a tomada de decisão deve ser feita entre todas as partes envolvidas no processo, e não somente da alta administração.

Alguns desses elementos importantes em relação ao processo de terceirização são listados por Torres (2008) como sendo:

- Definição clara e precisa do objetivo esperado com o projeto.
- Requisitos técnicos que a empresa contratada deve atender para executar o projeto de forma completa e detalhada.
- Mapeamento de riscos, onde eles devem ser levantados através de uma análise crítica, e os mesmos devem ser contingenciados no contrato que será assinado entre as partes.
- Definição de papéis de responsabilidades no relacionamento com a empresa contratada é essencial, para avaliar o desempenho da empresa

[3] “RFPs são requisições de ofertas, mais especificamente, uma promessa que se torna contratualmente vinculativa a partir da assinatura entre as partes.” (EDWARDS, 2000, p. 39).

contratada, mantendo assim o nível adequado dos serviços e atuando em ajustes quando necessário, sempre mantendo boa comunicação.

- Enviar uma minuta com os termos contratuais que resguardem as partes;
- Definir como será o tipo de remuneração, preço fixo ou através de demandas de trabalhos;
- Solicitar comprovação do conhecimento dos recursos através do fornecimento de certificações e currículos;
- Solicitar documentos da empresa que comprovem a saúde financeira;
- Solicitar histórico de projetos similares que comprovem a experiência da empresa proponente;
- Listar os aspectos de segurança da informação envolvidos no projeto.

Dentre os elementos acima destaca-se a segurança da informação, pois o processo de terceirização de TI permite que as empresas parceiras tenham acesso e até, manipule informações muitas vezes confidenciais, tal fato aumenta a vulnerabilidade da empresa sob o ponto de vista de operar com segurança, conforme enfatiza Costa (2010). Nesse contexto a melhoria da gestão interna, com processos e pontos de controles de segurança bem definidos, e que auxiliem na gestão dos recursos internos e terceiros, é uma forma da empresa manter o controle e evitar que pequenos incidentes se potencializem.

Porém para que a organização consiga mitigar e reduzir os riscos, é importante entender a área de segurança e quais aspectos ela abrange, para que assim ela possa realizar uma análise dos riscos envolvidos no processo de terceirização de TI. O próximo capitulo traz uma abordagem sobre o tema Segurança da Informação em TI para auxiliar a compreensão do mesmo.

3 SEGURANÇA DA INFORMAÇÃO EM TI

Para definir o termo segurança da informação, é necessário entender o que é a informação, e qual sua importância no mundo dos negócios. Sêmola (2003), relata que independente do momento econômico, ou ramo de atuação da empresa, as informações sempre serão fator decisório para tomada de decisões e definição de planos estratégicos. Ainda ressalta o potencial competitivo do sucesso do negócio atrelado ao fator chave que seria o bom gerenciamento da informação.

Essas afirmações confirmam o valor da informação no ambiente corporativo e além disso, mostram como o decorrer do tempo e avanço da tecnologia transformou a forma de gerenciamento da informação, que deixou de ser centralizada em algumas pessoas para estarem armazenadas em servidores de armazenamento robustos, e trafegarem através da rede em uma velocidade e capacidade cada vez maior, deixando de lado os papéis e arquivos, hoje já obsoletos para qualquer negócio.

Apesar dos benefícios, os riscos trazidos por essas mudanças são cada vez maiores, e para que a segurança da informação ocorra, se faz necessária a implementação de controles e mecanismos integrados com intuito de reduzir e administrar os riscos a um nível aceitável.

3.1 ASPECTOS DE SEGURANÇA DA INFORMAÇÃO

Conforme a ABNT NBR ISO/IEC 27001, a segurança da informação pode ser considerado um conjunto de medidas com o objetivo de preservar e proteger a informação e os ativos em qualquer momento do ciclo de vida dos negócios, garantindo a confidencialidade, a integridade e a disponibilidade dos dados, considerados os pilares essenciais da segurança da informação. Podendo ser entendidos da seguinte forma:

- Confidencialidade, é a garantia de que a informação é acessível somente por pessoas autorizadas (NBR ISO/IEC 27002, 2013). O acesso sem

autorização, podendo ser intencional ou não, pode causar danos irreversíveis financeiros, e nos piores casos até a imagem da empresa, comprometendo a confiança do mercado, isso pode levar até a falência;

- Integridade, garantindo o conteúdo da informação e dos métodos de processamento (NBR ISO/IEC 27002, 2013), isso significa afirmar que a informação não sofra alterações sem autorização. Basicamente é o mínimo esperado por quem envia ou recebe uma mensagem via meios eletrônicos, o que foi enviado deve chegar com seu conteúdo integro, sem alterações no meio do caminho;

- Disponibilidade, que é a garantia de que somente usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 27002, 2013). Sistemas inoperantes, falhas de rede, ou qualquer outra falha do gênero que impossibilite o acesso a informação é uma falha grave de segurança e pode causar prejuízos para a imagem da organização, imagine uma empresa de cartões de crédito inoperante por 24 horas, quanto dinheiro não foi perdido nesse meio tempo, e quantos usuários não vão optar pela empresa concorrente que possuí sistema mais confiável.

Além dos pilares, outro ponto importante a ser compreendido, é o ciclo de vida da informação, sendo ele as ações que podem ser tomandas usando-a como: o manuseio, o armazenamento, o transporte e o descarte, comuns a qualquer tipo de negócio empresarial, porém podem ser alvo de atraques oriundos de ações mal intencionadas ou simplesmente descuido humano, potencializando os riscos de segurança. Esses ataques podem vir de elementos internos e externos comprometendo a segurança da informação, através das redes, dos computadores, de vírus, dos *hackers*, dos servidores e até da internet. O conjunto dos elementos e ciclo de vida da informação devem ser mapeados, para que se possa definir quais riscos estão atrelados a cada um deles.

3.1.1 RISCOS, VULNERABILIDADES E AMEAÇAS RELACIONADOS A SEGURANÇA DA INFORMAÇÃO

Segundo Fontes (2010), a permanência da empresa no mercado está intimamente ligada a sua preparação para atuar em falhas e interrupções que levam a impactos monetários, a imagem e até as operações. Todos estes aspectos refletem de forma negativa para a confiabilidade no mercado sobre os negócios da organização. Complementado com a visão de Semôla (2003), que entende que é um mito operar com risco zero, dado as inúmeras variáveis atreladas ao contexto empresarial, o que se deve fazer é procurar reduzir ao máximo a probabilidade do risco ocorrer, e isso é feito através de um trabalho constante de gestão de risco, através do mapeamento das vulnerabilidades e ameaças.

Com base nos autores observa-se que é essencial conhecer os riscos associados ao negócio, isso ajuda não somente no processo de resolução e gerenciamento de incidentes e problemas, mas também traz confiança de cliente e acionistas que conseguem ver um processo maduro e estruturado.

Para implementar a gestão de risco, a ABNT NBR ISO/IEC 27002 (2013) recomenda uma a avaliação dos riscos associados aos objetivos e estratégias da organização, isso deve ser feito através da análise das potenciais ameaças que podem atingir as vulnerabilidades, gerando uma estimativa que calcula o impacto da ocorrência no âmbito dos negócios.

Para entender melhor, os ativos podem sofrer ameaças, através de ações, acidentais ou não, enquanto os meios de armazenamento, manipulação e transmissão são vulneráveis, como uma falha no processo de segurança. Isso ocorre por motivos externos e internos, causados por mudanças no contexto no qual a empresa está inserida, como alteração de leis, mudança de processos internos, implementação de um novo sistema de processamento de dados e etc..

Para se atingir um nível aceitável de segurança da informação na organização devem ser implementadas técnicas e métodos de controle, como políticas, processos e procedimentos, esses itens devem ser usados para provocar uma mudança de cultura para todos os funcionários, e devem ser sempre apoiados pela

alta gerência. Após implementados, eles devem seguir uma rotina de controle, através do treinamento, monitoramento e análise dos resultados, para que em caso de detecção de falhas medidas de ajustes possam ser tomadas.

4 NORMA ABNT NBR ISO/IEC 27002 SET 2013

A Norma ABNT NBR ISO/IEC 27002 de 2013 foi elaborada para substituir a versão anterior datada de 2005. Trata-se de uma norma que estabelece diretrizes e práticas para implementação e controle de técnicas de segurança da informação. Está dividida em 14 seções com 35 objetivos e 114 controles. Apesar de não ter caráter normativo, veio para ser usada nas organizações de todo tipo ou tamanho, e que utilizam informações em suas ações, como referência na implementação de controles de gestão de segurança da informação com base na ABNT NBR ISO/IEC 27001. Devido a abrangência e objetividade do documento, o mesmo será utilizado como parâmetro para o estudo de caso proposto neste trabalho. Sendo assim, este capítulo busca analisar os aspectos recomendados pelas seções do documento ABNT NBR ISO/IEC 27002 de 2013, com o objetivo de dar subsídios para a realização do estudo de caso proposto.

4.1 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

Basicamente a Norma ABNT ISO/IEC 27002 (2013) auxilia no processo de adoção de controles que podem ser implementados para se obter os níveis assumidos de risco pela organização, considerado as legislações regulamentadoras nacionais e internacionais, assim como o enfoque no negócio.

O primeiro passo sugerido pela norma é a criação da política de segurança da informação, com o objetivo de guiar o negócio com o respaldo necessário. A política de segurança da informação é um documento que deve ser aceito por todos os funcionários da empresa, e as pessoas externas que fazem parte do negócio, ou seja, deve estar enraizado na cultura organizacional, sempre apoiada pela alta gestão da empresa.

Geus e Nakamura (2010, p.188) afirmam que:

> “A política de segurança da informação é a base para todas as questões relacionadas à proteção da informação, desempenhando

> um papel importante em todas as organizações. [...] Seu desenvolvimento é o principal passo da estratégia de segurança das organizações. É por meio dessa política que todos os aspectos envolvidos na proteção dos recursos existentes são definidos e, portanto, grande parte do trabalho é dedicado à sua elaboração e ao seu planejamento".

A política definida deve observar aspectos internos relacionados ao ciclo de vida da informação durante a execução das atividades, assim como os externos de organizações regulamentadoras, entre outros órgãos, que possam afetá-la de alguma forma. Para que isso ocorra é necessário a definição de um gestor, que apoiado por uma equipe multidisciplinar, trabalharão para analisar todos os riscos envolvidos e atualizar os requisitos no documento oficial, assim como trabalhar no processo de divulgação, treinamento e comunicação eficaz das mudanças aplicáveis.

Então, após a definição da parte mais generalista do documento, deve-se descer para a parte mais específica, onde está o contexto de aplicação prática da política, que baseado na ABNT NBR ISO/IEC 27002 (2013) seria, o controle de acesso a informação, classificação e tratamento, segurança física do ambiente, segurança lógica, uso aceitável dos ativos, mesa limpa e tela limpa, transferência das informações, dispositivos móveis e trabalho remoto, restrições sobre o uso e instalação de software, backup, transferência da informação, proteção contra códigos maliciosos, gerenciamento de vulnerabilidades técnicas, controles criptográficos, segurança nas comunicações, proteção e privacidade da informação de identificação pessoal e relacionamento na cadeia de suprimento.

4.1.1 DISPOSITIVOS MÓVEIS

Pensar que até pouco tempo atrás o dispositivo móvel que existia era o famoso disquete com poucos *kilobytes* de capacidade de armazenamento, em pouco mais de uma década essa realidade foi transformada, vieram os cd-room, dvds, pen drives usb, *blue-ray*, HD externo, que mudaram muito a forma e capacidade de armazenamento, saindo casa dos *kilobytes* e entrando na casa dos terabytes, aumentando assim a capacidade e a agilidade do armazenamento de

informações. Ao mesmo tempo que essa evolução trouxe benefícios para as empresas e usuários, trouxe também o desafio para a segurança da informação. Fontes (2010, p. 225) afirma que deve haver a identificação dos ativos e dos respectivos responsáveis, assim como as recomendações de utilização, com a finalidade de garantir a proteção da informação.

Para auxiliar o processo de gestão de dispositivos móveis a ABNT NBR ISO/IEC 27002 (2013) observa que é importante ocorrer o registro de todos os dispositivos móveis que podem ter acesso a rede, assim como práticas que devem ser tomadas para a proteção física dos mesmos, restrições para a instalação de *softwares*, processos de gerenciamento de atualização de *softwares* e aplicativos, restrições para a conexão no ambiente empresarial, controle de acesso, técnicas criptográficas, proteção contra códigos maliciosos, desativação, bloqueio e exclusão de forma remota, política de *backup*, e regras de utilização de recursos *web*.

A aplicação de tais controles pretende minimizar os impactos do risco de se utilizar tais equipamentos, principalmente se vierem de fora da empresa, onde não existem cuidados especiais para tratamento de segurança, assim como o armazenamento das informações. Como muitos desses dispositivos são relativamente pequenos, não é difícil de serem perdidos, ou até mesmo furtados, e se isso ocorrer, as informações sigilosas contidas naquele pequeno armazenador estarão nas mãos de uma pessoa estranha, que poderá usá-las para tirar proveito ou até mesmo expor ao concorrente, causando danos irreversíveis a imagem da empresa. Por isso a política deve observar, quando necessário, a proibição de dispositivos móveis pessoais, assim como procedimento de utilização em eventos externos, como o transporte seguro, o armazenamento adequado, e tudo isso deve ser claramente repassado aos funcionários, parceiros e quem quer que participe do ciclo de vida da informação.

4.1.2 TRABALHO REMOTO

Outra possibilidade trazida pela evolução da tecnologia, é o trabalho remoto, tendência em países desenvolvidos, e cada vez mais normal no ambiente corporativo. Além de reduzir custos com manutenção de escritório, traz qualidade de vida ao funcionário, e aumento de escalabilidade.

Rifkin (1996, p. 8) traz exemplos de duas grandes empresas globais que optaram pela flexibilização nos negócios:

> “Comprimindo o tempo e flexibilizando o espaço, a nova mágica eletrônica transformou a própria idéia de escritório, de conceito espacial para temporal. Empresas, como AT&T, começaram a introduzir a idéia de “escritório virtual”. Os funcionários são equipados com escritórios móveis, completo com laptop, fax e telefone celular e, literalmente, mandados para casa. (...) A Ernst and Young, empresa de auditoria com sede em Nova Iorque, recentemente reduziu seu espaço físico de 35 mil para 28 mil metros quadrados e instituiu um programa de “hotelaria”. Todos os funcionários abaixo do nível sênior foram “desalojados” de suas mesas. Agora quando querem usar um escritório, precisam fazer uma reserva com antecedência.”

Isso traz novos desafios para a política de segurança da informação, que deve considerar controles específicos, listados pela ABNT NBR ISO/IEC 27002 (2013) como por exemplo, o cuidado com a segurança física do local no qual será executado o trabalho, a comunicação utilizada para conexão das informações, os equipamentos que serão utilizados, evitando conexão, processamento e armazenamento de equipamentos pessoais a rede corporativa, a restrição de acesso de terceiros não autorizados a informações confidenciais como parentes e amigos, a utilização e configuração de rede sem fio doméstica, questões ligadas a reconhecimento de propriedade intelectual relacionada ao desenvolvimento de materiais ou produtos em equipamentos particulares, necessidade de averiguação em equipamentos particulares para investigar possíveis delitos, questões ligadas a licenças de softwares instalados no equipamento particular, e os requisitos de segurança que devem ser considerados como antivírus, firewall, regras e etc.

Independentemente de onde o trabalho for executado, a empresa sempre será responsável por qualquer problema, principalmente relacionado a segurança do funcionário e da informação. Para evitar incidentes no trabalho remoto, as diretrizes da política de segurança, sempre com base na lei que regulamenta a empresa, deve considerar todos os aspectos citados, e ou adicionais observados pelo gestor no momento da elaboração. Convém a empresa disponibilizar um ambiente, equipamentos e mobílias adequados e seguros, que tipo de trabalho pode sofrer essa ocorrência, por quanto tempo, isso com base nas características de informação tratada pelo tipo de serviço executado. Existem informações que nunca devem ter seu ciclo de vida feito fora do contexto empresarial, como monitoramento em tempo real de sistemas bancários.

Além do ambiente propício para a execução do trabalho, outro ponto importante é o estabelecimento elementos de segurança para a comunicação, como uma VPN[4] (*Virtual Private Network*). Assim como regras para acesso de terceiros a equipamentos da empresa, ou com informações da empresa, disponibilizar suporte para o usuário remoto, auditoria e monitoramento das ações, gerenciamento de direitos e cessão de acesso quando houver desligamento.

4.1.3 SEGURANÇA EM RECURSOS HUMANOS

Os recursos humanos têm um papel muito importante para a segurança da informação. Conforme citado por Sêmola (2003, p. 23), “muitas empresas e seus executivos são surpreendidos por essa afirmação, pois ainda hoje mantêm uma deficiência de percepção do problema que costumo chamar de “visão de iceberg"”, isso leva a organização a subestimar esses elementos, então se investe muito em equipamentos avançados e com grande capacidade para promover a segurança do ambiente, mas esquecem do poder que o usuário tem de manipular, corromper, extraviar a informação na qual ele tem acesso. Por isso essa consideração é tão

[4] VPN - Virtual Private Network, ou Rede Virtual Privada, é um termo usado para definir o processo onde os dados que trafegam em uma estrutura de rede pública são encapsulados por um tunelamento criptográfico, que devido a restrição de acesso, garante a privacidade e integridade das comunicações. (LINO, 2002).

importante, e deve ser observada logo na contratação do recurso humano, e as vezes perdurar determinado tempo após desligamento.

Conforme afirma Ferreira e Araújo (2008), o departamento de recursos humanos deve estar ciente das funções que um funcionário contratado irá desempenhar, se o mesmo possui restrição de acesso, quais documentos de confidencialidade o funcionário deve assinar garantindo sigilo das informações nas quais ele terá acesso, garantir que ele possua conhecimento técnico para executar a atividade, assim como conhecimento das penas previstas em casos de não cumprimento das ações de segurança. Uma opção é o estabelecimento de um código de conduta, além de treinamento e conscientização constantes.

Por fim, em caso de cessão do trabalho, antes do funcionário ser desligado de suas atividades seus acessos devem ser removidos, seus equipamentos devolvidos, seu acesso físico controlado, ele deve estar consciente das obrigações contratuais que se comprometeu após término do vínculo empregatício. Muito se sabe de profissionais, que descontentes por terem demitidos causam estragos para a imagem da empresa, ou até aplicam estratégias em negócios próprios.

4.1.4 GESTÃO DE ATIVOS

Segundo Fontes (2010, p. 225), é essencial a identificação dos ativos, assim como os seus responsáveis. Os ativos são elementos associados ao ciclo de vida da informação dentro da empresa, e para que ocorra o controle é necessário que seja criado um inventário dos ativos da empresa. O mesmo deve ser completo e atualizado constantemente, dado a velocidade das mudanças, a definição de um responsável por cada ativo, ou conjunto de ativos, também se faz essencial. A ABNT NBR ISO/IEC 27002 (2013) indica a ABNT NBR ISO/IEC 27005, como base para implementação de gestão de ativos, levando em consideração a importância deles na gestão de riscos.

O proprietário do ativo deve ser relacionado no momento da compra, ou transferência, e o mesmo será responsável por ele durante a sua estada como dono do ativo, garantindo que ele conste no inventário, sua classificação e proteção.

Também devem ser definidos levantamentos periódicos para controle de acesso, e tratamentos a serem aplicados quando houver exclusão ou destruição, fator este importante e que muitas vezes são esquecidos pelas organizações. Lembre-se que ativos que participaram do ciclo de vida da informação, mesmo que obsoletos são alvo potencial de ameaças, por isso o tratamento deve ser tratado de forma eficaz.

Além da classificação dos ativos, Araújo e Ferreira (2008, p. 34) recomendam que “Toda informação seja classificada, quando passar por alteração de conteúdo deve ser submetida a novo processo de classificação, com o objetivo de rever o nível mais adequado”. A ABNT NBR ISO/IEC 27002 (2013) cita um exemplo de classificação da informação quanto a confidencialidade em quatro níveis, um onde nenhum dano foi causado, outro quando houve um pequeno constrangimento por um incidente operacional, um que causa pequeno, porém significativo impacto nas operações e objetivos, e o último que afetou a longo prazo os objetivos e imagem da organização.

4.1.5 CONTROLE DE ACESSO

O acesso a informação deve ser observado como um privilégio dado a um usuário que desempenhará funções utilizando-a, e sempre com base na política definida para o controle que indicará os as necessidades do negócio e as regras de forma clara e precisa. (CAMPOS, 2007). Essa política deve também observar a cadeia de aprovações necessária de todos os proprietários e responsáveis, assim como a qualificação do nível de acesso que o usuário deverá ter ao sistema de acordo com o seu papel desempenhado, a criação de um sistema de controle de acessos, de preferência eletrônica, gerenciamento de transferência de acesso ou perfis, isso para possibilitar um maior controle do que está sendo acessado, por quem e em que momento. Mecanismos modernos conseguem emitir alertas de acesso não autorizado, e em um ambiente corretamente gerenciado o usuário é identificado e pode sofrer as sanções previstas na política de segurança.

Os detentores de acessos privilegiados, sendo eles administradores dos sistemas, com poderes especiais para atuar em atividades que requerem maior

confiança, também devem ser controlados com as mesmas regras citadas acima, e o grau de monitoramento deve ser considerado ainda maior, uma vez que o impacto do poder atribuído pode ser considerado de maior proporção.

A norma ABNT ISO/IEC 27002 (2013) recomenda que:

> “Convém que os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação sejam retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança dessas atividades.”

4.1.6 CRIPTOGRAFIA

A definição de criptografia é dada por Denis (2007, p. 1) como, “o método automatizado (ou algorítmico) que garante o cumprimento dos requisitos de segurança estabelecidos”, isso ocorre através do embaralhamento das mensagens trocadas via rede de computadores por mecanismos modernos, onde apenas o emissor e receptor possuem a técnica usada para elaborar a conversão da mensagem.

Existem vários métodos de aplicação, porém a definição do mais eficaz deve ser considerada por meio da análise das particularidades de cada negócio, como por exemplo através do levantamento do nível de criticidade classificado para cada transação. Outro ponto importante é a aplicação de um gerenciamento de chaves de criptografia e decriptografia que prevê ações em caso de perda ou comprometimento da chave, essas tarefas serão feitas pela definição dos papéis e responsabilidades que deverão garantir a implementação e manutenção da política de criptografia.

A ABNT NBR ISO/IEC 27002 (2013) descreve a criptografia como um elemento fundamental na busca de operar com segurança nas atividades empresariais, e recomenda a procura de um especialista em casos de não se ter conhecimento sobre esse tema.

4.1.7 SEGURANÇA FÍSICA E DO AMBIENTE

Young (2015, p. 3), faz as seguintes afirmações sobre o aspecto de segurança física:

> “O diretor de segurança decidiu instalar catracas para minimizar o risco de terrorismo, e à possibilidade de outras ameaças, reduzindo a vulnerabilidade que existia através do acesso físico não autorizado. No entanto, o indivíduo que passa por uma catraca pode estar usando ID de outra pessoa para ganhar acesso físico não autorizado. Se a probabilidade de isso é considerada baixa, alguma forma de autenticação pode ser utilizado como um controlo adicional, como a identificação biométrica ou um agente de segurança verificando fotografias do cracha? As respostas para essas questões de segurança nem sempre são claras uma vez que tais movimentos envolvem um custo.”

Young traz a importância de gerenciar esse aspecto, e já aponta um dos erros mais cometidos por alguns gestores, considerar no momento da definição da política de segurança da informação, somente o acesso lógico, esquecendo que parte dos ativos utilizados são físicos, e ficam alocados em ambientes físicos, os quais podem ser manipulados por pessoas. Assim, como já mencionado anteriormente, é necessário se fazer uma análise dos riscos, para se definir o que deve ser protegido com base em dados que justifiquem a ação.

Para evitar esse problema a ABNT NBR ISO/IEC 27002 (2013) estabelece algumas recomendações, como a definição da resistência do perímetro físico de segurança, a implementação de meios de identificação de acesso para cada ambiente, os requisitos de segurança contra incidentes naturais, a implementação de um sistema de detecção de intrusos, uma atenção especial para o cabeamento de redes, e cuidados com a manutenção dos equipamentos, através do registro dos ativos.

Além da segurança do ambiente e equipamentos, outra preocupação necessária é com relação aos ativos operados pelos usuários, os mesmos devem ser orientados sobre as regras de segurança que devem ser mantidas e as sanções previstas, para que assim os funcionários não deixem informações confidenciais expostas nas estações de trabalho, ou locais que possam conter informações confidenciais, como impressoras.

Todas essas observações ajudam a garantir a segurança das informações, porém como tanto o elemento físico e humano estão envolvidos, treinamento constante, monitoramento das regras e as sanções, são essenciais para a manutenção, o que não for implementado deve ser considerado na lista de controle de vulnerabilidades e ficar em constante observação.

4.1.8 SEGURANÇA NAS COMUNICAÇÕES

Esse item de segurança está relacionado a forma como as informações serão protegidas no momento em que estão trafegando na rede, através da análise das tentativas de acesso, podendo controlá-las de forma à negar tentativas de acesso consideradas não seguras, e também garantindo que os equipamentos conectados possuem todos os requisitos de segurança atualizados e funcionando, como o antivírus e os *patches*[5] liberados pelos fabricantes.

Porém para garantir a segurança nas comunicações contra o acesso não autorizado é essencial definir as responsabilidades pelo gerenciamento dos equipamentos em rede, onde os responsáveis devem controlar as regras de utilização, através da implementação de autenticação no acesso, a criação da distinção dos departamentos através de VLAN[6] (*Virtual Local Area Network*), e também com a definição de regras de filtragem adequadas no equipamento de *firewall*[7]. A extensão de alcance das redes está cada vez maior, possibilitando a comunicação da empresa sem barreiras geográficas ou físicas, e a política de segurança deve acompanhar essa evolução considerando todos os equipamentos que fazem parte do ciclo de vida da informação.

---

[5] São programas de computador criados pelos fabricantes de *software* para corrigir erros que são identificados nos códigos dos produtos comercializados. É considerado um itém muito importante para a segurança da informação, pois sua aplicação corrige vulnerabilidades e reduz risco de um ataque. (NICASTRO, 2011)

[6] VLAN é um termo criado para definir a separação lógica dos recursos conectados a rede com base nas portas ou no endereço MAC dos dispositivos, isso faz com que os diferentes grupos não consigam acessar informações um do outro, garantindo segurança de acesso a informações e também evitando que riscos se propaguem na rede. (ANGELUSCU, 2010).

[7] *Firewall* é um dispositivo onde regras são definidas com o objetivo de controlar (permitir ou negar) o fluxo entre diferentes redes. (STEWART, 2014).

4.1.9 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Um item muito importante para o tema proposto, é o aspecto relacionado aos sistemas uma vez que a maior parte dos sistemas de informação são adquiridos de fornecedores especializados em programas e soluções. Para garantir a segurança da informação durante esse processo, é recomendável que se mantenha requisitos, tanto para os novos fornecedores, quanto para os já existentes, assegurando que a entrada, saída ou manutenção em ambiente de produção não traga riscos, e se trouxer que os mesmos sejam apropriadamente mensurados. Tais requisitos devem considerar a confiança exigida pelo negócio no gerenciamento dos usuários, a proteção dos ativos envolvidos, a monitoria e não repúdio das atividades executadas, além de políticas especiais para gerenciamento de redes públicas.

ABNT NBR ISO/IEC 27002 (2013) recomenda que um processo de testes seja definido para aquisição de produtos, e que os contratos com fornecedores enderecem os requisitos de segurança identificados, isso ajudará a manter a segurança quando houver a introdução dos novos produtos ou serviços no ambiente corporativo, sendo eles:

- Acordar a propriedade intelectual e direitos autorais do conteúdo desenvolvido;
- Exigir um modelo de tratamento de ameaças aprovado aplicável ao negócio;
- Definir critérios de aceitação para a qualidade dos entregáveis, baseado em níveis pré-estabelecidos;
- Possibilitar a auditoria para garantir que a segurança acordada foi mantida, para a privacidade dos dados, os testes do ambiente pós desenvolvimento tanto para ataques maliciosos quanto existência de vulnerabilidades;
- Acordar um prazo de garantia que cobre riscos que o serviço possa trazer após o termino da execução;
- Inserir penalidades monetárias para não cumprimento dos níveis de serviço pré-estabelecido, com o cálculo baseado no impacto acarretado.

Para esse tipo de serviço é recomendado a utilização da ABNT NBR ISO/IEC 27036-1 (2014) que trabalha especificamente com o gerenciamento de serviços terceirizados em serviços de TI.

4.1.10 RELACIONAMENTO NA CADEIA DE SUPRIMENTO NOS ACORDOS COM FORNECEDORES

Com base em Arway (2013, p. 1), a cadeia de suprimento é formada por conexões com o objetivo de facilitar a movimentação dos suprimentos, podendo ser pequena com poucas ligações e células, ou podendo ser longa e complexa, considerando a terceirização nesse contexto, onde funcionários externos irão realizar parte dos serviços e terão acesso à informações internas enquanto desempenham suas atividades. O gestor da política de segurança da informação precisa entender como essa interação irá ocorrer para que assim consiga mitigar os riscos associados e cobrar da empresa contratada os requisitos necessários para manter o ambiente seguro, e em caso de falhas como o repasse das responsabilidades irá ocorrer, através de multas, notificações e etc.

Segundo a ABNT NBR ISO/IEC 27002 (2013):

> “As organizações são aconselhadas a trabalhar com fornecedores que entendam a cadeia de suprimento de tecnologia da comunicação e informação e quaisquer questões que tenham impacto relevante sobre os produtos e serviços que estão sendo fornecidos.”

O documento ainda faz observações específicas para esse tipo de contratação, em que antes mesmo da empresa lançar no mercado a licitação para serviços de tecnologia da informação, é recomendado uma reunião técnica interna com o objetivo de definir os requisitos da aquisição, assim como os impactos esperados durante o desenvolvimento, isso pode ajudar a empresa contratante a gerenciar o comportamento do fornecedor durante ciclo de vida da informação.

Os pontos mencionados acima são os seguintes: a definição do termo de confidencialidade das informações trocadas durante a negociação e durante todas

as fases do projeto, assim como as sanções que serão tomadas em caso de violação; estabelecimento de um termo de comprometimento de todo o time envolvido no projeto que terá acesso a informação da empresa contratante; definição de uma política de segurança que irá conduzir o contrato de prestação de serviços; um processo de resolução de incidentes claro e bem definido para ambas as partes; treinamento contínuo da equipe para conscientizar sobre os riscos e sanções aos quais os funcionários estão sujeitos em caso de violação da política de segurança; inclusão de item regulamentando a possibilidade de subcontratação para realização de parte dos serviços e as responsabilidades para gestão do subcontratado; definição de contatos estratégicos para fácil acesso em casos de incidentes ou questionamentos de segurança; definir pré-requisitos para a seleção do fornecedor com base nas normas de segurança; possibilitar auditoria nos processos do fornecedor para verificar a aderência ao itens acordados em contrato; definir período de garantia para resolução de falhas e conflitos gerados durante ou após a entrega do serviço ou produto contratado; estabelecer termos de aceitação para os entregáveis do projeto, assim como prazos e níveis para resolução para os serviços não aceitos; e garantia contratual que o fornecedor e toda a equipe envolvida irá atuar conforme definido na política de segurança da informação.

Apesar de essenciais para resguardar os direitos da contratante com relação aos itens de segurança, os mesmos devem ser analisados conforme o tipo de serviço que será prestado, por qual tipo de organização, qual o grau de risco associado, negociações desse tipo envolvem aspectos particulares, onde a importância pode ser considerada subjetiva. O importante na gestão é que toda flexibilização deve ser alinhada ao risco que poderá surgir.

4.1.11 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Blyth (2009), define o gerenciamento de incidentes como um componente do plano de continuidade dos negócios, e ele oferece as orientações necessárias para resposta de forma rápida e eficaz as crises que ocorrem dentro do ambiente enquanto atividades são desempenhadas, esse direcionamento é baseado no resultado da gravidade de cada incidente definido na análise de riscos elaborada.

Para isso a gestão de incidentes de segurança da informação que deve ser clara quanto a definição dos papéis e responsabilidades que deverão ser acionados em cada caso, como deverão manter o monitoramento dos itens definidos como críticos, mantendo sempre o registro das atividades realizadas em cada processo, incluindo aspectos de escalabilidade e comunicação interna e externa. Afinal um incidente de segurança não tratado de forma adequada pode atingir proporções maiores e causar danos irreparáveis aos negócios.

4.1.12 GESTÃO DA CONTINUIDADE DO NEGÓCIO

O autor Hiles (2014, p. 1), define a continuidade dos negócios como “a habilidade da organização sobreviver e ter sucesso, dependendo da capacidade de se recuperar após um desastre”, e a ABNT NBR ISO/IEC 27002 (2013) define como item essencial no gerenciamento de segurança, que ele deve ocorrer através do estabelecimento de um estrutura que responda em casos de interrupção dos serviços, com recursos treinados para atuarem nas atividades definidas como vitais a existência dos negócios, documentando as ações para usar como respostas a questionamentos futuros, ou seja todos os procedimentos devem garantir que em situações adversas a empresa continue a operar de forma rápida e eficaz, sem que os clientes sejam afetados com tal evento.

Porém para garantir que o plano de continuidade funcione, testes de contingência devem ser executados com regularidade, onde os recursos treinados irão desempenhar as atividades críticas, assim como a manutenção de um ambiente redundante para o caso dos servidores sofrerem danos. Em ambos os casos, o investimento pode ser considerado alto, porém o efeito causado pela indisponibilidade em casos de desastre é incalculável.

Os benefícios esperados com o programa de continuidade dos negócios, é deixar a estrutura operacional da empresa resiliente, manter a conformidade com requisitos exigidos por órgãos externos, capacidade de alcançar os objetivos definidos mesmo em caso de um desastre, e o mais importante manter a imagem, reputação e os valores da empresa perante o mercado, mostrando a confiabilidade de que tais eventos não irão afetar os clientes finais.

5 ESTUDO DE CASO

Esse estudo de caso visa analisar se os aspectos de segurança da informação recomendados pela ABNT NBR ISO/IEC 27002 (2013) são observados nas solicitações de propostas (RFPs) de empresas que buscam parcerias para implementar, desenvolver ou realizar a manutenção dos serviços de tecnologia da informação.

5.1 FORMA DE ABORDAGEM E COLETA DE DADOS

Para a realização do estudo de caso foi utilizada a abordagem de forma qualitativa através da seleção de solicitações de propostas de empresas de grande porte, que optaram pela terceirização dos serviços de tecnologia, e dentro de um universo, sete foram selecionadas de forma aleatória.

Após a seleção dos documentos uma planilha foi montada com os parâmetros indicados pela ABNT NBR ISO/IEC 27002 (2013), para que fosse usada como suporte a análise dos documentos possibilitando a identificação da menção dos controles especificados na Norma, para cada item encontrado foi atribuído um ponto na planilha, para que assim no final fosse possível obter o resultado esperado.

5.1.1 APRESENTAÇÃO DAS EMPRESAS

EMPRESA A

A primeira RFP objeto de estudo, é a empresa denominada como Empresa A, sendo ela uma organização brasileira privada que atua no ramo educacional para ensino superior.

Os sistemas de tecnologia da informação dessa empresa evoluíram de forma a cobrir as necessidades de negócio, porém ciente da necessidade de implementar modelos de gerenciamento com base nas melhores práticas de mercado e estar

preparada para suportar os novos crescimentos e desafios impostos pelo crescente mercado de educação, a TI do grupo decidiu revisar as práticas de fábrica de software, consolidando o desenvolvimento, manutenção e suporte de terceiro nível de suas aplicações dos sistemas acadêmicos de acordo com as especificações constantes em um documento de RFP.

EMPRESA B

A segunda RFP objeto de estudo, é a empresa denominada como Empresa B, sendo ela uma organização multinacional com atuação no mercado brasileiro de indústrias automobilísticas.

A empresa B busca prospectar, homologar e selecionar uma empresa para a prestação de serviços de suporte, manutenção e desenvolvimento de aplicativos móveis, no qual o cliente já possuía um serviço advindo de uma contratação anterior, porém necessitava de uma parceira para absorver novos serviços previstos nesta contratação.

EMPRESA C

A terceira RFP objeto de estudo, é a empresa denominada como Empresa C, sendo ela uma organização nacional com atuação no ramo farmacêutico.

O objetivo do processo de terceirização é selecionar fornecedores para a implementação de uma nova ferramenta ERP com módulos fiscais, financeiros e contábeis.

EMPRESA D

A quarta RFP objeto de estudo, é a empresa denominada como Empresa D, sendo ela uma organização multinacional com atuação no ramo de commodities agrícolas.

O objetivo desta RFP é obter informações com maior agilidade e precisão para tomada de decisão na companhia, no que dis respeito a gestão de processos,e apuração de custo de suas operações agrícolas, industriais e logísticas.

EMPRESA E

A quinta RFP objeto de estudo, é a empresa denominada como Empresa E, sendo ela uma organização multinacional com atuação no setor telecomunicações.

A empresa busca com esta RFP conhecer a oferta no mercado que atenda à necessidade de adquirir consultoria de mapeamento, definição e implantação de processos.

EMPRESA F

A sexta RFP objeto de estudo, é a empresa denominada como Empresa F, sendo ela uma organização multinacional com atuação no setor de telefonia móvel.

A empresa busca com esta RFP uma solução para suportar análise de tecnologias móveis, que emitisse relatórios que suportasse a tomada de decisões estratégicas.

EMPRESA G

A sétima RFP objeto de estudo, é a empresa denominada como Empresa G, sendo ela uma organização multinacional com atuação no setor mineração.

A empresa busca no mercado a prestação de serviços de concepção, construção, implantação, manutenção e coordenação de projetos de soluções de compras corporativas online e de gestão da base de fornecedores.

5.2 ANALISE DAS SOLICITAÇÕES DE PROPOSTAS

Através de uma análise individual das solicitações de propostas que foram aleatoriamente selecionadas, o objetivo deste estudo de caso foi realizar a identificação dos parâmetros de segurança de informação indicados pela ABNT NBR ISO/IEC 27002 (2013) nestes documentos, como forma de avaliar a relevância dos aspectos de segurança da informação no momento da contratação de fornecedores de serviços de tecnologia da informação e comunicação.

Nas seções a seguir, estão apresentados as análises sobre cada aspecto abordado pela ABNT NBR ISO/IEC 27002 (2013).

5.2.1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Através da análise dos documentos foi possível observar que a política de segurança foi mencionada em três solicitações de proposta, onde nestas as empresas exigem que a prestadora de serviços siga o documento de política de segurança já estabelecido pela contratante, porém não mencionam quais aspectos estão contidos no mesmo. Uma vez que o documento é mencionado na solicitação de proposta, a empresa que está interessada no fornecimento do serviços pode vir a solicitar este documento para que avaliado durante o processo de elaboração da proposta.

A ABNT NBR ISO/IEC 27002 (2013) alerta neste sentido que qualquer uma das políticas de segurança da informação que for distribuída fora da organização, convém que cuidados sejam tomados para não divulgar informações confidenciais a empresa. Inclusive menciona que algumas organizações usam outros termos para estes documentos da política, como "Normas", "Diretrizes" ou "Regras".

5.2.2 GESTÃO DE DISPOSITIVOS MÓVEIS

Essa seção propõe apresentar como as empresas tratam a gestão de dispositivos móveis dentro do documento de solicitação de proposta.

De acordo com a análise foi verificado que dentre as empresas que observaram esse aspecto, foi exigido que a proponente garantisse: a orientação dos funcionários quanto ao acesso apenas as informações exclusivas para execução seu trabalho; não deixar informações do cliente disponibilizadas nas telas do computador ou em cima da mesa quando houver possibilidade de visualização ou acesso por pessoas ao redor; certificação de que a estação de trabalho ou qualquer outro equipamento sob o controle do funcionário possui a última atualização de antivírus e versão de segurança; evitar armazenar dados do cliente em dispositivos ou mídias portáteis com possibilidade de roubo, caso seja inevitável, usar mídia portável; é obrigatório criptografar dados eletrônicos e armazenar o dispositivo em ambiente seguro, assim que a informação do cliente não for mais necessária para o trabalho, desfazer-se da informação; dados de cliente que precisem ser transferidos devem estar criptografados ou os protocolos de segurança industriais.

5.2.3 GESTÃO DE TRABALHO REMOTO

Gestão de trabalho remoto foi um aspecto de segurança que apareceu em apenas uma das RFPs, o que chama a atenção, uma vez que estas empresas podem estar expostas a riscos inerentes da própria terceirização de serviços, já que é bastante usual nesses tipos de contratos a contratante conceder a terceiros o acesso remoto a sua rede interna.

Uma das recomendações da ABNT NBR ISO/IEC 27002 (2013) em relação ao aspecto de Gestão de Trabalho Remoto é que seja realizada a provisão de equipamento de comunicação apropriado, incluindo métodos para acesso remoto seguro. Ficou evidente nesta amostra que poucas empresas deixam explícita na RFP este aspecto de segurança, o que posteriormente poderá ser uma ameaça a

empresa caso não sejam definidas as regras e os recursos disponíveis para concretização da Gestão de Trabalho Remoto.

5.2.4 SEGURANÇA EM RECURSOS HUMANOS

O aspecto da segurança em recursos humanos é por muitas vezes preterido devido a uma maior preocupação das empresas com os aspectos tecnológicos, fato percebido durante a revisão bibliográfica, e também verificado no momento da análise das solicitações, onde apenas uma empresa destacou a necessidade de que a proponente considerasse na proposta elaborada, itens relacionados a gestão dos profissionais, como definição de papéis e responsabilidades de cada funcionário, constante treinamento e revisões periódicas das práticas seguras, o preparo do time de recursos humanos para selecionar pessoas levando em consideração as exigências do cargo ocupado.

Dado o poder que o usuário tem em manipular, corromper, extraviar a informação na qual ele tem acesso, é importante que a empresa prestadora do serviço adote práticas seguras que vão desde garantir que seus profissionais sejam treinados antes do início efetivo do suporte, até a remoção completa dos acessos em caso de perda do vínculo empregatício, ou perda da necessidade que justifique o acesso, para que não ocorra nenhuma prática que comprometa a prestação do serviços.

5.2.5 GESTÃO DE ATIVOS

Essa seção aborda a gestão de ativos como a criação de um inventário que visa classificá-los com informações específicas para localização, definição de riscos associados, responsabilidades em caso de incidentes e gestão do ciclo de vida que envolvam ativos sob sua responsabilidade.

Apesar da importância deste aspecto, ele não foi encontrado em nenhuma das solicitações de propostas, isso pode ser compreendido ao se analisar as RFPs

onde o tipo de alguns serviços prestado será apenas consultoria, sem disponibilização de máquinas e/ou desenvolvimento de programas porém deveria ter sido contemplado para as RFPs que cujo o serviço prestado não se restringe apenas a consultoria.

Ao se analisar as RFPs que prevêm o desenvolvimento e a manutenção de sistemas, a empresa contratada deverá fornecer programas, equipamentos físicos e a própria informação. Todos estes itens são considerados ativos que serão manipulados no momento dos testes até a implementação. Nesses casos, a ABNT NBR ISO/IEC 27002 (2013) aconselha a definição de regras para a gestão dos ativos onde também devem ser definidas as responsabilidades da contratada, e quais ficarão sob a gestão da contratante, isso ajudará a resolver incidentes mais rapidamente, e também otimiza a organização dos recursos da empresa.

5.2.6 CONTROLE DE ACESSO

Durante a análise das RFPs foi possível verificar que duas empresas observaram este item como exigência a ser cumprida pela empresa proponente. Em uma delas consta que a empresa que desempenha o serviço objeto da proposta deverá se basear em um documento interno chamado “Controle de Acesso à Aplicações”. Já a outra empresa é mais abrangente exigindo uma lista dos ativos que serão acessados durante o desempenho das atividades acompanhado da justificativa de negócio. Nesta, consta também um processo de aprovação para liberação de acesso envolvendo responsáveis de ambas as empresas.

O controle de acesso, tanto o físico, quanto o lógico, é considerado um dos aspectos mais importantes. A ABNT NBR ISO/IEC 27002 (2013) recomenda a definição de regras de liberação de acesso ao usuário com base, única e exclusivamente, relacionada as atividades desempenhadas, assim como recomenda deixa-lo ciente das sanções que sofrerá em casos de utilização do acesso para fins que tragam riscos aos negócios. Por isso, empresas que não mencionam esse aspecto acabam deixando a empresa vulnerável e sem respaldo caso um terceiro venha a acessar informações sensíveis e a utilize de forma incorreta, que podem trazer danos aos negócios.

5.2.7 CRIPTOGRAFIA

Está seção buscou identificar nas solicitações de propostas a menção quanto a utilização de técnicas de criptografia exigida pelas empresas constratantes para a execução dos projetos.

Levando em consideração que independente do tipo de projeto base da contratação, os profissionais da contratada terão acesso a rede para troca de mensagens, acesso aos banco de dados internos e equipamentos físicos, é importante a exigência da aderências as práticas de criptografias mais apropriadas para cada atividade. No entanto, apenas duas empresas destacaram esse aspecto como obrigatório nas RFPs. Este fato pode ser considerado por falta de conhecimento das melhores práticas durante a elaboração do documento, ou devido ao alto custo que poderia aumentar o valor do projeto, o que é um erro uma vez que incidentes de segurança traz danos incalculáveis à imagem da organização.

A ABNT NBR ISO/IEC 27002 (2013) descreve a adoção de métodos criptográficos adequados a cada equipamento como uma forma eficaz de proteção a informação, e a ausência traz vulnerabilidades por deixar a informação trafegando em texto claro, onde qualquer ameaça pode capturá-la e obter vantagem sobre isso.

5.2.8 SEGURANÇA FÍSICA E DO AMBIENTE

A segurança física e do ambiente visa proteger os locais onde os equipamentos estão disponibilizados, assim como barreiras de resistência de acesso a esses lugares. A norma ABNT NBR ISO/IEC 27002 (2013) recomenda que alguns itens seguros sejam implementados, como localização estratégica, identificação de acesso autorizado, proteção contra acidentes naturais, detecção de intrusos, também recomenda cuidados especiais para parte de cabeamento de redes e regras de utilizações das estações de trabalho.

Durante a análise das RFPs em apenas uma delas verificou-se a exigência que a empresa proponente garantisse que as áreas onde existem processamentos de informações sensíveis e críticas, deveriam ser fisicamente protegidas contra acesso não autorizado, danos e interferências, assim como controle de acesso físico e registros de entrada e saída. Quando o serviço for realizado nas depêndencias da contratante, o fornecedor deverá seguir as regras vigentes da política interna desta empresa.

As demais solicitações que não atendem a este aspecto podem estar vulneráveis, caso a contratada opere seus dados sem condições seguras, podendo ser alvo de ataques que resultem em roubo de dados, e até desastres naturais que podem atingir o ambiente físico e causar destruição dos dados.

5.2.9 SEGURANÇA NAS COMUNICAÇÕES

Este aspecto está relacionado a forma como a empresa contratante deseja que a contratada trate as informações que circulam na rede, a Norma ISO define que controles quanto a definição de segmentação da rede entre os departamentos e regras de filtro de mensagens.

A análise das RFPs mostrou que cinco das empresas que buscam parceria no mercado observaram este item, exigindo que a empresa prestadora do serviço utilize métodos seguros em todos os protocolos de comunicação entre sistemas, respeitando as políticas de acesso implementadas nos firewalls, equipamentos de segurança, antivírus e outras proteções implantadas no ambiente do cliente. Também estabelecem que qualquer mecanismo de comunicação fora dos padrões internacionais de mercado deverá ser negociado e aprovado pela equipe de segurança da informação do cliente.

5.2.10 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO

Este aspecto está mais relacionado as solicitações que buscam parcerias para a implementação e desenvolvimento de programas e aplicativos, onde a empresa contratada será responsável por entregar um software como resultado final do contrato.

A análise mostrou que três empresas mencionaram a preocupação com o plano que seria considerado para o desenvolvimento do código do programa seguindo recomendações seguras, como a definição da propriedade intelectual para a contratante, a definição do controle de qualidade dos serviços por etapas, a penalização por falhas encontradas nos códigos dos programas, um período de garantia após o término do contrato, uma fase de testes antes da implementação com o objetivo de encontrar falhas e vulnerabilidades que possam a vir a afetar o ambiente de produção.

A empresa que não tinha como objetivo o desenvolvimento de programas de computador, não se preocupou com esse item, o que é compreensível. As demais empresas, que visam implementação de sistemas de informação, poderão sofrer durante a execução do projeto, pois esse aspecto ajudaria a conduzir todo processo de desenvolvimento, assim como respaldar em casos de falhas que podem causar problemas para o ambiente de produção como a indisponibilidade e brechas que podem vir a ser exploradas por ameaças.

5.2.11 ACORDO COM FORNECEDORES

Está seção buscou identificar nas RFPs a preocupação das empresas contratantes com relação a gestão dos fornecedores.

A análise mostrou que três empresas observaram aspectos relacionados ao item como: a definição de termos de confidencialidade dos dados entre fornecedores; as sanções que serão tomadas em caso de não cumprimento; o

treinamento dos funcionários terceirizados com relação as normas de segurança necessárias; a possibilidade do fornecedor subcontratar e sob quais exigências da empresa que contratou os serviços e penalidades aplicáveis em casos de não cumprimento com os requisitos de segurança.

Definir regras no acordo com fornecedores ajuda a alinhar entre as partes o que a empresa contratada aceita durante a prestação do serviço, e também prevê a possibilidade de término de contrato sem ônus em caso de não cumprimento das exigências e não definí-las pode amarrar a empresa a um serviço de má qualidade e que não alcança os resultados esperados.

5.2.12 GESTÃO DE INCIDENTES

A definição da gestão de incidentes mostra maturidade da empresa em resolver os mesmos de forma rápida e eficaz, evitando que uma pequena falha, ou interrupção se torne um grande problema para os negócios.

Apesar da importância deste aspecto, ele não foi mencionado em nenhuma das solicitações de propostas, o que pode ser considerado arriscado uma vez que a empresa executará atividades no ambiente do cliente podendo causar incidentes, e a resolução não seguirá um método pré-acordado para o tempo e forma necessária para se resolvê-lo. Isso deixa a empresa contratante por vezes sem o conhecimento de que existe um incidente, ou se ele foi ou não resolvido.

5.2.13 CONTINUIDADE DE NEGÓCIOS

Assim como o item anterior, o aspecto da continuidade dos negócios também não foi encontrado em nenhuma RFP.

Como a prestadora de serviços irá operar recursos como banco de dados do cliente, poderá armazenar dados referentes a elaboração do projeto entre outros itens. Seria necessário a preocupação sobre este tema, se por acaso ocorrer algum

problema como a perda dos dados durante a execução do projeto, todo o trabalho feito será perdido gerando retrabalho, ou até a impossibilidade de término dependendo da severidade do problema causado. Por isso a norma ABNT NBR ISO/IEC 27002 (2013) recomenda que seja implementada políticas de backup periódicos, e em locais seguros, treinamento e testes de contingência para preparar os recursos para casos de desastres e redundância dos ambientes, para que em caso de perda de um equipamento ou informação, isso não afete a continuidade dos negócios.

A perda de dados causada pela falta de um plano de continuidade de negócios gera uma imagem negativa da empresa para o mercado, fazendo com que a vantagem competitiva desejada possa não ser alcançada pela falta de confiança dos clientes para com aquela companhia.

5.3 RESULTADOS OBTIDOS

Na **Tabela *1*** estão apresentados os resultados consolidados das análises das RFPs das sete empresas deste estudo de caso, sobre os aspectos recomendados pela ABNT NBR ISO/IEC 27002 (2013):

Tabela 1. Análise de aderência das RFPs aos aspectos de segurança.

Empresa	Escopo da RFP \ Aspectos de Segurança da Informação	Política de SI	Dispositivos Móveis	Trabalho Remoto	Segurança em Recursos Humanos	Gestão de Ativos	Controle de Acesso	Criptografia	Segurança Física e do Ambiente	Segurança nas Comunicações	Aquisição, Desenvolvimento e Manutenção	Acordos com Fornecedores	Gestão de Incidentes	Continuidade do Negócio
1	Desenvolvimento e Manutenção de Software	■	■	■	■		■	■	■	■	■	■		
2	Desenvolvimento e Manutenção de Aplicativos	■	■				■	■		■	■	■		
3	Implementação e Manutenção de SIs	■	■							■	■	■		
4	Implementação e Manutenção de SIs									■				
5	Mapeamento e Implantação de Processos									■				
6	Implementação e Manutenção de SIs													
7	Implementação e Manutenção de SIs													

Legenda:

Existente	■

Fonte: Próprio autor

Com base na análise foi possível identificar que as empresas que buscam parcerias para algum tipo de serviço de TI, independente do ramo de atuação, observam apenas alguns aspectos de segurança da informação, porém não mencionam outros essenciais para execução segura do serviço objeto da contratação, o que as deixam vulneráveis em tais parâmetros e pode trazer riscos ao negócio.

Adicionalmente, pode-se observar que as empresas que buscam fornecedores para desenvolvimento e manutenção de software ou aplicativos são as que mais se preocupam em detalhar na RFP os aspectos de segurança propostos pela ABNT NBR ISO/IEC 27002 (2013).

5.4 SUGESTÕES PROPOSTAS

Com base na revisão bibliográfica, e no estudo de caso elaborado, uma sugestão para as empresas que optam pela terceirização dos serviços de TI através da disponibilização de RFPs no mercado, que elas baseiem a elaboração do documento em padrões reconhecidos pelo mercado, sempre apoiada pela área de tecnologia interna, pela área que será afetada com a nova solução e a alta administração da empresa.

Nos casos em que a empresa contratante não possuir equipe interna de tecnologia com conhecimento necessário para elaborar um anexo de segurança, é recomendado que a empresa procure por um consultor externo com conhecimento para ajudar a definir quais aspectos são relevantes dado o tipo de serviço que a empresa busca através da parceria.

Também é aconselhado nesse caso que antes de assinar o contrato de parceria, a empresa contratante forneça uma cópia para que o fornecedor saiba com que itens está se comprometendo, ou então que seja criado um anexo de segurança em conjunto, onde ambos concordem com os parâmetros aplicáveis ao serviço objeto da contratação.

6 CONSIDERAÇÕES FINAIS

À partir da análise dos dados, observa-se que, a tecnologia da informação é essencial para a sobrevivência das empresas no mercado, seja qual for o porte ou segmento de atuação, e os investimentos em TI são necessários e essenciais para que a empresa seja competitiva no mercado. Diante desta condição, muitas empresas optam pela terceirização desses serviços, que apesar dos benefícios, envolve também vários aspectos, como a segurança da informação, que deve ser prevista desde a elaboração do documento de solicitação de proposta a ser enviado ao mercado na busca de parceiros. Recomenda-se que tais empresas baseiem-se em em normas reconhecidas pelo mercado.

Nesse contexto, o presente trabalho propôs o estudo da norma NBR ISO/IEC 27002, sobre o contexto de gerenciamento de segurança da informação em caso de terceirização, e também a análise de RFPs lançadas por empresas de diferentes segmentos de atuação e tipos de serviços, com o intuito de identificar quais aspectos de segurança eram observados, e discutir formas de introduzir os aspectos de segurança da informação nas negociações de serviços de TI.

Os resultados das análises foram obtidos de forma satisfatória, onde verificou-se que as empresas observam alguns aspectos de segurança da informação no momento em que elaboram as solicitações de proposta a serem publicadas ao mercado. Porém, algumas empresas parecem não se preocupar com todos os aspectos recomendados pela norma NBR ISO/IEC 27002, o que poderá acarretar em risco potencial durante a execução do projeto.

Para trabalhos futuros, recomenda-se estudar as práticas que as empresas fornecedoras de serviços de TI podem adotar ou tem adotado durante a análise das solicitações de propostas de licitações, de forma a identificar os potenciais riscos aos futuros contratos, que poderão ser impactados pela ausência de especificação ou clareza dos requisitos de segurança da informação.

Também aconselha-se o estudo dos motivos pelas quais as empresas adotam alguns itens, e deixam os outros de lado, relacionando-os com a necessidade dos negócios.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. Projeto da NBR ISO/IEC 27002:2013. **Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação.** Associação Brasileira de Normas Técnicas, 2013.

ABNT. Projeto da NBR ISO/IEC 27001:2006. **Sistemas de gestão de segurança da informação – Requisitos.** Associação Brasileira de Normas Técnicas, 2006.

ALBERTIN, A. L; SANCHEZ, O.P. **Outsourcing de TI:** impactos, dilemas, discussões e casos reais. São Paulo: FGV, 2008.

ANGELESCU, S. **CCNA certification all-In-one for dummies.** Indiana: John Wiley & Sons, 2010.

ARWAY, A. G. **Supply chain security:** a comprehensive approach. New York: CRC Press, 2013.

BLYTH, M. **Business continuity management:** building an effective incident management plan. New Jersey: John Wiley & Sons, 2009.

CAMPOS, A. L. N. **Sistema de segurança da informaçao**: controlando os riscos. 2. ed. São Paulo: Visual Books, 2007.

COMER, D. **Interligação de redes com TCP/IP.** 6. ed. Rio de Janeiro: Elsevier, 2015.

COSTA, G. R. **Terceirização de Serviços de TI:** aspectos de segurança, 2010.

DENIS, T. S. **Cryptography for developers.** Massachusetts: Syngress Publishing, 2007.

EDWARDS, V. J. **Source selection answer book**. Los Angeles: Management Concepts Inc, 2000.

FARIA, F. **Qual é o melhor momento para o outsourcing de TI nas organizações?** In: Albertin, A.L.; Sanchez, O. P. (Orgs). Outsourcing de TI: impactos, dilemas, discussões e casos reais. Rio de Janeiro: FGV, p. 10-26, 2008.

FERREIRA, F. N. F.; ARAÚJO, M. T. **Política de Segurança da Informação:** guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna Ltda., 2008.

FONTES, E. L. G L, **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2010.

GEUS, P. L. de; NAKAMURA, E. T. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Novatec, 2007.

GRIFFITHS, P. D. R; REMENYI, D. **The burning question in ICT:** what and how should we outsource? In: Albertin, A.L.; Sanchez, O. P. (Orgs). Outsourcing de TI: impactos, dilemas, discussões e casos reais. Rio de Janeiro: FGV, p. 61-74, 2008.

HILES, A. **Business continuity management:** global best practices. 4. ed. New York: Rothstein Publishing, 2014.

LAUDON, C. L; LAUDON. P. J. **Sistemas de informação gerenciais:** Administrando a empresa digital. São Paulo: Pearson Prentice Hall, 2004.

LINO, S. S. **Virtual private network: aprenda a construir redes privadas virtuais em plataformas linux e windows.** São Paulo: Novatec, 2002.

MEIRELLES, F. S, **Préfacio** In: Albertin, A.L.; Sanchez, O. P. (Orgs). Outsourcing de TI: impactos, dilemas, discussões e casos reais. Rio de Janeiro: FGV, p. 7-8, 2008.

MITCHELL, W. J. **A lógica da arquitetura:** projeto, computação e cognição. São Paulo: Unicamp, 2008.

NICASTRO, M. F. **Security patch management.** 2. ed. Florida: Taylor & Francis Group, 2011.

PRADO, E. P. V.; TAKAOKA, H. **A terceirização da tecnologia de informação e o perfil das organizações.** São Paulo: Revista de Administração da Universidade de São Paulo, 2006.

RIFKIN, J. **O fim dos empregos:** o declínio inevitável dos níveis dos empregos e a redução da força global de trabalho; trad. Ruth Gabriela Bahr. São Paulo: MAKRON Books do Brasil, 1996.

SAAD, A. C. **Terceirização de Serviços de TI.** Rio de Janeiro: Brasport, 2006.SÊMOLA, M.. **Gestão da segurança da informação:** uma visão executiva**.** Rio de Janeiro: Elsevier, 2003.

STEWART, J. M. **Network security, firewalls and VPNs.** 2. ed. Massachusetts: Jones And Bartlett Publishers, 2014.

TORRES, N. A. **Seleção de provedores e contratos.** In: Albertin, A.L.; Sanchez, O. P. (Orgs). Outsourcing de TI: impactos, dilemas, discussões e casos reais. Rio de Janeiro: FGV, p. 111-134, 2008.

VIDAL, A. G.. **Terceirização:** a arma empresarial. São Paulo: Erica, 1993.

YOUNG, C. S. **The science and technology of counterterrorism:** measuring physical and electronic security risk. Massachusetts: Elsevier, 2015.