A GESTÃO DE RISCOS NA SEGURANÇA DA INFORMAÇÃO E OSPOSSÍVEIS IMPACTOS DA CONSUMERIZAÇÃO NO GRUPO CORDEIRO ALVES, EMPRESA DO SEGMENTO FARMACÊUTICO EM FEIRA DE SANTANA- BA

Hadarlenne Morais da Cruz[1]
Prof. Orientador: Kleverton MoisésSilva (FAT)[2]

RESUMO: A informação tornou-se o principal ativo das organi zações. Portanto, éimprescindível que seja adequadamente protegida. Ela é fator determinante para o poder decisório dos gestores, para garantir a continuidad e dos negócios e para maximizar o retorno sobre os investimentos. O presente artigo buscou mapear através da gestão de riscos, por meio de técnicas do método ISRAM, as possíveis ameaças que a consumerização poderá ocasionar para a Segurança da Informação (SI) para uma empres a situada em Feira de Santana, bem como propor soluções em SI para minimizar os riscos descritos. Através da análise dos riscos torna-se possível estabelecer escala de priorização para o tratamento dos mesmos.

Palavras-chave: Segurança da Informação. BYOD. Gestão de Riscos. IS RAM. Consumerização.

RISK MANAGEMENT IN INFORMATION SECURITY AND POSSIBLE IMPACTS OF THE CONSUMERIZATION IN THE CORDEIRO ALVES GROUP, A PHARMACEUTICAL COMPANY SEGMENT IN FEIRA DE SANTANA - BA

ABSTRACT: The information has become the main asset of organizations. Therefore, it isessential that it is properly protected. It is a determining factor in the decision-making power of managers, to ensure business continuity and to maximize return on investments. This paper aims to map through risk management, through ISRAM method techniques, possible threats that the consumerization could lead to Information Security (IS) for a company located in Feira de Santana and propose solutions in SI to minimize the risks described. Through risk analysis becomes possible to establish prioritization scale for the treatment thereof.

Keywords: Information Security. BYOD. Risk Management. ISRAM. Consumerization.

1. INTRODUÇÃO

A partir da década de 1990 ocorreram profundas mudanças na sociedade, sobretudo na comunicação pessoal e no ambiente corporativo. D evido à crescente popularização dos computadores pessoais e dispositivos móveis, vi venciamos a era da informação, na qual as pessoas estão constantemente conectadas. Consequ entemente, a informação tornou-se o principal ativo em uma organização.

---

[1] Graduanda em Tecnologia em Redes de Computadores - Faculdade Anísio Teixeira (FAT).
[2] Professor especialista em Gerência de Projetos emTI.

A informação transformou-se em parte estratégica do negócio. Para protegê-la, é perceptível para os gestores do setor de Tecnologia da Informação e Comunicação (TIC) a necessidade da adoção da Segurança da Informação (S I), utilizando-se de técnicas de Gestão de Riscos, possibilitando a minimização dos mesmos.

Com o passar dos anos e a evolução tecnológica, a f orma de trabalho mudou. Diversos colaboradores já utilizam recursos pessoais como dispositivos móveis nas empresas, obrigando ao setor de TIC a se adequar às novas práticas como a Consumerização e o BYOD, este último caracteriza-se pela adoção de dispositi vos móveis pessoais como *Smartphones*, *notebooks* e *tablets* também para fins corporativos.

Segundo Sêmola (2003), mudanças interferem nos riscos operacionais do negócio. Assim, a adoção de dispositivos móveis pessoais tra z desafios ao setor de TIC das organizações. Isso porque a TIC não possui controle sobre tais equipamentos, podendo potencializar os riscos à segurança dos dados da or ganização. Percebe-se então, que há uma crescente necessidade de avaliar as ameaças e vulne rabilidades decorrentes de mudanças, bem como identificar e avaliar os riscos nos processos de negócio.

O presente artigo busca mapear através de uma pesquisa a atual situação do grupo Cordeiro Alves em relação à Segurança da Informação utilizando técnicas de Gestão de Riscos, permitindo a mensuração dos possíveis im pactos e ameaças que a prática da consumerização poderá ocasionar.

O grupo Cordeiro Alves está, aproximadamente, há 14anos no mercado, atuando na área farmacêutica onde sua principal atividade édistribuiçãoa de medicamentos. O grupo é composto por quatro empresas sendo elas Vilfarma, Methafarma, Genfarma e Tinafarma além de duas farmácias que são denominadas Farmácia Dinâmica sendo uma matriz e a outra filial.
O seu setor de TIC é composto por um funcionário responsável, o qual conta com o apoio de uma empresa especializada nesta área, que o ajuda no gerenciamento de toda infraestrutura de TIC da organização.

O presente trabalho é composto por 4 seções, a seçã o 1 é esta introdução, a seção 2 apresenta o referencial teórico que aborda os conce itos de SI, Gestão de Riscos e consumerização e seus possíveis impactos na SI que são fundamentais para a compreensão da Análise de Riscos. A seção 3 demonstra a metodologia utilizada para a análise dos riscos de SI no grupo Cordeiro Alves e os resultados obtidos. E por fim, a seção 4 trata das considerações finais sobre o trabalho acadêmico apresentado.

Torna-se indispensável salientar que este trabalhonão possui a pretensão de delimitar todas as etapas da Gestão de Riscos, restringindo-s e apenas a mapear alguns ativos e suas

variáveis de forma a demonstrar a importância da SIpara a continuidade dos negócios do grupo Cordeiro Alves.

2. REFERENCIAL TEÓRICO

2.1 Segurança da Informação

O cenário corporativo vem sofrendo grandes mudanças, no qual a informação tornou-se uma das principais vantagens competitivas das organizações. Isto se deve ao fato dela agregar valor às empresas e ser uma das causas da c ontinuidade do negócio. Além disto, a informação é o principal fator que influencia no poder decisório dos gestores. Consequentemente, as empresas estão cada vez mais d ependentes desse ativo, obrigando a TIC estar continuamente alinhada aos objetivos estratégicos do negócio.

Compreende-se como informação um conjunto de dados ordenados logicamente de forma que tenham um significado. Ela é vital para que os processos de negócio funcionem corretamente, portanto deve ser adequadamente protegida.

Para que haja a devida proteção da informação, é ne cessária a utilização de técnicas de segurança da informação a qual pode ser definida como um conjunto de políticas, padrões e processos que tem a finalidade de proteger o principal ativo das organizações. Classifica-se como ativo tudo que tem valor para os processos de negócios da organização (ABNT. NBR ISO/IEC 27001, 2006). Para Jucá (2011, p.26) Segurança da Informação "é a proteção de informações de uma ampla gama de ameaças para ga rantir a continuidade dos negócios, minimizar os riscos de negócios e maximizar o retor no sobre investimentos e oportunidades de negócios". A NBR ISO/IEC 27001 (ABNT, 2006) acre scenta que a SI deve prover métodos para proporcionar a preservação dos pilares da segurança da informação, são eles: a confidencialidade, a integridade e a disponibilidade.

A confidencialidade é o atributo que visa assegurarque informações armazenadas ou transmitidas devem estar disponíveis somente para usuários autorizados. Sêmola (2014) informa que conservar a confidencialidade, consiste em manter a informação protegida tendo em vista o grau de sigilo de seu conteúdo, para que seu acesso e uso sejam limitados apenas às pessoas autorizadas. Integridade é o atributo que sinaliza a equivalência das informações armazenadas com as transmitidas, ou ainda, garante que a manipulação (alteração, exclusão e inserção) dos dados realizada por um usuário autorizado terá conformidade com os dados que chegarão ao receptor. A disponibilidade atesta que as informações estarão acessíveis aos processos e usuários autorizados sempre que for requisitada.

Adicionalmente, outras quatro propriedades: autenticidade, legalidade, não-repúdio e auditabilidade podem contribuir para a segurança. A autenticidade atesta que a fonte das informações é verídica. A legalidade certifica que o sistema estará em conformidade com a legislação vigente no país. O não-repúdio é a propriedade que assegura que a fonte das informações não negará a sua autoria. A auditabilid ade permite que as informações possam ser auditadas, ou seja, permite a identificação da entidade e rastreamento das manipulações realizadas nas informações.

À medida que ocorrem mudanças nos processos, surgem novos riscos a segurança da informação. A crescente necessidade de interconecti vidade expõe as informações a diversas ameaças. Estas podem explorar as vulnerabilidades g erando impacto para as instituições. A Associação Brasileira de Normas Técnicas (ABNT) salienta que:

> Ativos são objetos de ameaças, tanto acidentais qua nto deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes. Mudanças nos processos e sistemas do negócio ou out ras mudanças externas (tais como novas leis e regulamentações), podem cri ar novos riscos de segurança da informação. Desta forma, em função das várias maneiras nas quais as ameaças podem se aproveitarem das vulnerab ilidades para causar dano à organização, os riscos de segurança da infor mação estão sempre presentes. Uma segurança da informação eficaz reduz estes risco a organização das ameaças e vulnerabilidades e, ass im, reduzin aos seus ativos. (ABNT. NBR ISO/IEC 27002:2013, p.04).

Ameaças são eventos que podem comprometer a confide ncialidade, integridade e disponibilidade. Para Sêmola (2014), as ameaças podem ser organizadas em três grupos ao levar em consideração a sua intencionalidade: natur ais, involuntárias e voluntárias. As ameaças naturais que são derivadas de fenômenos da natureza, tais como terremotos, enchentes, maremotos, entre outros. As involuntárias são quase sempre causadas por acidentes, falta de conhecimento, etc. e sem a consciência que são ameaças. As voluntárias são ameaças propositais geralmente causadas por hum anos.

Sêmola (2014) considera vulnerabilidades, as fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações que ao serem exploradas por ameaças, permitem a ocorrência de um incidente que comprometa um ou mais dos princípios básicos da segurança da informação.

Sêmola (2014, p.48) informa que risco é a "probab**i**ldade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade". A NBR ISO/IEC 27005 (ABNT, 2008, p.01) reitera ainda que riscos de segurança da informação é "a possibilidade de uma determinada am eaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos". Compreende-se e ntão que risco é a possibilidade da

concretização de um incidente por meio de ações que explorem as vulnerabilidades. Para minimizá-los, são definidos controles, os quais são métodos de proteção implementados com a finalidade de minimizar os riscos.

O impacto ao qual a NBR 27002 da ABNT refere-se pode ser conceituado como a abrangência das consequências ocasionadas por um cidentein. A NBR ISO/IEC 27005 (ABNT, 2008, p.01) define impacto como "mudança adv ersa no nível obtido dos objetivos de negócio".

Tendo como referência o que foi apresentado, perceb-se a importância de gerir e metrificar os riscos por meio de técnicas de gestão de riscos, para que desta forma seja possível definir o nível ideal de proteção a ser ap licado em cada ativo de acordo com o grau de impacto ocasionado pela sua indisponibilidade. Além disso, permite criar políticas de segurança mais eficientes e eficazes.

2.2 Gestão de riscos de tecnologia da informação e comunicação

O mundo está cada vez mais complexo e os avanços tecnológicos geram incertezas, provocando um crescente interesse das organizações em avaliar os riscos. Esta prática possibilita a tomada de decisões de forma estrutura da possibilitando priorizar aspectos críticos.

Em TIC, gestão de riscos pode ser caracterizada com o o processo de gerir os riscos de forma a identificá-los, avaliá-los e prover me**d**asi que o reduzam a um nível aceitável para a organização. Há alguns métodos que podem auxiliar os gestores neste processo como o ISRAM (*Information Security Risk Analysis Method*) que é amplamente utilizado em SI.

De acordo com a NBR ISO/IEC 27005, a gestão de risc os consiste em algumas etapas principais: Definição do Contexto, Análise/Avaliaçã o de riscos, Tratamento do risco, Aceitação do risco, Comunicação do risco e Monitora mento e Análise Crítica de riscos. É importante salientar que este processo é contínuo e interativo, pois mudanças podem gerar novos riscos.

Na etapa de Definição do Contexto são definidos os parâmetros básicos que são os critérios de avaliação de riscos, critérios de impacto e critérios de aceitação do risco. Também são definidos o escopo e os limites da gestão de ri scos, bem como o estabelecimento de uma organização para operar a gestão de riscos de SI.

Na fase de Análise/Avaliação, os riscos serão identificados, quantificados ou descritos qualitativamente e priorizados. Possibilitando assim aos gestores a tomada de decisão (tratar

ou não o risco) a partir do entendimento do mesmo, tendo sempre em vista os objetivos de negócio da organização.

No estágio de Tratamento do risco, tendo como referência a Análise/Avaliação, convém que os riscos estejam ordenados por prioridade e sejam selecionados controles para reduzir, reter, evitar ou transferi-los. Nessa etapa é estabelecido um plano de tratamento dos riscos.

Para o ciclo de Aceitação do risco, pode-se definir que este processo está sujeito a decisão dos gestores da empresa relativo ao risco r esidual do tratamento de riscos e deve ser devidamente documentado e justificado, caso haja necessidade. Para que os critérios referentes a aceitação sejam atendidos eles devem e star em conformidade com o plano de tratamento.

No passo de Comunicação do risco tem-se como objeti vo desta atividade chegar a um consenso sobre a forma a qual os riscos serão geren ciados. Para que isso aconteça é importante que os gestores e os outros interessados (*stakeholders*) estejam cientes das decisões tomadas e dos motivos que as tornaram nece ssárias.

A etapa de Monitoramento e análise crítica do risco é imprescindível, visto que mudanças podem gerar novos riscos ou atenuar os exi stentes, por isso convém que os riscos sejam constantemente monitorados e analisados criticamente de forma que qualquer mudança no valor dos riscos seja detectada em tempo hábil.

Figura 1 - Fases da Gestão de Riscos da SI Fonte: NBR ISO/IEC 27005

Conforme mostrado na Figura 1, a gestão de risco de SI é um processo interativo que permite e deve ser constantemente monitorado e avaliado. Este processo possibilita que algumas etapas sejam realizadas mais de uma vez o que torna a gestão mais eficaz.

O ISRAM é um dos métodos para análises de riscos deSI. Segundo Amaral (2011) este método define o risco baseando-se em um questionário relacionado com problemas de segurança. Posteriormente realiza-se o cálculo de índice dos riscos através da formula: risco é igual a probabilidade de ocorrer uma quebra de segurança multiplicada pela consequência da ocorrência da quebra de segurança. Estas duas varáveis têm como valor máximo 5, assim o produto final tem valor máximo 25. Desta forma, para obter resultado percentual, é aplicada uma regra de três simples, considerando que o valormáximo é 100%. Assim, a seguinte fórmula é obtida: ISRAM = ((P*I)*100)/25. Onde "P" refere-se à probabilidade e "I" faz referência ao impacto ou consequência da ocorrênciade quebra de segurança.

O ISRAM segue as diretivas propostas pela NBR ISO/IEC 27005 sendo suas etapas as listadas abaixo conforme definido por Amaral (2011):

1. Identificar os problemas de segurança que envolvem a organização em estudo;
2. Listar todos os fatores que podem influenciar a ocorrência de uma quebra de segurança;
3. Elaborar um questionário com base nos fatores identificados na fase anterior;
4. Elaborar a tabela de conversão das respostas obtida s em função de valores quantitativos e qualitativos para a probabilidade de ocorrer uma quebra de segurança e para as consequências de uma quebra desegurança;
5. Aplicação dos questionários utilizadores;
6. Cálculo do índice do risco;
7. Análise dos resultados com o intuito de tentar apontar medidas que corrijam o problema de segurança. (AMARAL, 2011, p.29)

O ISRAM trata-se de um método basicamente quantitativo o qual utiliza uma escala com valores numéricos representados em uma escala de 1 a 5 para classificar as métricas e assim obter o índice dos riscos.

2.3 Consumerização e os possíveis impactos na segur ança da informação

A crescente utilização de dispositivos eletrônicos como computadores, *notebooks,tablets* e *smartphones* em instituições, a necessidade de mobilidade e de c ompartilhamentode informações em tempo real e a facilidade que os dispositivos apresentam no seu uso trouxe um novo conceito para o setor de TIC, a consumerização de TI (CoTI). No entanto, este conceito traz ameaças à segurança da informaçã o das empresas.

Silva e Maçada (2012) informam que a CoTI pode ser definida como a utilização de recursos pessoais de tecnologia da informação com f inalidade de trabalho. Aliada a esta

definição tem-se o conceito de BYOD (*Bring Your Own Device*), este trata-se da utilização dos dispositivos móveis pessoais para fins de traba lho. Percebe-se assim que o BYOD é parte da CoTI.

A busca das empresas principalmente por produtividade e redução de custos tem impulsionado esse processo, visto que os dispositivos são de propriedade dos colaboradores. No entanto, a utilização desses dispositivos pode g erar riscos à SI ou atenuar os já existentes, pois o setor de TIC não tem controle sobre os mesmo s.

Segundo Cunha e Castro (2014) são oferecidas divers as vantagens com a implantação dos conceitos citados acima, alguns podem ser mencionados como: a flexibilidade, pois há alternância entre a vida pessoal e a corporativa e os colaboradores valorizam isto; satisfação do funcionário já que eles poderão escolher com quais ferramentas trabalhar; maior produtividade porque o uso do aparelho não está restrito apenas ao ambiente da empresa; e redução de custos para a organização, pois os própr ios colaboradores investem na tecnologia que irão utilizar.

Entretanto, podem ser abordados alguns desafios para a implantação como a utilização do dispositivo por pessoas que não fazem parte do q uadro de funcionários da empresa e consequente acesso à informação sem a devida autori zação; risco de perda ou roubo do dispositivo o que pode comprometer a vantagem competitiva da empresa devido a perda de propriedade intelectual; diversidade dos Sistemas Operacionais e *hardware* nos dispositivos móveis clientes, dificultando a manutenção dos sist emas que a empresa utiliza; ameaças de infecções causadas por vírus; entre outras questões .

3. METODOLOGIA

O presente artigo trata-se de um estudo de caso, uma vez que foram realizadas as análises dos riscos e possíveis impactos que a consumerização ocasiona na Segurança da Informação em uma empresa de Feira de Santana. N este sentido foi efetuado um questionário com gestor de TI do grupo Cordeiro Alves conforme apêndice A. Após a aplicação do questionário, foi possível definir os principais ativos, as prováveis ameaças e vulnerabilidades utilizando as técnicas do método SRAMI (descrito na sessão 2.2), com o intuito de mensurar o grau de impacto ocasionado pela indisponibilidade de alguns destes ativos.

3.1 Análise dos dados

Atuante na área farmacêutica, o grupo Cordeiro Alves dispõe de pouco mais de 120 funcionários e aproximadamente 52 prestadores de serviço que trabalham interna e externamente, possuindo uma ampla estrutura de TIC. Este setor conta com um colaborador que é responsável pelas demandas de tecnologia do rupog e recebe apoio especializado de uma empresa de suporte técnico para o gerenciamento da infraestrutura de TIC. Além disto, possui contrato de suporte com uma organizaç ão especializada em monitoramento de banco de dados.

No que discerne à estrutura de TIC, a empresa utili za um software que tem as funcionalidades de *proxy* e *firewall*, possui redundância de *links* de internet, adota virtualização de servidores, possui antivírus corpo rativo, política implementada para acessos externos (tanto acesso físico de pessoas à empresa quanto acesso à estrutura lógica), servidor de contingência, políticas de níveis de acesso comatenção especial aos colaboradores que acessam externamente à rede da instituição e políti ca de *backup*.

No entanto, alguns processos necessitam ser revistos, pois não há política de SI aprovada pela direção, documentada, publicada e com unicada de forma que todos os colaboradores tenham consciência da sua responsabilidade por ela. Não há treinamentos para os colaboradores que utilizam computação móvel com a finalidade de aumentar o nível de conscientização dos mesmos a respeito dos riscos ad icionais resultantes desta forma de trabalho. Os testes de recuperação de *backup* (*restore*) não é implementado e a comunicação do setor pessoal com o de TIC para a informação dos colaboradores contratados ou desligados não tem sido eficiente.

A partir desta análise de contexto, foi aplicado ométodo ISRAM para que fosse possível analisar alguns dos riscos referente à SI, sendo que as métricas adotadas para os cálculos podem ser visualizadas nos quadros 1, 2 e3, contidos no apêndice B.

Ao se verificar o quadro 4, contido no apêndice B,observa-se que para o ativo banco de dados, tem-se a ameaça de corrupção de dados; pa ra o ativo processos, tem-se o uso não autorizado de informações; para os ativos humanos, observa-se o vazamento de informações; para o *backup* das informações, tem-se a impossibilidade da restau ração da base de dados; para o servidor de aplicação, tem-se a falha de *hardware* por falta de refrigeração adequada e por fim, para os dispositivos móveis dos colabora dores que tem acesso a aplicação, verifica-se a ameaça de acesso indevido.

Para os ativos descritos foi efetuado o cálculo do risco e o resultado pode ser observado na coluna Risco do quadro 4, que pode ser observado no apêndice B. Portanto,

tem-se o gráfico 1 a seguir, demonstrando em valores percentuais o nível do risco à cada ativo:

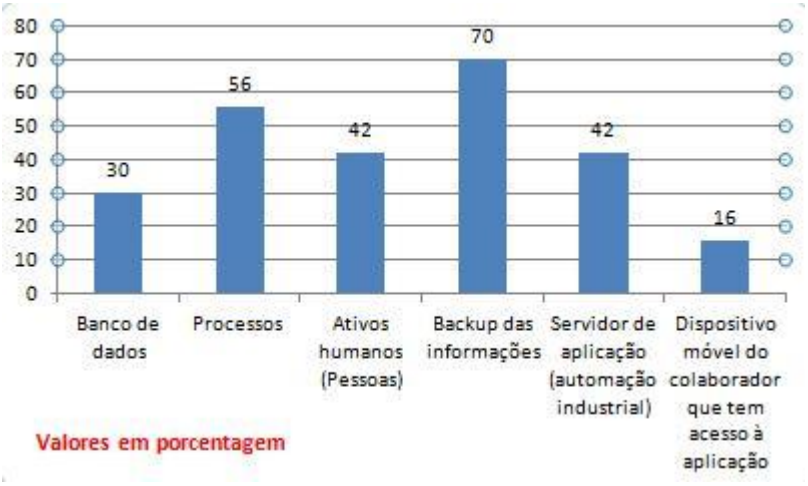

Gráfico 1 - Percentual de riscos para os ativos
Fonte: Autoria própria

Assim, percebe-se que o ativo mais vulnerável no momento é o *backup* das informações, apresentando um percentual de 70% de r isco de concretização da ameaça; depois tem-se os processos, com 56%; ativos humanos e servidor de aplicação que ficaram com mesmo grau de riscos, 42%; e finalmente, tem-se os dispositivos móveis dos colaboradores com 16% de risco. Desta forma, observa-se que por possuir diversos controles, os incidentes relacionados à consumerização apresen ta-se para o grupo Cordeiro Alves com menor risco de ocorrência que os outros ativos citados anteriormente.

Tendo como ponto de análise o que foi apresentado, comprova-se que a consumerização pode facilitar vulnerabilidades que possivelmente culminarão em precipitar ameaças, entretanto se alguns controles estiverem i mplementados isto pode ser minimizado. É essencial destacar que os riscos devem ser comuni cados ao tomador de decisão da organização e aos gestores e convém que eles definam o que será feito com o risco (se será tratado ou aceito, por exemplo) tendo como referência a análise/avaliação de riscos realizada.

Como sugestão para atenuar os riscos identificados pode-se citar a implantação de uma política de segurança da informação que considere a lguns aspectos, tais como a consumerização e a responsabilidade dos colaborador es pela SI; determinação de um cronograma para efetuar testes de *restore* do *backup*; definir cronograma de treinamento sobre SI para os funcionários. Desta maneira, poderá serminorada as chances de haver vazamento de informações; reestruturar o processo de comunica ção entre o setor pessoal e o de TIC, de forma que este último seja avisado em tempo hábil arespeito da contratação ou desligamento de trabalhadores; projetar a aquisição de um equipa mento de contingência para refrigeração

da sala onde ficam os servidores, isto para que sejam evitadas falhas de *hardware* por superaquecimento. Em relação à utilização dos dispo sitivos móveis, prevenções adicionais podem ser implementadas como inclusão de cláusulasespeciais no contrato de trabalho que contemplem aspectos da consumerização e elaborar um a breve cartilha de boas práticas na utilização de dispositivos móveis.

4. CONSIDERAÇÕES FINAIS

Manter a informação protegida é essencial para a continuidade dos negócios. Assim, é imprescindível que a TIC esteja alinhada com os objetivos estratégicos do negócio provendo meios de minimização dos riscos, aplicando ações pr eventivas e corretivas.

Com a evolução tecnológica, novas práticas em ambie nte corporativo tem sido adotada, tendo como destaque a consumerização. Apes ar de trazer diversos benefícios, ela pode também acentuar os riscos à Segurança da Infor mação.

Desta forma, é perceptível a necessidade de avaliar os riscos, pois permite a alta gerência tomar decisões priorizando ações que estej am de acordo com a necessidade da empresa. Salienta-se que a gestão de riscos é um processo contínuo e deve, periodicamente, ser reavaliado. A utilização de técnicas de gestão de riscos poderá reduzir consideravelmente as ameaças à SI.

Apesar de se apresentar como uma prática que proporciona a incidência de vulnerabilidades, a consumerização ao contrário do que se pressupunha, não é o principal fator de risco para o grupo Cordeiro Alves, conforme observado no gráfico 1 (sessão 3.1). Isto deve-se ao fato de a organização possuir diversos c ontroles implementados.

Assim, a utilização das técnicas de gestão de risco s no grupo Cordeiro Alves possibilitou a verificação dos seus ativos críticos , no que discerne a SI, para que sejam priorizados e possam ser implementados controles de forma que os riscos sejam reduzidos. Recomenda-se que após o tratamento dos riscos seja realizada outra análise de riscos para que seja possível comparar os resultados.

5. REFERÊ NCIAS

AMARAL, Marisa Muneratto. **Metodologia para Análise e Avaliação de Riscos por Composição de Métodos.** Santa Maria, 2011. Disponível em: <http://cascavel.cpd.ufsm.br /tede/tde_arquivos/31/TDE-2011-10-26T142647Z-3290/Publico/AMARAL,%20MARISA %20MUNARETTO.pdf>. Acesso em: 09 out. 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:** Tecnologia da informação - Técnicas de segurança - Gestão de r iscos de segurança da informação. Rio de Janeiro: ABNT, 2008.

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

___. **NBR ISO/IEC 27002:** Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. R io de Janeiro: ABNT, 2013.

CUNHA, I. K. B.; CASTRO, R. C. C. **Uma análise holística dos riscos da adesão do BYOD dentro do ambiente corporativo.** Canindé, 2014. Disponível em: <http://redes.caninde.ifce.edu.br/images/artigos/16.pdf>. Acesso em: 25 out. 2014.

JUCÁ, Kathia Regina Lemos. **Gestão da Segurança de Informação e comunicação Orientada à Percepção do Risco de TI:** Um Estudo de Caso em uma Instituição de EnsinoSuperior. Brasília, 2011. Disponível em: <https://dsic.planalto.gov.br/documentos/ cegsic/ monografias_2009_2011/40_Kathia.pdf>. Acesso em: 08 out. 2014

SÊMOLA, Marcos. **Gestão da Segurança da Informação** : uma visão executiva. Rio de Janeiro: Elsevier, 2003.

SÊMOLA, Marcos. **Gestão da Segurança da Informação** : uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SILVA, Sidney Roberto Feliciano da; MAÇADA, Antônio Carlos Gastaud. **Consumerização de TI e seus Efeitos no Desempenho e na Governança de TI.** *In:*Revista de Administração eNegócios da Amazônia, v. 4, n. 3, p. 254-269, 2012. Disponível em: <http://www.periodicos .unir.br/index.php/rara/article/view/575/625>. Acesso em: 25 out. 2014.

APÊNDICE A - Questionário para avaliação do context o de Segurança da Informação o qual a organização encontra-se inserida.

QUESTIONÁRI O

Questionário a ser aplicado no setor de Tecnologiada Informação e Comunicação (TIC) do grupo Cordeiro Alves com a finalidade de mapear os possíveis riscos à Segurança da Informação da empresa.

1- Você sabe o que é consumerização?

( ) SIM (X) NÃO

2- O setor de TIC possui alguma medida para o caso de haver algum incidente relacionado à consumerização?

(X) SIM ( ) NÃO

3- Há treinamentos para os colaboradores que utilizam a computação móvel, com a finalidade de aumentar o nível de conscientização a respeito dos riscos adicionais resultantes desta forma de trabalho?

( ) SIM (X) NÃO

4- Há política de Segurança da Informação (SI) apro vada pela direção, documentada, publicada e comunicada a todos os colaboradores?

( ) SIM (X) NÃO

5- O manual de normas e procedimentos determina as responsabilidades dos funcionários pela SI?

( ) SIM (X) NÃO ( ) Não disponibiliza o manual

6- Alguma política formal é adotada levando em conta os riscos de trabalhar com recursos de computação móvel?

(X) SIM ( ) NÃO

7- É implementada auditoria através de logs (Registro de Eventos) para os sistemas de informação da organização?

(X)
SIM ( ) NÃO

8- Há contrato formal que defina os requisitos SI para prestadores de serviços, quando a organização terceiriza algum ativo de sistema de informação?

(X)
SIM ( ) NÃO

9- Há inventário ou registro dos ativos de informação importantes relacionados com cada sistema de informação?

( ) SIM (X) NÃO

10- Há esquema ou diretriz de classificação da informação (levando em consideração o grau de impacto gerado pela sua indisponibilidade)?

(X) SIM ( ) NÃO Obs.: Não é documentado

11- Há política ou controle para acessos externos de forma a assegurar que apenas pessoas autorizadas acessem a rede da empresa (*firewall*, ferramentas de detecção de intrusão, autenticação para conexões externas)?

(X) SIM ( ) NÃO CITE UMA: Winconnect ion

12- Há controles implementados (Antivírus corporativo, controle de internet)?

(X) SIM ( ) NÃO

13 - A empresa possui proteção criptográfica para redes Wi-Fi? Se sim, qual?

(X) SIM ( ) NÃO

( ) WEP ( )WPA (X)WPA2

( )Outra: 14- A internet é _____ liberada ou há bloqueio?

(X)
( )Liberada Bloqueada

15- Os fornecedores acessam estrutura física da empresa sem identificação?

(X)
( ) SIM NÃO

16- Há adequações contra incêndio?

(X)
( ) SIM NÃO

17- A empresa disponibiliza acesso remoto através da internet aos

colaboradores

e/ou
fornecedores?

( )
(X) SIM NÃO

18- Há política de níveis de acesso?

( )
(X) SIM NÃO

19- Há política de*backup*?

( )
(X) SIM NÃO

20- A sala onde ficam os servidores possui *backup* de refrigeração?

(X)
( ) SIM NÃO

21- Há copias do*backup* armazenadas fora da empresa (Caso haja *backup*)?

(X) SIM ( ) NÃO

22- Há testes de*Restore* do *backup*?

(X)
( ) SIM NÃO

23- Possui servidor de contingência para o caso deo principal falhar?

(X)
SIM ( ) NÃO

24- Há*link* de internet redundante?
(X)
SIM ( ) NÃO

25- Utiliza virtualização?
(X)
SIM ( ) NÃO

26- Utiliza *softwares* licenciados?
(X)
SIM ( ) NÃO

27- Utiliza *no-breaks* para os ativos críticos?
(X)
SIM ( ) NÃO

28 - O local onde ficam instalados os servidores émonitorado com sistema de

câmeras?
(X)
SIM ( ) NÃO

29- Existe política de restrição de acesso físico a o local onde ficam os servidores?

(X) ( ) NÃO

SIM

30- Caso haja furto do dispositivo móvel há algum mecanismo que proteja as informações da empresa?

(X) SIM ( ) NÃO

31- O setor pessoal comunica em tempo hábil ao setor de TIC o desligamento ou férias dos funcionários?

( ) SIM (X) NÃO

APÊNDICE B - Análise dos riscos de Segurança da Informação.

Métrica para calcular a PROBABILIDADE		
Estimativa	**Descrição**	**Indicadores (histórico)**
Muito Alta (Muito provável,5)	Pode ocorrer todos os anos ou com possibilidade igual ou superior a 50%.	Já ocorreu algumas vezes dentro de um período de tempo, e tem grande chance de ocorrer várias vezes, dentro de um período de tempo.
Alta (Provável, 4)	Pode ocorrer todos os anos ou com possibilidade superior a 25% e menor que 50%.	Grande chance de ocorrer várias vezes dentro de um período de tempo.
Média (Possível, 3)	Pode ocorrer a cada 2 anos ou com possibilidade inferior a 25%.	Pode ocorrer mais do que uma vez dentro do período de tempo. Pode ser difícil de controlar devido a algumas influências externas.
Baixa (Remota, 2)	Não existe a possibilidade de ocorrer a cada 2 anos ou com possibilidade inferior a 5%.	Não ocorreu, mas é possível que ocorra
Muito Baixa (Muito remota, 1)	Não existe a possibilidade de ocorrer a cada 4 anos ou com possibilidade inferior a 2%.	Não ocorreu, e é improvável que ocorra.

Quadro 1 - Métricas para o cálculo da probabilidade
Fonte: Autoria própria

Métrica para calcular o IMPACTO	
Estimativa	**Descrição**
Muito Alta (Muito provável,5)	1.O impacto financeiro sobre a organização ultrapassa um determinado valor. 2.Muita preocupação das partes interessadas.
Alta (Provável, 4)	1.O impacto financeiro sobre a organização ultrapassa um determinado valor. 2. Grande preocupação das partes interessadas.
Média (Possível, 3)	1.O impacto financeiro sobre a organização deve estar entre dois valores. 2. Preocupação moderada das partes interessadas.
Baixa (Remota, 2)	1.O impacto financeiro sobre a organização deve ser inferior a um valor. 2.Pouca preocupação das partes interessadas.
Muito Baixa (Muito remota, 1)	1.O impacto financeiro sobre a organização deve ser inferior a um valor. 2.Nenhuma preocupação das partes interessadas.

Quadro 2 - Métricas para o cálculo do Impacto
Fonte: Autoria própria

Análise dos Controles Existentes	
Estimativa	**Descrição**
1, 2 ou 3	Implantado e Eficaz
4	Implantado e não-eficaz
5	Não implantado

Quadro 3 - Métrica para a análise dos controles
Fonte: Autoria própria

ATIVOS	AMEAÇAS	CONTROLES		VULNERABILIDADES	HISTÓRICO	PROBABILIDADE	CONFI DENCI ALIDA DE	DISPONIBILI DADE	INTEGRIDADE	IMPACTO		RISCO	
		Descrição	Valor							Valor		Valores em percentual (%)	
Banco de dados	Corrupção de dados	Monitoramento da base de dados	1	Controle inadequado da base de dados	2	1,5	-	5	5	5	7,5	30	
Processos	Uso não autorizado de informações	Comunicação eficiente do setor de RH com o de TIC	5	Tempo elevado para realizar o bloqueio do login quando o funcionário é desligado.	2	3,5	4	-	4	4	14	56	
Ativos humanos (Pessoas)	Vazamento de Informações	Treinamento sobre SI para os colaboradores	5	Falta de treinamento dos colaboradores em relação a SI	2	3,5	3	-	-	3	10,5	42	
Backup das informações	Impossibilidade de restauração da base de dados	Testes periódicos de restore de backup	5	Falta de teste de restore do backup	2	3,5	-	5	5	5	17,5	70	
Servidor de aplicação (automação industrial)	Falha de hardware por falta de refrigeração adequada	Possuir mais de um equipamento de refrigeração (ar condicionado)	5	Falta de refrigeração de backup	2	3,5	-	3	-	3	10,5	42	
Dispositivo móvel do colaborador que tem acesso à aplicação	Acesso indevido (devido a furto do dispositivo ou utilização do dispositivo do colaborador por pessoas não empregadas na empresa, por exemplo.)	Controle de acesso (login e senha) para usuários que se conectam através de dispositivo móvel	2	Falta de monitoramento do dispositivo	2	2	2	-	2	2	4	16	

Quadro 4

- Análise de Riscos Fonte: Autoria própria