Associação Propagadora Esdeva
Centro de Ensino Superior de Juiz de Fora – CES/JF
Curso de Bacharelado Em Sistemas De Informação
Trabalho de Conclusão de Curso

CONTROLE E ACESSO SEGURO AOS SISTEMAS OPERACIONAIS EMPRESARIAIS

Jonas Henrique Ventura
Centro de Ensino Superior de Juiz de Fora, Juiz de Fora, MG

Daves Márcio Silva Martins
Centro de Ensino Superior de Juiz de Fora, Juiz de Fora, MG

ENGENHARIA DE SOFTWARE e SISTEMAS DE INFORMAÇÃO
Sistemas Operacionais e Rede de Computadores

RESUMO

É de fundamental importância que o Sistema de Informações, assim como todo o conjunto de normas e procedimentos voltado para a segurança da informação, possibilite à empresa a ter controle eficaz e permanente de seus dados, com agilidade e confiabilidade, para que a empresa possa acessar estes dados em tempo real e utilizar com segurança, fazendo assim, o bom uso para seu desenvolvimento e crescimento. O sistema de informações das empresas precisa ter segurança para que possam ser armazenados dados confidenciais sem que sofra de invasões e desvio de dados sigilosos, evitando que este fato traga á empresa perdas, financeira, judicial ou quanto a imagem que a empresa transmite a sociedade e seus colaboradores. Por esse motivo, as empresas desenvolvedoras de softwares trabalham em constante atualização desenvolvendo softwares que tem por finalidade impedir invasões e coletas de dados internos dos sistemas operacionais das empresas. Devido aos desafios empresariais em implantar o ambiente seguro para as informações nas empresas e a necessidade de se ter as políticas e normas de segurança que possibilite aplicações em funcionamento, hardware em produção e softwares eficientes, a contribuição deste trabalho será de apresentar normas de segurança da informação que garante a segurança de toda e qualquer informação da empresa, esteja ela em meios eletrônicos, em formato de texto, imagem, áudio ou qualquer outro meio pelo qual se possa armazenar e movimentar os dados nela contido, assim como suas especificações.

Palavras-chave: Sistema de Informações. Softwares de segurança. Segurança de dados, Segurança na TI.

ABSTRACT, RÉSUMÉ ou RESUMEN

It is of fundamental importance that the Information System, as well as all the set of rules and procedures focused on information security, enables the company to have effective and permanent control of its data, with agility and reliability, so that the company can access these data in real time and use safely, thus making good use

for their development and growth. The information system of companies must have security so that confidential data can be stored without being subject to invasion and diversion of confidential data, preventing this fact from bringing the company losses, financial, judicial or as the image that the company transmits society and your employees. For this reason, software companies are constantly updating software designed to prevent intrusions and internal data collection of companies' operating systems. Due to the business challenges of deploying a secure environment for information in companies and the need to have security policies and standards that allow running applications, production hardware and efficient software, the contribution of this work will be to present security standards information that guarantees the security of any information of the company, be it in electronic means, in text format, image, audio or any other means by which the data contained therein, as well as its specifications, can be stored and moved.

1 INTRODUÇÃO

Em virtude aos avanços no campo da tecnologia as empresas, independentemente de sua área de atuação, ramo ou segmentação estão mais inseridas no mundo digital. A tecnologia passou fazer parte de todo o processo produtivo, comercial e prestação de serviços, assim como pode fazer parte do cotidiano de seus clientes, GONÇALVES (1994). Este avanço tecnológico trouxe a modernidade, agilidade, competitividade e inovação, onde cada vez mais as empresa necessitam de estarem inseridas neste meio e fazendo o uso da tecnologia em todo o processo organizacional, encurtando distancias e tempo, com isto a tecnologia acabou trazendo para a empresa maior fragilidade, vulnerabilidade, risco de perda ou roubo de dados confidenciais, exposição e fraudes. Devido a estes fatores de risco e vulnerabilidade as empresas necessitam de um sistema de Informações confiável, para que sua coleta e permanência de dados e sigilo de informações sejam precisas e seguras, para atingir tal objetivo utilizam de softwares e procedimentos que possam contribuir na segurança de suas informações.

Neste artigo é apresentado procedimentos, métodos e softwares cuja finalidade é proteger a segurança dos dados das empresas, assim como sua utilização, e funcionalidade; serão apresentadas normas de segurança da informação que garante a segurança de toda e qualquer informação da empresa, assim como suas especificações.

2 SISTEMA OPERACIONAL

Um sistema de computação tem suas partes fundamentais constituídas por hardware e software. Sendo o hardware composto por diferentes circuitos

eletrônicos e componentes periféricos sejam eletro, óptico ou mecânicos, já os softwares são os programas destinados ao usuário do sistema e são utilizados para o meio a qual foram criados. Ou seja, para se formar um sistema de Informações é preciso de hardwares, os componentes físicos que formam a máquina e de softwares programas que colocam a máquina em operação e por onde serão coletados e armazenados dados. Os sistemas de Informações são elementos fundamentais para o funcionamento do sistema de computação. Assim como são necessário softwares que possibilite a funcionalidade do sistema de Informações e coleta de dados, também é de fundamental importância a utilização de softwares que cuide dos dados armazenados de tal forma que garanta a segurança e o sigilo das informações arquivadas, MAZIERO (2019).

Para um sistema de Informações a utilização de software de segurança de dados é de fundamental importância tanto para a empresa quando para seus clientes, REDAÇÃO (2019). O sistema de Informações deve possibilitar à empresa ter controle eficaz e permanente de seus dados, favorecendo o trabalho com agilidade e confiabilidade, para que a empresa possa acessar estes dados em tempo real e utilizar com segurança, fazendo assim o bom uso para seu desenvolvimento e crescimento; O sistema de Informações precisa ser seguro quanto à armazenagem e a confidencialidade das informações guardadas, assim como garantir que a empresa não sofra de invasões e desvio de dados sigilosos, para atingir tal objetivo as empresas utilizam software que atua de forma silenciosa garantindo a estabilidade do sistema e da não violação dos dados.

Inúmeras empresas desenvolvedoras de softwares de segurança trabalham em constante atualização desenvolvendo softwares que tem por finalidade impedir invasões e coletas de dados internos dos sistemas operacionais das empresas.

3 METODOLOGIA

A metodologia aplicada a este trabalho será de pesquisa bibliográfica, com a utilização de materiais publicados em livros, artigos, dissertações e teses e pesquisas junto a internet e terá caráter estudos descritivos, descrevendo características, e relações existentes entre softwares. Serão apresentadas normas de segurança da informação que garante a segurança de toda e qualquer informação da empresa, esteja ela em meios eletrônicos, em formato de texto,

imagem, áudio ou qualquer outro meio pelo qual se possa armazenar e movimentar os dados nela contido, assim como suas especificações.

4 SEGURANÇA DA INFORMAÇÃO

A informação é um importante patrimônio que a empresa possui na atualidade, e necessita ser cuidado e mantido em sigilo, sendo revelado apenas aos de interesse da empresa, (CHIAVENATO, 2008). As informações são construídas através de dados coletados, classificados, armazenados e relacionados formando assim o que é nomeado como informação.

Sobre os dados, CHIAVENATO, 2008, diz que:

> "dados são os elementos que servem de base para a formação de juízos ou para a resolução de problemas. Um dado é apenas um índice ou um registro. Em si mesmo, os dados têm pouco valor. Todavia, quando classificados, armazenados e relacionados entre si, os dados permitem a obtenção da informação. Assim, os dados isolados não são significativos e não constituem informação. Os Dados exigem processamento (classificação, armazenamento e relacionamento), para que possam ganhar significado e consequentemente informar. A Informação apresenta significado e intencionalidade, aspectos que a diferenciam do dado simples." CHIAVENATO (2008),

É com base em dados, transformados em informações que as empresas se apoiam para sua tomada de decisão, sendo assim de fundamental importância para a organização que tais informações sejam precisas e sigilosas uma vez que sua imprecisão pode causar a tomada de decisão errada trazendo à empresa prejuízo grandiosos e a ausência de sigilo, podendo dar para a concorrência a possibilidade de alavancar seu negócio utilizando informações valiosas que deveria ser de domínio privado. Desde o início do século, Rezende e Abreu já haviam destacado que a informação e o conhecimento seriam os diferenciais das empresas e dos profissionais que pretendesse destacar-se no mercado e manter a sua competitividade. REZENDE e ABREU (2000). É possível perceber que este fato não mudou, pelo contrário se torna cada vez mais imprescindível e não estão associadas apenas aos dados sigilosos da empresa, suas estratégias e tomadas de decisão, quando se trata de dados de clientes, se estes se tornam públicos ou de fácil acesso

a invasões podem causar danos aos clientes e consequentemente afetará a imagem da empresa trazendo danos, perda de clientes e possíveis processos judiciais para a empresa.

Atualmente as empresas necessitam de trabalhar com a comunicação em tempo real independente das distâncias, o armazenamento de dados na internet, transferências de arquivos confiáveis e confidenciais, passaram a fazer parte do cotidiano diário das organizações deixando-as vulneráveis frente a possíveis ataques de softwares mal-intencionados ou até mesmo profissionais que atuam em busca de informações restritas. O que obriga que cada vez mais as empresas se equipem com softwares de segurança de dados. Como destaca LAUREANO (2005) frente à atualidade:

> “Com a dependência do negócio aos sistemas de informação e o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.” (Laureano 2005, pag. 11).

Para se ter a segurança da informação é preciso que a empresa atue com políticas, processos e métodos que poderão ser utilizados para que a circulação de dados, assim como suas informações tenha segurança e controle, o que evitará o roubo e utilização das informações por pessoas não autorizadas

5 OS PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Benevento (2012), publicou em seu blog: mauriliobenevento.wordpress.com, que existem cinco princípios básicos que representa a segurança da informação que são:

CONFIDENCIALIDADE

Acesso apenas por pessoas atualizadas e devidamente credenciadas. É necessária a utilização de mecanismos de segurança de tecnologia da informação que sejam capazes de impedir que pessoas não autorizadas acessem informações confidenciais.

Ferramenta: Criptografia

CONFIABILIDADE

A informação deve ser precisa e verdadeira e de boa qualidade ao qual a empresa possa confiar inteiramente.

Ferramenta: Componentes e sistema de medição.

INTEGRIDADE

É garantir que a informação estará completa, exata e preservada sem adultério, fraudes ou destruição, seja ele por acidente ou mesmo proposital.

Ferramenta: assinatura digital e Backup

DISPONIBILIDADE

É ter a informação acessível e disponível continuamente aos usuários com autorização de acesso e uso.

Ferramenta: nobreak, firewall, backup

AUTENTICIDADE

Ter capacidade de saber, por meio de registro realizado acessos, ou feito alguma modificação, inclusão e exclusão de informações, tendo registro que identifique o autor.

Ferramentas: biometria, certificado digital e assinatura

Estes princípios se tratados com critérios e cuidados beneficia a organização, assim como seus clientes internos e externos.

6 PRINCIPAIS AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

Dentre as diversas ameaças à segurança da informação é possível destacar:

> “Falhas no desenvolvimento, na implementação ou na configuração de mecanismos de segurança em softwares; negação de serviço — bloqueio de acesso por hackers; phishing — captura de dados para realização de fraudes; malwares — roubo ou sequestro de dados por meio de invasões a computadores e bases de dados; vírus — danos a sistemas e aplicativos”. Assim destaca Adrielle Fernanda Silva do Espírito Santo, do Departamento de Ciência da Computação - Instituto Cuiabano de Educação (2017)

6.1 VULNERABILIDADES, PERIGOS E AMEAÇAS À SEGURANÇA

Com a utilização da Internet as empresas se tornaram vulneráveis na rede interna, passando a ser alvo de espionagem comercial, fraudes, erros e acidentes, porém como o uso das tecnologias mais recente os riscos vão além, as empresas também precisam se preocupar com os hackers, invasões, vírus e outras ameaças a qual estão sujeitas devido ao acesso virtual.

Para evitar as ameaças algumas práticas de segurança da informação são essenciais, BRASIL, (2018), dentre elas a primeira atitude a ser realizada é reconhecer os pontos de vulnerabilidade e de maior ataque dos invasores que na maioria das vezes são os bancos de dados, sistema de energia e comunicação, o qual requer atenção nos elementos básicos como:

Vulnerabilidades de hardware e software: hardware e software devem ser substituídos periodicamente, levando em conta aspectos técnicos e de qualidade. Não basta ter o equipamento e o sistema, é necessário que este esteja adequando à tecnologia atual para que esta possa suprir as necessidades da empresa e dos clientes em tempo hábil, com eficiência e confiabilidade.

Para se ter segurança é preciso evitar a possibilidade das estações de trabalho armazenar chaves privadas e informações pessoais estas estações são sujeitas a execução de programas desconhecidos (grampos de teclado e outras armadilhas). Já os softwares estão sujeitos a falhas técnicas e de configurações de segurança, uso errado ou negligência na guarda segura e secreta de login e senha de acesso.

Ter cópias de segurança – backup: é o armazenamento da informação, fora do servidor, para evitar perdas de dados caso haja danos ou roubo no sistema. Podendo ser armazenado em dispositivos físicos ou em nuvem. Para o armazenamento em dispositivos físicos (servidores de backup, CD, pendrive, HD externo) é devido ser guardado fora do ambiente onde está o servidor evitando assim a perda por acidentes ou roubo desta copia também.

Para a realização do backup pode ser utilizado a ferramenta de backup fornecido pelo software do sistema de informações utilizado, desde que este seja configurado com mudanças de acessos padrões externo pra evitar ataques de força

bruta, que são programas que ficam tentando acesso 24hs por dia em buscar de login e senhas.

Manter permanente Segurança no servidor: A empresa deve utilizar firewalls que protegem o acesso através de um Servidor de controle no ponto único de entrada/saída dos dados, assim controla os serviços e acessos permitidos, monitora o uso e tentativas de violação e protege contra invasões externas. Deve utilizar o servidor com base de dados, ou seja, apenas como banco de dados onde os colaboradores não deverão ter acesso e sim apenas o profissional de TI deverá ter acesso através de login e senha.

Manter permanente controle e Segurança no meio de transporte: Para o meio de transporte é preciso fazer uso de algumas tecnologias como firewalls, criptografia e outros.

6.2 FATOR HUMANO

Entre as principais ameaças à segurança da informação, uma que se destaca e pode ser o maior causador de perda de dados nas organizações é a falta de capacitação do usuário interno, Mandarini (2004). A falta de orientação, ausência de conhecimento operacional dos equipamentos, sistemas, aplicativos, riscos virtuais e outros recursos que a organização utiliza deixam vulnerável a segurança da informação, assim como o desconhecimento de técnicas de proteção. Para evitar estes erros é preciso que haja na organização uma política que valorize a capacitação do colaborador, as equipes devem ser preparadas para desenvolver ações conscientes no sentido de resguardar a organização e suas informações, incluindo a responsabilidade em suas atitudes evitando a negligência frente suas funções e o que lhe é tido com confiança.

6.3 MECANISMOS LÓGICOS DE SEGURANÇA DA INFORMAÇÃO

Firewall - Controle o Tráfego da Rede

Mecanismo que controla o tráfego de dados entre os computadores de uma rede interna e os de outras redes externas. Atuam garantindo o correto funcionamento da comunicação de entrada e saída de informações com o objetivo

de impedir invasões praticadas por pessoas mal-intencionadas, em busca de dados confidenciais da organização ou de seus clientes.

Assinatura digital

É um meio ao qual é possível fazer a identificação do usuário que está acessando os recursos, da validade legal aos documentos digitais, assegurando a autenticidade de quem enviou a informação.

Biometria

Por meio das características físicas da pessoa, (impressão digital, voz ou padrões da íris do olho ou do rosto inteiro), previamente cadastrada no sistema é liberada a autorização de acesso das informações restritas em que aquela pessoa poderá ter acesso.

7 ANTIVÍRUS E SUA FUNCIONALIDADE

De acordo com a redação do site Canal Tech, disponível pelo link: https://canaltech.com.br/antivirus/o-que-e-antivirus/, com o tema: O que é antivírus? É possível entender que o antivírus é o recurso de segurança de uso quase obrigatório em qualquer sistema de informações, sua escolha deve levar em consideração a exposição a ameaças, o nível de criticidade das informações e a infraestrutura que deve ser protegida, não bastando apenas instalar qualquer software antivírus. Este software tem a função de detectar, impedir e atuar na remoção de programas de software maliciosos, como vírus e worms. Estes programas maliciosos podem ser contraídos por meio de pendrives, emails, sites de conteúdo erótico ou duvidoso, download de arquivos e programas infectados etc.

Para uma empresa definir qual sistema de proteção utilizar é importante que se tenha em projeto definido quais suas ameaças e o que precisa de proteção, entender que existe um número enorme e muito variado de ameaças cibernéticas, incluindo variedades de malware, vários tipos de vírus e ataques de phishing que irão ameaçar seu banco de dados e todo o sistema de TI todos os dias. Podendo se infiltrar, acessar informações confidenciais e sigilosas, de grande importância para a organização ou danificar o dispositivo, assim é preciso conhecer o Software que será utilizado e ter algumas informações com antecedência sobre sua funcionalidade,

confiabilidade e segurança, utilizar pesquisas já realizadas podem ajudar nesta escolha.

7.1 SOFTWARES DE PROTEÇÃO E DEFESA

A Redação do site Canal Tech, ainda afirma que os softwares de proteção geralmente são ofertados em versão gratuita, dependendo da política de cada empresa, esta gratuidade é apenas para teste de 30 dias ou um ano, sendo que poucas empresas permitem a extensão da gratuidade.

As versões gratuitas possuem: antivírus gratuito que prometem defender contra todos os tipos de Malwares, proteger o computador contra ameaças on-line, e offline. incluindo sites de phishing. (Versão básica, não recomendada para empresas).

As Versões Antivírus Pagas: defende contra todos os tipos de vírus, Malwares, proteger o computador contra ameaças on-line, ransomware, phishing, spyware, sites perigosos e outras ameaças. (Versão mais simples e custo mais acessível).

As versões Internet Security: defende de vírus, ransomware, phishing, spyware, sites perigosos e outras ameaças; protege a privacidade e as informações pessoais; protege o dinheiro em transações bancárias e compras on-line. (Versão intermediária e custo intermediário).

As versões Total Security: defende de vírus, ransomware, phishing, spyware, sites perigosos e outras ameaças; Protege pagamentos com criptografia de nível bancário; Protege e gerencia senhas e documentos confidenciais; Criptografa com VPN tudo que enviar e receber on-line; Impede que espiões vejam empresa através de dispositivos de filmagem ou pela webcam; quando voltado para família, ajuda a proteger as crianças com controle para pais avançado. (Versão completa e custo superior).

8 AS NORMAS DE SEGURANÇA

Ao pensar na segurança da informação é preciso entender que se refere a proteção de um conjunto de informações, com o objetivo de preservar o valor que tais informações contém para a empresa, MULLER,(2017). As normas de segurança da informação são importantes para se fazer uma gestão da informação eficiente, garantindo a proteção de dados estratégicos. Segundo o administrador de empresas

Marney Muller estas normas podem garantir políticas, processos, hardwares e softwares supram suas necessidades, considerando todos os riscos e atividades do negócio. E ainda considera que a “maneira de ter certeza de que está tudo sendo feito corretamente é seguir orientações de normas de segurança da informação, que determinam controles regras e diretrizes para a área”. MULLER (2017).

As normas técnicas criam regras, diretrizes e características mínimas a ser seguida em pela empresa, seguir estas normas pode dar a empresa certificados de gestão segurança e inovação. As normas de segurança que estão relacionadas à elaboração e aplicação de um Sistema de Gestão de Segurança da Informação servem para garantir a confidencialidade, integridade e disponibilidades da informação, que torna um sistema para gestão empresarial estável e seguro, esta segurança inclui todos as dados que formam a informação, sejam informações organizacionais ou pessoais, guardada para uso restrito ou exposta ao público.
Exemplo de Normas de segurança da Informação:
(British Standard) BS 7799; ISO/IEC 17799:2000; NBR ISO/IEC 17799; ISO/IEC 17799:2005; ISO/IEC 27000; ISSO/IEC 27001:2006; A ISO/IEC 27002:2005;

8.1 APRESENTAÇÃO DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO

(British Standard) BS 7799: Esta norma foi criada tendo como base vários documentos preliminares e sua utilização, o objetivo para sua criação foi ser utilizada para a consultoria pública. Após varias alterações passou a ser conhecida como a norma ISO/IEC 17799:2000, e receber reconhecimento internacional.

ISO/IEC 17799:2000: Esta norma é a versão internacional da BS7799. O conceito da norma de segurança da informação ISO/IEC 17799:2000 visa preservar a confidencialidade, integridade e disponibilidade da informação. Este conceito embora seja antigos continua a servir de norte para as demais normas de segurança da informação que surgiram posteriormente.

NBR ISO/IEC 17799: é a versão brasileira da norma ISO/IEC 17799:2000, homologada pela ABNT em 2001. Assim como em outros países esta norma abrange diversos setores da área de segurança, com diversos controles e requerimentos há serem seguidos pela empresa com o intuito de garantir a segurança da informação e ainda possibilita a obtenção do certificado, o qual

demonstra à sociedade a seriedade e responsabilidade da empresa com os dados armazenados e manipulados.

ISO/IEC 17799:2005: Esta norma abrange toda a segurança da informação independente o tipo de informação, garante que as informações contidas na empresa permaneçam em sigilo seja ela em forma de dados eletrônicos, papel ou até mesmo em idéias ou informações que o funcionário tenha em mente.

ISO/IEC 27000: esta norma representa a família de normas 27000 as quais definem os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI), onde o SGSI é abordado como sendo parte do sistema de gestão global da empresa, considera como base a possibilidade de risco que a empresa possui para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação. Esta família de normas ou sistemas inclui estrutura organizacional, processos e recursos, políticas, responsabilidades, práticas, procedimentos, atividades de planejamento.

Para que a empresa possa adquirir o certificado empresarial em gestão da segurança das informações são necessário que esta utilize a versão ISO 27001, pois esta versão é a única norma internacional auditável que serve como base para definir os requisitos para Sistema de Gestão de Segurança da Informação (SGSI).

A família da ISO/IEC 27000 se estende sequencialmente e vão se completando onde o uso de uma norma pode depender da outra ou completar a anterior. Atualmente as normas ISO/IEC ultrapassaram a sequência ISO/IEC 27050, porém após a numeração da norma ISO 27011 muitas delas ainda estão em fase de elaboração, ou relacionadas para uma área específica, como o caso de setor público, área da saúde, comércio etc., e ainda existem casos como a ISO 27020 e 27030 que não dizem respeito à gestão da segurança da Informação.

9 **QUADRO COMPARATIVO**

Família ISO/IEC 17799	**Família ISO/IEC 27000**
Visa preservar a confidencialidade, integridade e disponibilidade da informação;	ISO 27001:2006 - Define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI),

Demonstra à sociedade a seriedade e responsabilidade da empresa com os dados armazenados e manipulados.	Aborda como sendo parte do sistema de gestão global da empresa, considera a possibilidade de risco para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação.
A primeira versão serviu como base e guia para a criação das outras normas da família	As normas criadas após a primeira versão vão completando a original, deixando apropriada para a atualidade e utilização.
Passou por atualizações que a deixou apropriada para o uso na atualidade.	O uso de uma norma da família pode ou não ser obrigatório o ao uso da outra, vai de acordo com o tipo de atividade exercida, ou área de atuação.

Referencias: PALMA (2013)

Em uma breve comparação entre as normas da família ISO/IEC 17799 e as normas da família da ISO/IEC 27000 temos que, enquanto a ISO/IEC 17799:2000 e as posteriores de sua família são normas de segurança da informação que visam preservar a confidencialidade, integridade e disponibilidade da informação, têm a preocupação em demonstrar à sociedade a seriedade e responsabilidade da empresa com os dados armazenados e manipulados. As noras da família ISO/IEC 27000 trabalham com a segurança da empresa englobando todos os sistemas de gestão, relações e interferências. A ISO 27001:2006 define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI) e aborda como sendo parte do sistema de gestão global da empresa, considera a possibilidade de risco para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação. Presa pela responsabilidade, práticas, procedimentos, atividades de planejamento da empresa e suas atividades. Outro diferencial entre as normas citadas é que a ISO/IEC 17799:2000 serviu como base e guia para as demais normas de segurança da informação que surgiram posteriormente, esta norma passou por atualizações que a deixou apropriada à sua ultilização, enquanto a família das normas ISO/IEC 27000 vai se completando com suas novas versões, onde o uso de uma pode ou não ser obrigatório o ao uso da outra, essa

dependência pode estar ligada ao tipo de setor ou atividade desempenhada pela empresa, PALMA (2013).

10 CONSIDERAÇÕES FINAIS

Os sistemas de informações nas organizações têm como função a proteção dos dados coletados e armazenados pela empresa e que servem de base confiável para as tomadas de decisões, estes sistemas precisam ser confiáveis a ponto de oferecer segurança tanto para a empresa quanto para seus clientes, garantindo que as informações importante para a organização seja de sigilo e uso próprio, onde erros, invasões, fraudes e roubos não possam ocorrer, sendo assim necessário o uso de procedimentos e métodos que garanta a segurança das informações, assim como a utilização de software que atua de forma silenciosa garantindo a estabilidade e segurança das informações.

Existe inúmeras empresa que produzem softwares que previne e evitam invasões de pessoas e softwares mal intencionados em busca de dados sigilosos das organizações e seus clientes, mas para as empresas não bastam apenas ter equipamentos e programas para que esta esteja protegida de ataques maliciosos, é preciso ter capacitação e conscientização dos colaboradores, para que saibam atuar na utilização destas fermentas assim como identificar, corrigir e evitar erros humanos, uma vez que são os funcionários os responsáveis pela manipulação dos dados. Quanto mais capacitado e consciente o quadro de funcionários, menor é risco de erros humanos ou invasões, por exemplo: por email e arquivos contaminados e maior agilidade no reconhecimento de possíveis erros ou perdas no sistema.

Antes que a empresa realize a escolha por um software de segurança é preciso que entenda sua funcionalidade, quais as necessidades da empresa e qual a relação ou compatibilidade entre o software de segurança e o sistema operacional utilizado pela empresa, assim deve ser realizados testes de compatibilidade entre o sistema operacional utilizado e o sistema de informações. Após a escolha pelo sistema de informações mais adequado à empresa, a equipe de TI deve realizar todos os ajustes necessários no sistema de informações para que a empresa possa oferecer ao seu cliente interno e externo toda a confiabilidade nas informações oferecidas e a segurança necessária na armazenagem e manipulação dos dados, para que não sofra invasões e desvio de dados sigilosos, evitando que este fato

traga a empresa grande perdas, seja financeira, judicial ou quanto à imagem que a empresa transmite a sociedade e seus colaboradores.

Embora algumas das empresas e profissionais de segurança da informação podem não conhecer todas as normas de segurança da informação, ou não fazer o uso de tais normas é possível compreender que as normas permitem à empresa construir a sua política de segurança com controles eficientes, garantindo a confidencialidade, integridade e disponibilidade da informação, com a seriedade e responsabilidade aos dados armazenados e manipulados, considerando a possibilidade de risco e garantindo o uso adequado de práticas, procedimentos e atividades realizadas pela empresa.

De forma resumida, as normas da família ISO/IEC 17799, estão relacionadas à preservação à confidencialidade, integridade e disponibilidade da informação, abrangendo diversos setores da área de segurança da informação e demonstrando à sociedade a seriedade e responsabilidade da empresa com os dados armazenados e manipulados, enquanto a normas da família ISO 27000 possuem uma visão global da empresa e de suas responsabilidades frente aos dados armazenados, considerando as possibilidades de risco da armazenagem e movimentação de dados contidos no sistema de informação; possui definição para os requisitos para um Sistema de Gestão da Segurança da Informação e são um conjunto de normas complementares que podem ser utilizadas em conjunto ou isoladas umas das outras, dependendo a área de atuação ou ramo de negocio da empresa.

As dificuldades encontradas para a conclusão deste trabalho se deram devido a falta de fontes de informações confiáveis referentes às normas trabalhadas, junto a diversidade de fontes de pesquisa e a complexidade que o assunto “Controle e Acesso Seguro aos Sistemas Operacionais Empresarial” e “Sistemas de Informações” podem abranger.

Visto que é necessário para qualquer empresa realizar a coleta, armazenagem e manipulação de dados são de fundamental importância que as empresas e os profissionais da área de segurança das informações façam a utilização das normas de segurança e busquem pela conquistas de certificados de segurança, pois assim irão manter a conformidade, terão vantagens de mercado e redução de despesas e ainda manterão a organização da empresa.

Este trabalho deve servir como fonte de informação para profissionais e estudantes da área de TI, administração e educação, assim como e fonte de pesquisa para novos trabalhos relacionados ao tema Sistemas de Informação, além de possibilitar a discussões para a elaboração de novos trabalhos relacionados ao tema em estudo.

REFERÊNCIAS

BRASIL, hsc, **Boas Praticas de Segurança da Informação**, disponível em: https://www.hscbrasil.com.br/boas-praticas-de-seguranca-da-informacao/ acesso em: 10 de abril de 2019.

BENEVENTO, Maurilio , **Do Tripé da Segurança da Informação aos 5 Pilares,** ano 2012**.** Disponível emhttps://mauriliobenevento.wordpress.com/2015/04/12/do-tripe-da-seguranca-da-informacao-aos-5-pilares/, acesso em 10 de abril de 2019.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. 01/06/2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf . Acesso em: 02/04/2019.

MANDARINI, M. **Segurança Corporativa Estratégica**. São Paulo: Usina do Livro, 2004.

MAZIERO, Carlos A. **Sistemas Operacionais: Conceitos e Mecanismos**, Curitiba PR, Abril de 2019, disponível em: http://wiki.inf.ufpr.br/maziero/doku.php?id=socm:start, acesso em: 18 de maio de 2019.

MULLER Marney, **Quais são e para quê servem as normas de segurança da informação?** Disponível em: https://www.anyconsulting.com.br/normas-de-seguranca-da-informacao/, acesso em: 04 de junho de 2019.

PALMA, Fernando, **As normas da família ISO 27000**, disponível em: https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html, acesso em 04 de junho de 2019.

REDAÇÃO, **O Que É Antivírus?** Disponível em: https://canaltech.com.br/antivirus/o-que-e-antivirus/,a cesso em 10 de abril de 2019.

REZENDE, d.a.; ABREU, a. f. de. **Tecnologia da informação aplicada a sistemas de informações empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas**. São Paulo: Atlas, 2000.