CENTRO UNIVERSITÁRIO ATENAS

JOÃO VICTOR GONÇALVES BRAGA

SEGURANÇA DA INFORMAÇÃO EMPRESARIAL E SUA GESTÃO: Princípios e melhores práticas para proteção de dados e informações organizacionais de pequeno e médio porte

Paracatu

2022

JOÃO VICTOR GONÇALVES BRAGA

SEGURANÇA DA INFORMAÇÃO EMPRESARIAL E SUA GESTÃO: Princípios e melhores práticas para proteção de dados e informações organizacionais de pequeno e médio porte

Monografia apresentada ao Curso de Sistemas de Informação do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

Área de Concentração: Segurança da informação empresarial e sua gestão.

Orientador: Prof. Me. Romério Ribeiro da Silva.

Paracatu

2022

JOÃO VICTOR GONÇALVES BRAGA

SEGURANÇA DA INFORMAÇÃO EMPRESARIAL E SUA GESTÃO: princípios e melhores práticas para proteção dados e informações dentro das organizações de pequeno e médio porte

Monografia apresentada ao Curso de Sistemas de Informação do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

Área de Concentração: Segurança da informação empresarial e sua gestão.

Orientador: Prof. Me. Romério Ribeiro da Silva.

Banca Examinadora:

Paracatu- MG, 21 de junho de 2022.

_____

Prof. Me. Romério Ribeiro da Silva

Centro Universitário Atenas.

_____

Prof. Douglas Gabriel Pereira.

Centro Universitário Atenas.

_____

Prof. Anelise Avelar de Araújo.

Centro Universitário Atenas

RESUMO

Os serviços de tecnologia da informação estão cada vez mais presentes no dia a dia das pessoas e organizações, mas com a disponibilização desses serviços vêm também os ataques cibernéticos que podem comprometer os sistemas e serviços de tecnologia da informação e a usabilidade, prejudicando as organizações e seus usuários. A falta de um método de avaliação e métodos de controle de segurança pode levar uma organização a adotar métodos de controle fracos em muitas situações e deixando ela aberta a ameaças. Uma avaliação crítica dos controles relacionados à segurança da informação é necessária porque tecnologias, processos de negócios e pessoas mudam, alterando constantemente o nível de risco atual ou criando riscos para a organização. Este artigo apresenta o método de gestão de segurança da informação. Os padrões e fontes de referência mais importantes para segurança da informação e gestão de riscos foram identificados através da revisão da literatura. O modelo de avaliação está estruturado na forma de um processo de gestão e na utilização de controles reconhecidos internacionalmente que incluem a segurança da informação. Ao mesmo tempo, o modelo oferece a oportunidade de medir o nível atual de segurança e sua evolução ao longo do tempo, o que facilita a identificação de necessidades de melhoria.

Palavras-chave: Segurança da informação; Gestão da segurança da informação.

ABSTRACT

Information technology services are increasingly present in the daily lives of people and organizations, but with the availability of these services also come cyber attacks that can compromise information technology systems and services and usability, harming organizations and their users. The lack of a security assessment and control methods can lead to an organization adopting weak control methods in many situations and leaving it open to threats. A critical evaluation of information security-related controls is necessary because technologies, business processes, and people change, constantly altering the current risk level or creating risks for the organization. This article presents the information security management method. The most important standards and reference sources for information security and risk management have been identified through the literature review. The assessment model is structured in the form of a management process and the use of internationally recognized controls that include information security. At the same time, the model offers the opportunity to measure the current level of security and its evolution over time, which facilitates the identification of improvement needs.

Keywords: Information Security; Information Security Management.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me concedido o dom da vida para ter conseguido chegar aonde estou nesse momento.

Agradeço aos meus pais que são os meus alicerces, que me apoiaram nos momentos mais difíceis, mas me mantiveram forte e focado. Também aos meus amigos e familiares que participaram de alguma forma nessa trajetória.

A meu orientador, Prof. Me. Romério Ribeiro da Silva, que me orientou durante esse trabalho e contribuiu para a minha vida acadêmica e pessoal desde os primeiros períodos do Curso de Sistemas de Informação.

E, por fim, a todos aqueles que, direta ou indiretamente, contribuíram para que eu pudesse chegar até aqui.

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

PME - Pequenas e Medias Empresas

TI – Tecnologia da Informação

SIE – Sistemas de Seguranças Essenciais

PSI – Políticas de Segurança da Informação

ABNT – Associação Brasileira de Normas Técnicas

CIA – Confidencialidade, Integridade e Autenticidade

SUMÁRIO

1 INTRODUÇÃO

A importância dos sistemas de informação para as organizações está na necessidade de competir em termos de tecnologia, tornando os processos mais dinâmicos e rentáveis, com isso em mente, todas as informações devem ser protegidas. Segurança da informação vem de vários fatores, ações, práticas e normas que necessitam ser seguidas para que tudo dê certo, tal que, essas medidas de segurança devem ser aplicadas em todas as empresas que trabalham com dados e informações (MARIANO, 2014).

Fontes (2012) explica que a segurança da informação não se limita à tecnologia, mas consiste em um processo que considera a informação em um ambiente tecnológico e tradicional. Portanto, estabelece-se que as medidas de segurança da informação devem abranger três dimensões: Pessoas, processos e tecnologias.

Baseando-se em uma sequencias de práticas e ações podemos controlar acessos não autorizados ou softwares mal-intencionados, assim, para que não haja prejuízo na empresa, ou que perca clientes (MARCONDES, 2020).

Neste presente trabalho, será apresentado estratégias de seguranças fundamentais para as organizações, mesmo que seja quase impossível um banco de dados estar completamente protegido contra esses ataques cibernéticos, mas usando vários métodos e camadas de segurança é possível dificultar a invasão ou desvio de dados.

1.1 PROBLEMA

Quais consequências a falta de segurança nas informações pode ocasionar no meio organizacional?

1.2 HIPÓTESES

Acredita-se que as consequências da falta de segurança da informação são notórias nas organizações, o que inclui riscos aos dados confidenciais, informações de identificação pessoal, dados e sistemas de informação. Sem os meios de segurança da informação, hackers e malware podem representar uma ameaça direta e indireta aos dados confidenciais da empresa, assim, podendo prejudicar também financeiramente.

Circunstâncias indiretas podem prejudicar as relações com os clientes e até mesmo expô-los a riscos legais. A realidade é que seja uma empresa pequena, média, grande ou multinacional, ela depende da segurança da informação todos os dias.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Identificar práticas para proteger dados e informações dentro das organizações de pequeno e médio porte.

1.3.2 OBJETIVOS ESPECÍFICOS

a) citar a história da segurança da informação no meio corporativo.
b) demonstrar a importância dos meios de segurança da informação empresarial.
c) identificar procedimentos e normas de segurança de acordo com suas necessidades.

1.4 JUSTIFICATIVA

É notório o avanço das tecnologias, sendo assim, no meio organizacional não seria diferente, a inclusão da tecnologia e informação no meio organizacional é algo indispensável nos dias de hoje, ajudando a aumentar os lucros e nos avanços das atividades dos colaboradores.

Assim o tráfego de dados e informações dentro desse meio corporativo é constante, e tendo isso em vista a segurança da informação precisa acompanhar o avanço nas pequenas e medias empresas, esse projeto de pesquisa traz de forma descritiva implementar a gestão da segurança da informação e identificar os fatores que influenciam as PME a adotarem medidas e práticas de gestão da segurança da informação (NETWORKS, 2018).

1.5 METODOLOGIA DO ESTUDO

A pesquisa abordada tem como objetivo a descritiva das características de determinada área da tecnologia e informação. Tem finalidade de identificar possíveis relações entre variáveis, pois o objetivo é descrever o processo de segurança da informação (GIL, 2007).

A fonte de consulta foi por meio bibliográfico, além da base de dados de conteúdo acadêmicos, artigos publicados e por maior parte leitura de livros, sendo assim, foi escolhido este tipo de pesquisa por conseguir melhor abranger o tema escolhido (GIL, 2007).

Tendo como conseguir aprimorar ideias, considerando vários aspectos relativos do assunto abordado, familiarizando mais com o tema, sendo que, este trabalho contextualiza o problema analisado e explica seus processos.

1.6 ESTRUTURA DO TRABALHO

A estrutura do trabalho é composta por uma introdução, um corpo, uma conclusão e uma bibliografia. A introdução apresenta o tema do trabalho e os objetivos a serem alcançados. O corpo é dividido em seções e subseções e apresentando práticas, Políticas e Normas da Segurança da Informação no meio corporativo.

Por sua vez, a partir da estrutura do trabalho será discorrido sobre os primeiros dados e informações usados no meio corporativo, daí em diante será apresentado um esclarecimento das ferramentas da Segurança da Informação e seus fins, e pôr fim à conclusão que trago como meio de esclarecimento desta monografia.

2 HISTÓRIA DA SEGUNRAÇA DA INFORMAÇÃO NO MEIO CORPORATIVO

Para melhor entendermos esse presente trabalho, devemos compreender o começo da segurança da informação e como funciona.

Ao longo da história, as pessoas sempre tentaram controlar informações que de alguma forma eram importantes, isso é verdade mesmo nos mais antigos tempos.

Sêmola (2003) destaca que, no começo os dados eram processados em um número centralizado e ainda não eram altamente automatizados. A tecnologia de computadores estava em sua infância e inicialmente era apenas uma nova ferramenta promissora, especialmente devido às limitações iniciais de armazenamento e preços exorbitantes dos primeiros computadores *mainframe*. Mas logo os investimentos industriais de alta tecnologia declinaram e seus frutos tornaram-se mais acessíveis.

Embora as empresas tenham muitas informações de documentos manuscritos, em arquivos de ferro familiares, os computadores *mainframe* herdaram gradualmente a função de processamento central e armazenamento de dados. Em breve veremos terminais distribuídos pelos ambientes da empresa que inicialmente um por departamento que possibilitam o monitoramento remoto (SÊMOLA, 2003).

O compartilhamento de informações foi considerado uma prática de gestão moderna que buscava agilidade operacional. Foi assim que criaram as primeiras redes de computadores e ao mesmo tempo, informações foram digitalizadas e armazenadas (SÊMOLA, 2003).

2.1 SISTEMAS DE INFORMAÇÕES

De acordo com Stair e Reynolds (2015), um sistema de informação (SI) é uma coleção de componentes interdependentes que coletam, manipulam, armazenam e disseminam dados e informações e que fornecem um mecanismo de feedback para atingir um objetivo, sendo que, esse mecanismo de feedback que ajuda uma organização a atingir seus objetivos, como aumentar os lucros ou melhorar o atendimento ao cliente.

2.2 SEGURANÇA DA INFORMAÇÃO

Para Oliveira (2013), uma compreensão concreta da segurança da informação não tem sido fácil para pesquisadores do assunto até agora.

O que é segurança? A maioria das pessoas pode responder a essa pergunta sem consultar livros ou dicionários. Segurança é um conceito que aparece no cotidiano da sociedade moderna em contraste com a violência ou a perda. No entanto, para encontrar o conceito de segurança de dados, vale passar pela definição do termo segurança (OLIVEIRA, 2013).

Nestas e outras definições semelhantes, o mais importante a distinguir é a mesma ideia de proteger alguém ou algo ou ser protegido das ações nocivas de alguém ou algo. Podemos observar um caráter proativo que nos leva à ideia de que a segurança não se limita a responder a qualquer agressão ou ações danosas, mas reflete a ideia de estar pronto para fornecer proteção para o que se quer garantir. Essa natureza proativa também está presente no conceito de segurança da informação (OLIVEIRA, 2013).

Cada vez mais importante para organizações, a informação é considerada um ativo valioso que deve ser armazenado e protegido adequadamente para manter a continuidade dos negócios e até mesmo a existência organizacional.

3 TECNOLOGIA E TRÁFEGO DE DADOS E INFORMAÇÕES

A importância dos sistemas de informação para as organizações reside no fato de que precisa ser tecnologicamente competitivo, tornando os processos mais dinâmicos e rentáveis, este é o objetivo primordial. Sendo, a utilização das tecnologias é essencial para a sobrevivência das organizações, pois através de sistemas tudo será planejado, executado, articulado e executado, é fundamental que as empresas devem estar estruturadas e organizadas para utilizar os sistemas de informação essenciais – SIE (LAMPERT; BADALOTTI, 2015).

Com a expansão das redes de computadores, o desenvolvimento e aprimoramento dos processos de comunicação de dados, facilitaram a disponibilização

de troca de informações entre pessoas, organizações, filiais, parceiros, para fornecedores e clientes, sendo assim, devem ser seguidos as práticas de armazenamento, manutenção e disponibilidade. Uma consequência é o aparecimento diário de novas vulnerabilidades nos sistemas operacionais, aplicativos e ferramentas que eles usam (CARVALHO, 2009).

Com a Internet, as organizações podem se comunicar entre seus usuários, clientes e fornecedores, independente da localidade, estado ou país em que estejam, com esses recursos, a avaliação de lances, produtos e serviços e o atendimento de pedidos de compra e venda ficarão muito mais fáceis. Muitas empresas estão usando a Internet e as tecnologias para capitalizar o crescimento que vem do uso da Internet em computadores e dispositivos móveis (LAMPERT; BADALOTTI, 2015).

Segundo Beal (2008), dados, informações e conhecimento são recursos cada vez mais críticos para a realização da missão e objetivos de uma organização devido à sua alta capacidade de agregar valor aos processos, produtos e serviços. Como qualquer outro ativo valioso para uma organização, as informações críticas de negócios devem ser protegidas contra ameaças que possam resultar em sua destruição, acesso temporário, violação ou divulgação não autorizada.

3.1 RISCOS, AMEAÇAS E VULNERABILIDADE

Risco é a probabilidade de que um determinado evento se materialize, bem como seus potenciais impactos (FERNANDES, 2014).

Ameaça é qualquer condição existente ou iminente que pode causar danos às partes interessadas (FERNANDES, 2014).

Vulnerabilidade é uma deficiência ou fraqueza que pode ser explorada para causar danos (FERNANDES, 2014).

3.2 RISCOS

Cada controle de segurança implementado para reduzir um ou mais riscos cai em custos e aumenta a probabilidade de que outros eventos positivos também diminuam e, como resultado, a organização perderá alguma flexibilidade e deixará de inovar (SILVA; CARVALHO; TORRES, 2003).

O gerente de segurança da informação deve, portanto, encontrar um equilíbrio entre os benefícios de aumentar a segurança contra as perdas resultantes dos investimentos em controle e as perdas associadas à flexibilidade organizacional reduzida (SILVA; CARVALHO; TORRES, 2003).

Para Silva, Carvalho e Torres (2003), a gestão de riscos é o processo de identificação de um conjunto de medidas pelas quais a Companhia pode atingir o nível de segurança desejado pela administração. Esse processo é parte integrante do programa de segurança da empresa e consiste em etapas nas quais os riscos são identificados e classificados, seguidos pela definição de um conjunto equilibrado de medidas de segurança para reduzir ou eliminar os riscos.

3.3 AMEAÇAS

Há um consenso no setor de segurança de que as ameaças podem ter duas origens, internas e externas.

Ameaças internas, conectadas à Internet ou não. Isso pode variar desde o trabalho impróprio de um funcionário ou má configuração de um servidor web até o roubo de informações dos funcionários da organização, como contaminação por vírus, funcionários mal treinados, divulgação de senhas e funcionários de empresas terceirizadas (FERNANDES, 2014).

As ameaças externas são ataques vindos de fora do ambiente da organização que visam explorar a vulnerabilidade de um determinado sistema.

O roubo de informações confidenciais por pessoas não autorizadas pode comprometer informações pessoais de funcionários ou consumidores, revelar esforços de marketing ou planos de desenvolvimento de novos produtos, causando interrupções ou inconveniências à organização. Organizações com operações extensas precisam de uma maneira de garantir a comunicação com funcionários e parceiros de negócios independentemente de onde estejam suas instalações (STAIR; REYNOLD, 2015).

3.4 VULNERABILIDADE

Devemos entender que o objeto é a informação e não está mais limitado a ambientes físicos específicos ou processos individuais. As informações agora circulam por toda a empresa, alimentam todos os processos de negócios, estão expostas a várias ameaças, violações de segurança ou vulnerabilidades e são fáceis de ser manipuladas (FERNANDES, 2014).

Na implementação de uma PSI eficaz não depende apenas da utilização de recursos financeiros ou do aprimoramento da infraestrutura de segurança da informação com firewalls, antivírus e outras barreiras tecnológicas, mas requer uma mudança na cultura. em relação ao processamento de dados. No caso da segurança da informação e da comunicação, segue-se o princípio de que “uma cadeia é tão forte quanto seu elo mais fraco” e o ponto mais vulnerável da gestão da informação tem sido considerado o aspecto humano. Os agentes mal-intencionados estão cientes dos recursos de segurança da informação das organizações e muitas vezes usam seu poder ofensivo como engenharia social, que consiste em explorar as fraquezas, a confiança ou a ingenuidade das pessoas em relação às suas atitudes cotidianas e habitual descuido com as informações (OLIVEIRA, 2013).

Sendo que Cabral e Caprino (2015) destaque que a empresa se tornou uma grande rede de comunicação integrada dependente de fluxos de informações compartilhados e distribuídos. Os mesmos dados que agora possuem vulnerabilidades que transcendem aspectos tecnológicos também são interrompidos por aspectos físicos e humanos.

Do ponto de vista da anatomia do problema, o fator crítico de sucesso é a identificação de elementos internos e externos que previnem riscos de segurança da informação. É hora de mapear, além dos planos estratégicos e definições de negócios, as características físicas, tecnológicas e humanas da empresa, os mercados em que atua, os concorrentes

3.5 IMPACTO

Para Cabral e Caprino (2015), o dano causado quando uma ameaça se materializa é conhecido como “impacto”. O efeito está diretamente relacionado ao enfraquecimento de uma das principais características da segurança da informação - confidencialidade, integridade e disponibilidade. O efeito pode se apresentar de várias maneiras, embora seja comum olhar para ele economicamente, ou seja. como custo ou prejuízo causado pela manifestação de perigo.

3.6 TRATAMENTO DE INCIDENTES

Todas as atitudes e medidas da organização para prevenir acidentes dizem respeito ao tratamento de violações de segurança da informação. Firewalls de rede e Internet, scanners para varredura de rede e sistemas, detectores de abuso e anomalias, softwares de filtragem de conteúdo como ferramentas para prevenir e detectar problemas de segurança da informação organizacional Beal (2005).

A ABNT NBR ISO/IEC 27002 (2013) recomenda que, quando descoberta uma violação de segurança de dados, o ponto de contato de segurança de dados seja notificado imediatamente, pois não está necessariamente claro se o caso levará a um processo administrativo, investigação, litígio ou simplesmente arquivado pela indústria de segurança. Retomando a praticar e aprendizado no trabalho, devem ser questionados se foram compartilhadas informações sobre medidas de segurança da informação que poderiam prevenir ou mitigar novos incidentes de segurança da informação. Por meio desses processos, é possível formalizar análises quantitativas e qualitativas de possíveis ataques.

A NBR/ISO/IEC 17799 (2005) diz que é conveniente criar um procedimento para relatar oficialmente uma violação de segurança, que determina as medidas necessárias após o recebimento dos incidentes. ponto de contato disponível e divulgado em toda a organização. A norma acrescenta que todos os colaboradores, fornecedores e terceiros estão cientes de sua obrigação de relatar um incidente de segurança da informação o mais rápido possível.

4 PROCEDIMENTOS E NORMAS PARA SEGURANÇA DA INFORMAÇÃO

Intranet é uma tecnologia amplamente utilizada pelas organizações para comunicação dentro de sua rede corporativa ou mesmo para comunicação entre matriz e filiais. Eles são definidos como o sistema que rege os processos e operações de negócios internos, funcionam como uma câmara de compensação e só podem ser acessados por usuários internos autorizados (LAMPERT; BADALOTTI, 2015).

A Extranet é uma tecnologia que possui funções semelhantes a uma intranet, mas nela podem ser configurados direitos de acesso para que as informações fiquem ainda mais restritas ao usuário, pois sua conexão se faz presente fora da rede corporativa, sem utilizar a rede interna, mas usando uma rede externa, como a Internet, para se conectar aos dados e informações disponíveis para a empresa. A comunicação por meio dessa ferramenta de extranet geralmente é realizada pelos fornecedores e clientes da organização e independe da localização do usuário, desde que ele tenha acesso à Internet (LAMPERT; BADALOTTI, 2015).

Gestão de acessos é uma área que vem despertando a atenção das organizações há algum tempo. O controle de acesso eficaz, tanto lógico quanto físico, ajuda outras áreas de segurança a implementar suas soluções de forma eficaz. Um conjunto de procedimentos deve ser estabelecido para garantir o acesso seguro a áreas restritas ou a uma instalação (OLIVEIRA, 2013).

A gestão da continuidade dos negócios é uma das questões mais importantes da segurança da informação e comunicação, aliás, traz essa importância em seu nome, ou seja. negócio não pode parar. Para isso é necessário conhecer bem as atividades comerciais da organização e ter um plano que antecipe o que será feito em caso de crise ou desastre que possa causar interrupções na atividade da organização (OLIVEIRA, 2013).

Assim, em termos simples, a função da gestão da segurança da informação é gerenciar o processo de segurança da informação através dos processos de planejamento, organização, direção e controle das ações relacionadas à segurança da informação na organização (MARCONDES, 2020).

4.1 ASPECTOS HUMANOS

Na segurança da informação, as pessoas trazem um ponto muito importante para o processo. É muito importante que todos os colaboradores da organização estejam envolvidos na implementação do PSI. O PSI em si não torna uma organização mais segura, mas sim o comprometimento de toda a organização. Quando se fala em recursos humanos, a mera confiança não é suficiente, mas o comportamento das pessoas na organização deve ser controlado, ou analisado, pois embora os ataques externos sejam geralmente mais notados, a maioria dos desastres de segurança são causados por pessoas que estão diretamente conectadas a a organização , seja de forma não intencional ou com a intenção de causar algum dano à organização (BEAL, 2008).

4.2 PROCESSO DE SELEÇÃO

No processo de seleção é importante que sejam realizadas as verificações de acordo com as leis, regulamentações e éticas, proporcionalmente aos requisitos do negócio, à classificação das informações e aos riscos detectados, sendo que, durante o processo de seleção é importante buscar informações das pessoas, tais como referências profissionais e pessoais para analisar o comportamento da pessoa antes da contratação, verificação curricular, qualificações acadêmicas, verificações criminais como fichas policiais e também de crédito junto aos órgãos de proteção ao cliente por exemplo (NBR/ISO/IEC 17799 2005).

4.3 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Os princípios e diretrizes, conhecidos como Política de Segurança da Informação, foram elaborados para mostrar o comportamento de segurança da informação dos funcionários. Essas diretrizes geralmente são documentadas pela função das SI, que também é responsável por coordenar sua implementação, validação e revisão. A alta administração, vários gerentes e proprietários também estão envolvidos na elaboração do PSI, recomendando que o cargo mais alto da organização seja responsável por aprová-lo (TCU, 2014).

A PSI deve prever por si o que fazer nos casos em que as suas ordens não sejam cumpridas, consoante a sua gravidade, âmbito e tipo de infrator. A punição pode ser uma simples advertência verbal ou escrita; ou por meio de ação judicial (TCU, 2014).

Baldissera e Nunes (2007) afirmam que a ABNT (Associação Brasileira de Normas Técnicas), em parceria com a *International Organization for Standardization* (ISO), procurou responder às necessidades nacionais de segurança da informação fornecendo uma versão brasileira da ISO/IEC 17799. A ABNT A norma NBR ISO/IEC (*International Electrotechnical Commission)* 17799 :2005 contém diretrizes e princípios gerais que nos permitem implementar, manter e aprimorar a gestão da segurança da informação na organização. No entanto, a norma é ampla e sua aplicação pode significar um baixo retorno sobre o capital investido.

Em 2005, porém, surgiu a norma ISO 27001, uma visão de processos já contemplada por normas de sistemas de gestão (CAUBIT, 2006).

No mesmo ano, a ISO aprovou e publicou a norma ISO 27002. No Brasil, a ABNT publicou a norma brasileira equivalente NBR ISO IEC 17799:2005. A norma utilizada para a certificação é a ISO/IEC 27001. A norma brasileira NBR ISO/IEC 17799:2005 é um guia prático que define diretrizes e princípios gerais para iniciar, implementar, manter e aprimorar a gestão de segurança da informação de uma organização (SILVA, 2020).

4.4 CONFIDENCIALIDADE

Confidencialidade é a capacidade de garantir que a confidencialidade exigida seja mantida em cada interseção das informações que estão sendo processadas. Além disso, é impedir sua divulgação não autorizada (SÊMOLA, 2003).

Os invasores podem burlar os mecanismos de confidencialidade por meio de monitoramento de rede, engenharia social e roubo de arquivos de senha (Sêmola, 2003).

A confidencialidade é garantida por técnicas de criptografia de dados e métodos de armazenamento e transmissão dos mesmos, além de monitoramento de tráfego de rede, controle rigoroso de acesso, classificação de dados e treinamento de pessoal no uso de dados na empresa (SÊMOLA, 2003).

4.5 INTEGRIDADE

A integridade é uma garantia da exatidão e confiabilidade dos dados e sistemas, e a ausência de alterações não autorizadas aos dados, e para a correta manutenção e processamento dos dados e entrega aos destinos, hardware, software e mecanismos de comunicação devem trabalhar em conjunto. desejado sem alterações não autorizadas ou inesperadas (SÊMOLA, 2003).

Os sistemas e a rede da empresa devem ser protegidos contra interferências e contaminações fora do ambiente tecnológico.

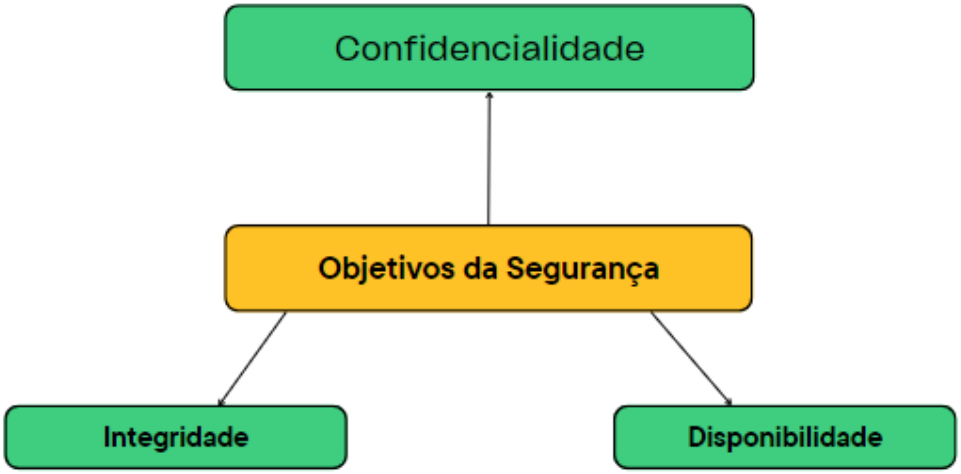
4.6 DISPONIBILIDADE

Os sistemas e redes devem ser capazes de realizar e fornecer dados de forma previsível e suficiente para as necessidades da empresa, e ser capazes de restaurar as contas disponíveis de forma rápida e segura e garantir a produtividade das operações da empresa. não é seriamente afetada (SÊMOLA, 2003).

Erros de hardware ou software podem afetar a usabilidade do sistema.

Assim como os backups que devem estar disponíveis para a rápida recuperação de sistemas e dados críticos em uma empresa, embora aspectos ambientais como calor, frio, umidade, eletricidade estática e produtos poluentes possam afetar a disponibilidade de sistemas e dados (SÊMOLA, 2003).

Figura 1 – Objetivo da tríade CIA



Fonte: autoria própria.

O programa de segurança tem vários objetivos, alguns pequenos e outros grandes. Os três princípios de todos os programas de segurança da informação citados a cima são: confidencialidade, integridade e disponibilidade - CIA (SÊMOLA, 2003).

5 CONSIDERAÇÕES FINAIS

O objetivo do trabalho foi alcançado no que se trata das quais consequências a falta de segurança nas informações pode ocasionar no meio organizacional.

Como você pode ver, a segurança da informação depende de tecnologias, mas também de pessoal treinado. Requer planejamento, bem como ações efetivas. Esse conhecimento foi apresentado durante neste presente trabalho, também sobre ameaças e riscos, bem como conhecimento da própria organização e, sobretudo, do negócio, pois a segurança da informação existe em função da empresa.

Ignorar tais medidas como processos, equipamentos e programas, pode ter consequências graves e, portanto, o investimento nesta área é essencial, mas em caso de incidentes, é conveniente criar um procedimento para relatar oficialmente uma violação de segurança, que determina as medidas necessárias após o recebimento dos incidentes.

Assim conclusão é que, o mais importante é atingir um nível aceitável de segurança, minimizando o impacto na organização tanto interna como externa, porque, afinal, não existe segurança absoluta. As informações aqui apresentadas são suficientes para obter pelo menos uma visão geral das ameaças e soluções relacionadas à segurança da informação, desde a história da segurança da informação, a importância de tê-la na organização e a identificar esses procedimentos e normas de acordo com cada necessidade, possibilitando inclusive a criação de uma política de segurança da informação ou seu aprimoramento, caso já exista.

Conclui-se que a segurança da informação é essencial para o meio corporativo, tanto em pequenas, medias e grandes empresas.

REFERÊNCIAS

ABNT. NBR ISO/IEC 27002: 2013: **Tecnologia da informação Técnicas de Segurança - Código de Prática para controles de segurança da informação.** Rio de Janeiro: ABNT, 2013.

BALDISSERA, Thiago André; NUNES, Raul Ceretta. **Impacto na implementação da NORMA NBR ISO/IEC 17799 Para a gestão da segurança da informação em colégios**: um estudo de caso. Foz do Iguaçu: Enegep, 2007. 10 p.

BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

BRASIL. **Instrução normativa GSI/PR nº 1, de 13 de junho de 2008**. Disponível em: < http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf >. Acesso em: 26 abril 2016.

CABRAL, Carlos; CAPRINO, Willian. **Trilhas em segurança da informação**: caminhos e ideias para proteção de dados. Rio de Janeiro: Brasport, 2015. 357 p.

CARVALHO, Rodrigo de Oliveira. **Segurança da informação nas organizações**. 2009. 41 f. TCC (Graduação) - Curso de Tecnologia da Informação, Faculdade de Tecnologia e Ciências Sociais Aplicadas, Brasília, 2009.

CAUBIT, R. **O que é a ISO 27001, afinal?** 19 Jan 2006. Modulo Security Magazine. Disponível em www.modulo.com.br Acesso em: 10 out 2022.

FERNANDES, Nélia Oliveira Campo. **Segurança da informação**. Cuiabá: Rede E-Tec Brasil, 2014. 105 p.

GIL, A. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo, Atlas: 2007.

LAMPERT, Edna da Luz; BADALOTTI, Greisse Moser. **Sistemas de Informação**. Indaial: Dante Alighieri, 2015. 189 p. Disponível em: https://www.uniasselvi.com.br/extranet/layout/request/trilha/materiais/livro/livro.php?codigo=21652. Acesso em: 24 abr. 2022.

MARCONDES, José Sérgio (20 de outubro de 2020). **Gestão de Segurança da Informação: O que é, O que faz, Processos**. Disponível em Blog Gestão de Segurança Privada: – Acessado em 25 abr. 2022.

MARIANO, Yuri Ribeiro. **Boas práticas de políticas de segurança da informação para microempresas**, 2014. Trabalho de conclusão de curso (Curso de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2014

NBR/ISO/IEC 17799. **Tecnologia da Informação**: Código de prática para a gestão da segurança da informação. ABNT, 2005.

NETWORKS, Telium. **Segurança de dados: Um panorama sobre a questão nas empresas**. 2018. Disponível em: https://www.telium.com.br/blog/seguranca-de-dados-um-panorama-sobre-a-questao-nas-empresas. Acesso em: 31 maio 2022.

OLIVEIRA, Fábio Cezar de. **A SEGURANÇA DA INFORMAÇÃO NO CNPq**: alinhamento à legislação e às boas práticas vigentes. 2013. 142 f. Dissertação (Doutorado) - Curso de Política e Gestão de Ciência e Tecnologia, Centro Sustentável, Universidade de Brasília Centro de Desenvolvimento Sustentável, Brasília, 2013. Cap. 23.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva. 17. ed. Rio de Janeiro: Estúdio Castellani, 2003. 163 p.

SILVA, Eliane Ferreira da. **Boas Práticas de Segurança da Informação nas organizações**. Rio de Janeiro: Dalagaia, 2020. 67 p.

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho. **SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO**: gestão estratégica da segurança empresarial. Lisboa Portugal: Centro Atlatico, 2003. 256 p.

STAIR, Ralph M.; REYNOLDS, George W. **Princípios de Sistemas de Informação**. 11. ed. São Paulo: Cengage Learning, 2015. 720 p. Tradução de: Noveritis do Brasil.

TCU. 2014. **Boas práticas em Segurança da Informação**. Brasília: Tribunal de Contas da União, 2014.