UNIVERSIDADE EVANGÉLICA DE GOIÁS – UniEVANGÉLICA
BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

PROPOSTA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA AMBIENTE DE TRABALHO *HOME OFFICE*

IVAN CRISTHIAN MEIRA ARAÚJO

Anápolis
2021-1

IVAN CRISTHIAN MEIRA ARAÚJO

PROPOSTA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA AMBIENTE DE TRABALHO *HOME OFFICE*

Trabalho de Conclusão de Curso I apresentado como requisito parcial para a conclusão da disciplina de Trabalho de Conclusão de Curso I do curso de Bacharelado em Engenharia de Computação da Universidade Evangélica de Goiás – UniEVANGÉLICA.

Orientadora: Profa. Natasha Sophie Pereira.
Coorientador: Prof. William Pereira dos Santos Júnior

Anápolis
2021-1

IVAN CRISTHIAN MEIRA ARAÚJO

PROPOSTA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA AMBIENTE DE TRABALHO *HOME OFFICE*

Trabalho de Conclusão de Curso I apresentado como requisito parcial para a conclusão da disciplina de Trabalho de Conclusão de Curso I do curso de Bacharelado em Engenharia de Computação da Universidade Evangélica de Goiás – UniEVANGÉLICA.

Aprovado pela banca examinadora em ___ de ___ de 2021, composta por:

_____
Profª. Natasha Sophie Pereira
Orientador

_____
Prof. William Pereira dos Santos Júnior
Coorientador

_____
Yuri Santiago da Silva Romano
Convidado

LISTA DE ABREVIATURAS E SIGLAS

CID	Confidencialidade, Integridade e Disponibilidade
DNS	Domain Name System
DoS	Denial of Service
IP	Internet Protocol
PSI	Política de Segurança da Informação
SGSI	Sistema de Gerenciamento da Segurança da Informação
TIC	Tecnologias de Informação e Comunicação

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

RESUMO

Este trabalho aborda a aplicação de conceitos de Segurança da Informação para a definição de uma proposta de Política de Segurança da Informação. Seu objetivo geral é definir uma proposta de Política de Segurança que possa ser implementada em ambientes de trabalho *Home Office* ou Teletrabalho. Esta proposta será baseada em pesquisa teórica, de autores como Mitnick (2003), Stallings (2014), Hintzbergen *et al.* (2018), Sommerville (2011), entre outros. Como resultado, é esperado que esta proposta demonstre a importância da Segurança da Informação e do desenvolvimento e aplicação de uma Política de Segurança em uma organização, bem como a conscientização de todos os colaboradores.

Palavras-chave: Segurança da Informação. *Home Office.* Teletrabalho. Política de Segurança da Informação.

1. INTRODUÇÃO

1.1. Problema

Ambientes de trabalho *Home Office* ou Teletrabalho vem ganhando grande destaque, principalmente nos anos de 2020 e 2021, devido a pandemia de COVID-19, sendo esse um fator decisivo para dar continuidade à economia (Organização Internacional do Trabalho, 2020). De acordo com a Confederação Nacional da Indústria (2020), 70% das empresas espanholas optaram pela modalidade de trabalho *Home Office* durante a pandemia, contabilizando um total de três milhões de trabalhadores no país nessa modalidade.

Nesse tipo de ambiente, a realização de atividades profissionais são executadas à distância física do ambiente empresarial, por meio de tecnologias de informação e comunicação (TIC), como computadores, celulares, *tablets*, etc (Organização Internacional do Trabalho, 2020).

Considerando a possibilidade de ataques, sendo eles de Engenharia Social, interceptação, vazamento ou perda de informações, contaminações por vírus, ataques de hackers, queda de energia, etc; qual seria o impacto na Segurança da Informação com a implementação de uma Política de Segurança da Informação (PSI) em ambientes *Home Office*?

1.2. Objetivos

1.2.1. Objetivo Geral

O objetivo geral desta pesquisa é propor uma Política de Segurança da Informação (PSI) para ambientes *Home Office*.

1.2.2. Objetivos Específicos

- Identificar conceitos de Segurança da Informação, através de pesquisa bibliográfica, junto às normas ISO/IEC e ABNT NBR ISO/IEC;
- Realizar pesquisa bibliográfica de conceitos de uma PSI, visando o seu desenvolvimento e aplicação;
- Realizar um estudo bibliográfico de ambientes *Home Office*;
- Propor uma Política de Segurança da Informação (PSI) para ambientes *Home Office* baseada no estudo realizado.

2. JUSTIFICATIVA

A utilização de *software* vem se expandindo cada vez mais, a sua aplicação vai de sistemas de infraestrutura, produtos elétricos, indústria, sistema financeiro, entretenimento como a indústria da música, jogos de computador, cinema e televisão (SOMMERVILLE, 2011).

Junto à constante evolução e popularização de sistemas de *software*, vem a crescente onda de ataques, que vão de ataques simples à ataques a grandes organizações.

Segundo Mitnick (2003, p. 207)

> "Nove entre dez grandes corporações e órgãos governamentais já foram atacados por invasores de computadores, a julgar pelos resultados de uma pesquisa realizada pelo FBI e reportada pela Associated Press em abril de 2002".

Evidencia-se a necessidade de investimento e planejamento na Segurança da Informação de uma organização, de forma a manter e proteger todos os seus ativos, pois organizações investem muito dinheiro em seus sistemas de *software*, tornando-os ativos de extrema importância para a organização (SOMMERVILLE, 2011).

Hintzbergen *et al.* (2018, p. 29), definem um ativo como "[…] qualquer coisa que tenha valor para a organização". Para Stallings (2014), eles se classificam como: dados, serviços, capacidade de sistemas, equipamentos e instalações físicas.

Ambientes de trabalho *home office* ou Teletrabalho, são definidos como a execução de atividades profissionais, fisicamente separada das instalações da organização, utilizando-se de tecnologias de informação e comunicação como *smartphones*, *tablets*, computadores, etc (Organização Internacional do Trabalho, 2020).

Nestes ambientes, a atenção à segurança também deve ser aplicada, e neste caso, Hintzbergen *et al.* (2018, p. 165) enfatizam que sempre que uma organização planejar, comprar ou desenvolver um sistema de informação, a segurança deve fazer parte do projeto. Recomenda-se a aplicação de segurança ao sistema de informação logo no início, pois a implementação em fases mais avançadas, em certos casos, se torna impossível devido a erros fundamentais de projeto, se tornando ainda mais caras.

Mitnick (2003) enfatiza que a gerência deve deixar claro a todos os empregados a importância da segurança da informação às operações da organização e que a contribuição de cada empregado é vital. Políticas de Segurança da Informação, são:

> "[...] instruções claras que fornecem as orientações de comportamento do empregado para guardar as informações, e são um elemento fundamental no desenvolvimento de controles efetivos para contra-atacar as possíveis ameaças à segurança" (MITNICK, 2003, p. 208)

Mitnick (2003) destaca ainda que os controles de segurança devem ser implementados através do treinamento dos empregados, com políticas e procedimentos documentados, com o objetivo de reduzir os riscos a um nível aceitável.

Hintzbergen *et al.* (2018) também destacam que a política de segurança da informação deve ser aprovada pelo conselho administrativo e que ela deve estar disponível para todos os funcionários e parceiros externos relevantes, levantando ainda a necessidade de um programa de conscientização de forma a atender todos os funcionários.

Mitnick (2003) reforça essa ideia ao apontar que a gerência adote e dê suporte ao desenvolvimento de políticas e programas, demonstrando a importância da segurança da informação para a organização aos demais funcionários. Portanto, uma Política de Segurança da Informação garante a proteção da informação e é fundamental como contramedida às possíveis ameaças. Desta forma garante-se a Segurança da Informação, que Hintzbergen *et al.* (2018, p. 33) definem como a "Preservação da Confidencialidade, integridade e disponibilidade da informação".

3. REFERENCIAL TEÓRICO

3.1. Segurança da Informação

Define-se Segurança da Informação ou Segurança de Computadores, conforme descrito pelo NIST - *National Institute of Standard and Technology* (1995, p. 9) e citado por Stallings (2014, p. 7), como:

> "A proteção oferecida a um sistema de informação automatizado para atingir os objetivos apropriados de preservação da integridade, disponibilidade e confidencialidade de ativos de sistemas de informação (incluindo *hardware, software, firmware*, informações/dados e telecomunicações)".

Sistemas de Informação são classificados por Hintzbergen *et al.* (2018, p. 36) como sendo uma "Aplicação, serviço, recursos de tecnologia da informação ou qualquer outro componente de manejo da informação". Os autores ainda destacam que esses sistemas se referem à interação entre pessoas, processos, dados e tecnologia, não apenas à Tecnologia da Informação e de Comunicações (TIC), mas também à forma de interação entre as pessoas e essas tecnologias.

Sistemas de informação estão sob constante ameaça, oriundas de diversas fontes como fraudes, espionagem, sabotagem, vandalismo, incêndio, inundação, etc; e que estas ameaças estão comumente associadas à causas de danos cada vez mais frequentes, como códigos maliciosos, ataques de *hackers,* ataques de negação de serviço (DoS – Denial of Service), etc (HINTZBERGEN *et al.*, 2018).

Essas ameaças são causas potenciais de incidentes, que podem acarretar danos a ativos. Os incidentes são definidos por um ou vários eventos que tenham a chance de causar impactos negativos ao negócio, ameaçando a Segurança da Informação. Já os eventos são mais especificamente definidos como Evento de Segurança da Informação, que são indicativos de que houve violação da política de segurança, falha de proteção ou qualquer outra situação que tenha impacto na segurança (HINTZBERGEN *et al.*, 2018).

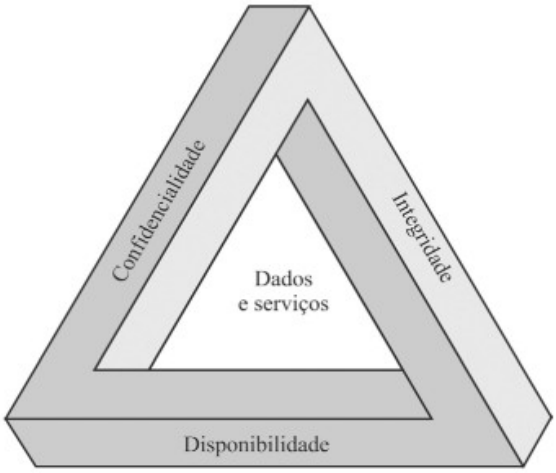
De acordo com a norma NBR 27002 (ABNT, 2013, p. X), garante-se a segurança da informação com a "[…] implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*". Esta norma enfatiza ainda que esses controles devem:

> "[...] ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos" (ABNT, 2013, p. X).

3.1.1. Princípios fundamentais da Segurança da Informação

Stallings (2014) considera três princípios fundamentais da Segurança de Computadores, citados mais especificamente pelo autor como o coração da segurança de computadores ou a tríade CID (Confidencialidade, Integridade e Disponibilidade). Eles englobam objetivos fundamentais de segurança para dados, informações e serviços de computação, como pode ser visto na Figura 1.

Figura 1. CID (Confidencialidade, Integridade e Disponibilidade)



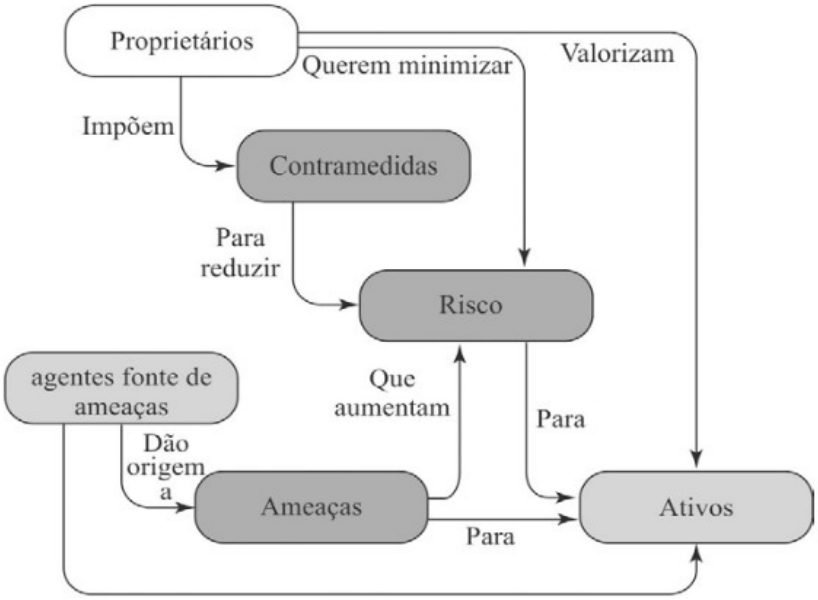
Fonte: Stallings (2014)

Além da tríade CID citada, Stallings (2014) ainda aponta conceitos adicionais recomendados por alguns profissionais da área de Segurança da Informação, que são:

- Autenticidade: Característica de genuinidade, verificabilidade e confiabilidade. Confiança atribuída à validade de uma transmissão, mensagem ou ao seu remetente, verificando se este remetente é realmente quem informa ser, validando que os dados que chegam ao sistema são de uma fonte confiável.
- Determinação de responsabilidade: O objetivo dessa característica é promover a capacidade de atribuir ações executadas às suas respectivas entidades executoras, através de registros de cada atividade executada. Isso garante que violações de segurança possam ser rastreadas até a entidade responsável.

A Figura 2 e o Quadro 2, detalham os conceitos e relações de segurança apresentados por Stalligs (2014) e a forma como eles estão relacionados no contexto da segurança da informação de um sistema.

Figura 2. Conceitos e relações de segurança



Fonte: Stallings (2014)

Quadro 1. Terminologias de Segurança de Computadores	
Terminologia	***Definição***
Adversário ou agente fonte de ameaça	Entidades que ameaçam ou atacam sistemas.
Ameaça	Potencial violação de segurança, ou seja, um possível perigo que pode explorar vulnerabilidades.
Ataque	Tentativa de violação por meio de técnicas ou métodos, visando burlar serviços e políticas de segurança.
Contramedida	Ação, dispositivo, procedimento ou técnica com o objetivo de reduzir ou aplicar ações corretivas às ameaças, vulnerabilidades ou ataques.
Política de Segurança	Conjunto de regras e práticas com o objetivo de regulamentar ou especificar como um sistema e organização devem proteger seus ativos.
Recursos de Sistema ou Ativos	Tudo que é de valor para a organização, ou seja, dados, serviços, capacidade de sistema, equipamento, instalações físicas.
Risco	Expectativa de perda de segurança ao uma ameaça explorar vulnerabilidades, podendo causar danos à organização e sistema.
Vulnerabilidade	Falha, defeito ou fraqueza que podem ser explorados com o objetivo de violar a política de segurança.

Estendendo estes conceitos, Hintzbergen *et al.* (2018) fazem a seguinte classificação:

Quadro 2. Definições e Conceitos de Segurança

Terminologia	***Definição***
Ação preventiva	Ação para eliminar potenciais causas de não conformidade ou situação indesejada.
Aceitação de Risco	Aceitar o risco, para posteriormente aplicar uma ação.
Ameaça	Potencial causa de um incidente, que pode gerar danos para um sistema ou organização.
Análise da Informação	Uma definição clara de como a organização trata a informação.
Análise de Riscos	Processo de compreensão do risco com o objetivo de determinar o seu nível, fornecendo a base para a estimativa de riscos e o seu tratamento.
Ataque	Ação com o objetivo de atingir ativos de um sistema ou organização, por meio de destruição, exposição, alterações não autorizadas, roubo, acesso não autorizado, etc.
Ativo	Tudo que há de valor para a organização, como instalações físicas, informação, *software*, equipamentos, pessoas, reputação, etc.
Autenticidade	Capacidade de uma organização comprovar ser quem realmente diz.
Avaliação do Risco	Identificação, análise e estimativa de risco
Confiabilidade	Capacidade de obter comportamentos e resultados desejados.
Confidencialidade	Capacidade de manter determinadas informações disponíveis apenas a pessoas, entidades ou processos autorizados.
Controle	Meios aplicados para o gerenciamento de risco, que incluem políticas, procedimentos, diretrizes e práticas ou estrutura organizacional.
Diretriz	Descrição do que deve e como ser feito para que se alcance os objetivos definidos nas políticas.
Disponibilidade	Capacidade de que uma informação esteja acessível sempre que requisitada.
Estimativa do Risco	Comparação de resultados provindos da análise de risco, determinando se este risco é aceitável ou tolerável.
Evento de Segurança da Informação	Indicativo de uma possível violação de uma Política de Segurança da Informação de um sistema, serviço ou rede.
Exposição	Exposição a prejuízos causados de um agente ameaçador.
Gerenciamento de Riscos	Atividades coordenadas que implementarão o

	controle do risco.
Gestão da Informação	Processo que define como a organização tratará a sua informação, definindo assim o valor dessa informação.
Gestão de Incidentes de Segurança da Informação	Processo que define como agir em casos de incidentes de segurança da informação.
Gestão de Segurança da Informação	Conjunto de atividades que farão o controle e implementação da Segurança da Informação em uma organização.
Identificação do Risco	Processo para definir os riscos, destacando causas, origem e consequências.
Incidente de Segurança da Informação	Um incidente é composto por um ou mais Eventos de Segurança da Informação.
Informação	Todo dado gerado e que apresente significado para o receptor.
Integridade	Capacidade de que uma informação seja alterada apenas por pessoas autorizadas.
Não repúdio	Provar a ocorrência e entidades de origem de eventos ou ações.
Política	Orientação formal expressa pela administração.
Procedimento	Especifica como conduzir atividade ou processo.
Processo	Conjunto de atividades que transformam entradas em saídas.
Processo de gerenciamento de riscos	Meio em que se aplicam políticas de gerenciamento, procedimentos e práticas relacionadas ao risco.
Responsabilidade	Ato de atribuir ações e decisões a uma entidade.
Risco	Combinação de análise e consequências de um evento. Também definido como o potencial de exploração de vulnerabilidades em ativos que causem danos à organização.
Risco Residual	Risco remanescente da análise de risco.
Segurança da Informação	Proteção da informação contra ameaças, preservando os pilares de segurança da informação CID (Confidencialidade, Integridade e Disponibilidade).
Sistema de Gerenciamento da Segurança da Informação (SGSI)	Parte do sistema de gerenciamento, incluindo estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.
Sistema de Informação	Uso da tecnologia da informação e a sua interação entre pessoas, processos e dados.
Tratamento de Riscos	Atividade para lidar com os riscos, ou seja, reduzir, eliminar ou prevenir que aconteçam.
Vulnerabilidade	O que pode ser explorado por uma ou mais ameaças.

3.1.1.1. Confidencialidade

A Confidencialidade define que a informação é de acesso apenas ao pessoal autorizado. Toda informação deve ser mantida confidencial enquanto armazenadas e transmitidas no ambiente da organização (HINTZBERGEN et al., 2018). Stallings (2014, p. 9) reforçam esse conceito definindo que “Uma perda de Confidencialidade consiste na revelação não autorizada de informações”.

Para Stallings (2014) a Confidencialidade abrange dois termos relacionados, sendo eles:

- Confidencialidade de dados: Garante que os dados estejam disponíveis apenas ao pessoal autorizado;
- Privacidade: Define aos envolvidos quais informações podem ser coletadas, a fonte da coleta e o destino dessas informações.

Hintzbergen *et al.* (2018) definem que a criptografia, o controle de acesso, a classificação de dados e o treinamento dos funcionários, deverão garantir que toda informação armazenada e transmitida esteja protegida. Os autores ainda destacam como medidas para garantir a Confidencialidade:

- Toda informação deve ser fornecida de acordo com a função desenvolvida pelo profissional. Nenhum profissional poderá acessar dados de outros departamentos.
- Nenhum material deve ser mantido em local de acesso comum a outros funcionários.
- Controle de acesso, garantindo que pessoas não autorizadas não tenham acesso a sistemas, base de dados, instalações da organização, etc.

3.1.1.2. Integridade

A integridade deve garantir que a informação não receba alterações não autorizadas, sejam por ataques, erros de usuário ou sistema. Qualquer violação de

dados é considerada como quebra de integridade de dados (HINTZBERGEN *et al.*, 2018).

Hintzbergen *et al.*, (2018) afirmam que uma informação pode estar correta, mas não possuir integridade. Isso indica que ela pode conter dados válidos, mas adulterados indevidamente.

Para Stallings (2014) a integridade abrange dois termos relacionados, sendo eles:

1. Integridade de dados: Os tipos de alterações realizadas devem estar previamente especificadas;
2. Integridade de sistemas: O sistema deve realizar sua função livre de alterações indevidas e não autorizadas.

Medidas como controle de acesso, detecção de intrusão e *hashing* são medidas destacadas por Hintzbergen *et al.*, (2018) como medidas de combate a ameaças à integridade.

3.1.1.3. Disponibilidade

A disponibilidade define que uma informação deve ser acessível sempre que requisitada. Elas se classificam seguindo as características descritas por Hintzbergen *et al.*, (2018):

- Oportunidade: Disponibilidade da informação;
- Continuidade: Capacidade de execução das atividades durante uma falha;
- Robustez: Capacidade de que toda a equipe tenha disponibilidade;

Quebra de disponibilidade é definido por Hintzbergen *et al.*, (2018, p. 29) como sendo “Qualquer atraso que exceda o nível de servido esperado para um sistema”. Sendo assim, qualquer caso que afete o acesso à informação é classificado como quebra de disponibilidade. Para exemplificar com mais detalhes:

- Falha de *hardware* e *software:* Defeitos em componentes de *hardware*, contaminação por vírus, falha de sistema operacional, atualizações de sistema não planejadas, condições do ambiente, etc;

- Ataques de negação de serviço: Conhecidos como *Denial-of-Service* (DoS), são ataques que visam sobrecarregar a rede de um sistema, enviando simultaneamente várias requisições, levando à instabilidade e queda;

Devem ser definidas ações de emergência que garantirão a recuperação em caso de falha (HINTZBERGEN *et al.*, 2018). Nos exemplos citados, as seguintes medidas podem ser recomendadas:

- Falha de *hardware* e *software*: *Backup*, armazenamento em nuvem ou em servidor são exemplos eficazes para proteção a esse tipo de falha. Caso algum equipamento seja danificado, nenhum dado é perdido e podem ser rapidamente substituídos. Lembrando que no caso de armazenamento em servidor, os dados devem receber *backup* da mesma forma e é recomendável que sejam separados fisicamente do local da organização. Hintzbergen *et al.*, (2018) ainda destacam que devem ser considerados requisitos legais quanto ao tempo de armazenamento de arquivos, que variam de acordo com o país.
- Ataques de negação de serviço ou *Denial of Service (DoS)*: É recomendável a implementação de medidas que filtrem o tráfego da rede. Localmente, com a instalação de *firewall* em cada máquina ou servidor, mas de forma mais ampla, com a utilização de serviços de *DNS (Domain Name System). DNS* é um protocolo que armazena nome de domínios e os associa ao seu respectivo número de *IP (Internet Protocol).* Essa associação é definida como tradução ou resolução, onde um endereço, por exemplo google.com, é traduzido para seu respectivo *IP*, abstraindo a necessidade de saber o endereço *IP* de cada site acessado (MITNICK, 2003).

3.1.2. Controle de Acesso

Controle de acesso é definido como quem ou quais processos terão acesso aos ativos, definindo ainda qual é o tipo de acesso. Controle de acesso ainda é apontado como o elemento central para a segurança de computadores, pois seu principal objetivo é garantir que acessos não autorizados não ocorram e que usuários legítimos obtenham acesso corretamente aos ativos (STALLINGS, 2014).

Para Stallings (2014), segurança física consiste em proteger ativos físicos, que são a base para o armazenamento e processamento de informações. Podendo ser ameaças:

- Ambientais: Desastres naturais e questões de ambiente, como aquecimento, ar-condicionado, fogo, fumaça, líquidos armazenados às proximidades de equipamentos; perigos químicos, radiológicos e biológicos; infestações, como insetos e mofo.
- Técnicas: Serviços de telecomunicações; energia elétrica; interferência eletromagnética.
- Causadas por seres humanos: Acesso físico não autorizado; roubo de equipamentos e dados; Vandalismo; Utilização indevida por funcionários, tanto os que não deveriam ter acesso, quanto aos que possuem, mas o fazem de forma indevida.

Ainda são destacados dois requisitos adicionais à segurança física por Stallings (2014):

- Prevenção de danos à infraestrutura: Equipamentos; ambiente físico em que se localizam os sistemas; serviços de energia elétrica, telecomunicações, equipamentos de aquecimento e ar-condicionado; Pessoal envolvido com a organização.
- Utilização indevida: Podendo ser acidental ou maliciosa, como roubo de equipamentos, documentos, serviços e acesso não autorizado a locais físicos.

Uma avaliação de riscos deve ser implementada, tanto para a segurança física, quanto para a lógica. Nessa etapa, deve-se determinar os recursos e sua alocação contra ameaças (STALLINGS, 2014).

A norma NBR 27002 (ABNT, 2013, p. 23), define que “[…] uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios”. Essa definição deve ser feita pelos proprietários dos ativos, associando os controles aos riscos de segurança da informação.

Estes requisitos garantem que a segurança seja implementada em sistemas de informação logo no início, evitando erros de projeto (HINTZBERGEN *et al.*, 2018).

3.1.3. Política de Segurança da Informação (PSI)

Stallings (2014, p. 28) define Política de Segurança como uma "[…] declaração formal de regras e práticas que especificam ou regulamentam como um sistema ou organização provê serviços de segurança para proteger ativos de sistema sensíveis e críticos". O autor ainda define que a primeira etapa para planejamento de serviços e mecanismos de segurança, é desenvolver uma política de segurança e que esta política deve ser cumprida pelos controles técnicos, gerenciais e operacionais.

Stallings (2014) afirma que ao desenvolver uma política de segurança, devem ser considerados os seguintes fatores e compromissos:

- Valor dos ativos;
- Vulnerabilidades;
- Ameaças em potencial e a probabilidade de ataques;
- Relação entre facilidade de uso e segurança: Mecanismos que afetem a facilidade de uso, por exemplo: mecanismos de controle de acesso e ferramentas de proteção que afetem desempenho de rede e equipamentos;
- Relação do custo de segurança com falha e recuperação: Além dos custos citados anteriormente, também os custos monetários necessários para implementação da segurança. Estes custos englobam valores dos ativos e os riscos.

Ao desenvolver políticas de segurança, a gerência deve sempre ter em mente e também transmitir aos demais colaboradores da organização, a importância da segurança da informação para a organização e que a contribuição de todos os colaboradores é essencial para que essa segurança seja efetiva (MITNICK, 2003).

Mitnick (2003) afirma que as políticas de segurança são as mais significativas ao combater ataques de engenharia social. O autor também destaca que o objetivo ideal dessas políticas é reduzir os riscos a níveis aceitáveis, apresentando ainda que

um programa de segurança abrangente, inclui inicialmente uma avaliação de riscos e que nessa etapa deve-se definir:

- Quais ativos precisam ser protegidos;
- Quais são as ameaças contra os ativos;
- Qual o dano à organização se essas ameaças se concretizarem.

O objetivo inicial da avaliação de riscos é classificar os ativos mais importantes, oferecendo e verificando se a proteção é eficaz com base em uma relação de custo/benefício. (MITNICK, 2003).

Hintzbergen *et al.* (2018) definem análise de riscos como um processo para entender o risco e definir o seu nível, fornecendo a base para a estimativa de risco e para as decisões de tratamento de risco.

Para Mitnick (2003), as políticas devem ser escritas de forma a serem compreendidas por profissionais de todas as áreas da organização, sem a utilização de termos técnicos e que essas políticas sejam de fácil acesso aos funcionários, por exemplo, por meio de *intranet* ou servidor de arquivos. Também é recomendado pelo autor a criação de um documento separado para os procedimentos, pois é provável que haja mais mudanças nas políticas que nos procedimentos.

Essas mudanças são destacadas por Mitnick (2003) ao salientar que a tecnologia está em constante evolução e as vulnerabilidades também acompanham essa evolução. Essas políticas devem passar por processos de avaliação e atualização.

Os empregados devem estar cientes de que o não-cumprimento das políticas e procedimentos tem consequências, que são definidas e divulgadas em forma de resumo. Também são recomendados programas de conscientização de segurança, destacando as políticas e o impacto que o não-cumprimento dessas políticas pode causar (MITNICK, 2003).

Por fim, Mitnick (2003) recomenda a aplicação de testes de penetração e avaliação de vulnerabilidades, aplicados periodicamente e devem ser informados aos funcionários sobre sua ocorrência. Esses testes usam meios de engenharia social, com o objetivo de expor pontos fracos relacionados ao treinamento ou ao não-cumprimento das políticas.

3.2. *Home Office* ou Teletrabalho

A Organização Internacional do Trabalho (2020) define que ambientes de trabalho *home office* ou Teletrabalho, são definidos na execução de atividades profissionais, fisicamente distante da organização. Isso se torna possível com a utilização de tecnologias de informação e comunicação como *smartphones*, *tablets*, computadores, etc.

Devido ao isolamento durante a pandemia de COVID-19 em 2020 e 2021, esse meio se tornou ainda mais popular, sendo apontado ainda pela Organização Internacional do Trabalho (2020) como fator decisivo de continuidade à economia.

A Confederação Nacional da Indústria (2020), destacou como cenário empresas espanholas, que optaram pela modalidade de teletrabalho ou *home office,* indicando 70% durante a pandemia, em um total de três milhões de trabalhadores.

Assim como descrito por Hintzbergen et al. (2018), a segurança sempre deve fazer parte do projeto ao desenvolver e comprar sistemas de informação. Recomenda-se aplicação logo no início, pois uma implementação posterior acarretaria em maior custo e em muitos casos na impossibilidade de aplicação devidos a erros de projeto.

4. METODOLOGIA

Este trabalho será realizado com pesquisa teórica, englobando conceitos, normas e técnicas de Segurança da Informação. Será realizada pesquisa bibliográfica, que de acordo com SILVA e MENEZES (2005, p. 21) é “[…] elaborada a partir de material já publicado, constituído principalmente de livros, artigos de periódicos e atualmente com material disponibilizado na Internet”.

A segunda parte será de listagem de vulnerabilidades, ameaças e riscos em ambientes *Home Office*, de forma a posteriormente definir os requisitos de segurança da informação.

A terceira parte será de definição dos requisitos de segurança da informação para ambientes *Home Office*. Conforme NBR 27002 (ABNT, 2013, p. xi), os requisitos de segurança da informação consistem em três principais fontes, sendo elas:

- Avaliação de riscos;
- Legislação vigente, estatutos, regulamentações e cláusulas contratuais e ambiente sociocultural;
- Conjuntos de princípios, objetivos e requisitos do negócio.

A quarta e última etapa consiste em englobar todos os conceitos pesquisados, onde a partir disso, será proposta uma Política de Segurança da Informação para ambientes *Home Office*.

5. CRONOGRAMA

Tabela 1. Cronograma de Atividades

ATIVIDADE	2021													
	Fev		Mar		Abr		Mai		Jun		Jul		Ago	
	1ª Quinzena	2ª Quinzena	1ª Quinzena	2ª Quinzena	1ª Quinzena	2ª Quinzena	1ª Quinzena	2ª Quinzena	1ª Quinzena	2ª Quinzena	1ª Quinzena	2ª Quinzena	ª Quinzena	2ª Quinzena
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
2	✓	✓	✓	✓	✓									
3									✓	✓				
4										✓	✓			
5												✓		

Fonte: Autor da pesquisa.

Atividades:

1. Pesquisa bibliográfica;
2. Pesquisa bibliográfica de conceitos de Segurança da Informação e PSI, junto às normas ISO/IEC e ABNT NBR ISO/IEC;
3. Estudo de ambiente *Home Office*, listando vulnerabilidades, ameaças e riscos;
4. Elaboração da proposta de PSI baseada no ambiente *Home Office*;
5. Aplicação da PSI em ambiente de trabalho *Home Office.*

6. RESULTADOS

6.1. Obtidos

A pesquisa realizada deixou mais claro tanto o cenário *home office,* quanto a necessidade da segurança da informação dentro de qualquer organização, bem como a importância do desenvolvimento, aplicação e conscientização para a utilização de Políticas de Segurança da Informação (PSI).

Com os conceitos aqui descritos, uma PSI pode ser desenvolvida visando ambientes de trabalho *home office*, garantindo a segurança da informação com a preservação da tríade CID descrita por Stallings (2014).

6.2. Esperados

O principal resultado esperado é que a proposta de Política de Segurança da Informação, possa ser implementada por profissionais que trabalhem em *Home Office,* de forma a garantir a Segurança da Informação nesse tipo de ambiente de trabalho.

Essa proposta visa a aplicação de conceitos, normas e técnicas, de forma a tratar ameaças à segurança, reduzindo-as a um nível aceitável de riscos, que são perigos que resultariam em acidentes, oriundos de ataques internos e externos (SOMMERVILLE, 2011).

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27001:2013: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.** 2013.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002:2013: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.** 2013.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27003:2020: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações.** 2020.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27004:2017: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação.** 2017.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27005:2019: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.** 2019.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27007:2018: Tecnologia da informação - Técnicas de segurança - Diretrizes para auditoria de sistemas de gestão da segurança da informação.** 2018.

ABNT – Associação Brasileira de Normas Técnicas. **ISO/IEC TS 27008:2019: Information technology -- Security techniques -- Guidelines for the assessment of information security controls.** 2019.

CNI - Portal da Indústria. **Teletrabalho no Brasil e no Mundo: Legislações Comparadas, Estudo de Relações do Trabalho**. Portal da Indústria, 2020. Disponível em:

<https://conexaotrabalho.portaldaindustria.com.br/publicacoes/detalhe/trabalhista/-geral/teletrabalho-no-brasil-e-no-mundo/>. Acesso em: 16 fev. 2021.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; HINTZBERGEN; SMULDERS, André; BAARS, Hans **Fundamentos de Segurança da Informação:** Com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Ed. BRASPORT, 2018.

ISO – Internacional Organization for Standardization. **ISO/IEC 27000: Information technology -- Security techniques - Information security management systems - Overview and vocabulary.** 2018.

ISO – Internacional Organization for Standardization. **ISO/IEC 27006:2015: Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.** 2015.

MARTELLO, Alexandro. **Home office no serviço público gerou economia de R$ 1 bilhão em 5 meses, diz governo federal**. G1, Seção Economia, 2020. Disponível em: <https://g1.globo.com/economia/noticia/2020/09/25/home-office-no-servico-publico-gerou-economia-de-r-1-bilhao-em-5-meses-diz-governo.ghtml>. Acesso em: 08 ago. 2020.

MITNICK, Kevin D. **A Arte de Enganar:** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Ed. Pearson Education, 2003.

MITNICK, Kevin D. **A Arte de Invadir:** As verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. São Paulo: Ed. Pearson Education, 2006.

OIT – Organização Internacional do Trabalho. **Teletrabalho durante e após a pandemia da COVID-19**. Organização Internacional do Trabalho, 2021. Disponível em: <https://www.ilo.org/brasilia/publicacoes/WCMS_772593/lang--pt/index.htm>. Acesso em: 29 mar. 2021.

PRESSMAN, Roger S. **Engenharia de Software:** Uma Abordagem Profissional. 7ª Ed. São Paulo: Bookman, 2011.

SILVA, E. L. da. MENEZES, E. M. **Metodologia Da Pesquisa e Elaboração de Dissertação**. 4. ed. rev. atual. Florianópolis: UFSC, 2005.

SOMMERVILLE, Ian. **Engenharia de Software**. 9ª Ed. São Paulo: Pearson Education, 2011.

STALLINGS, William. **Segurança de Computadores:** Princípios e Práticas. 2ª Ed. São Paulo: Pearson Education, 2014.