SEGURANÇA DA INFORMAÇÃO EMPRESARIAL

Amanda Engel OLIVEIRA[1]; Camila Eduarda AIO[1]; Giovana Gonçalves PINHEIRO[1]; Guilherme de MORAIS[2]

RESUMO:

O uso da tecnologia nas empresas cresce a cada dia, o que auxilia e ajuda nos trabalhos rotineiros com os dados obtidos. Contudo, prezar pela segurança dos dados é primordial. Neste artigo, pesquisas foram realizadas para coletar, apresentar e descrever sobre a Segurança da Informação Empresarial, além de um estudo de caso feito na Fundação Educacional de Fernandópolis, com o objetivo de mostrar como os dados estão seguros na instituição. Princípios fundamentais como, confiabilidade, integridade e disponibilidade devem ser essenciais em qualquer empresa.

PALAVRAS-CHAVE:

Segurança da Informação, empresas corporativas, confidencialidade, integridade, disponibilidade.

ABSTRACT:

The use of technology in companies grows every day, which helps and helps in routine work with the data obtained. However, valuing data security is paramount. In this article, research was carried out to collect, present and describe about Corporate Information Security, in addition to a case study carried out at the Fundação Educacional de Fernandópolis, with the objective of showing how the data are safe in the institution. Fundamental principles such as reliability, integrity and availability should be essential in any company.

KEYWORDS:

Information security, corporate companies, confidentiality, integrity, availability.

[1]Acadêmicos do 4º Ano do Curso de Graduação em Sistemas de Informação das Faculdades Integradas de Fernandópolis – FIFE-FEF, Fernandópolis-SP.
[2] Mestre em Ciências Ambientais, Professor do Curso de Graduação em Sistemas de Informação das Faculdades Integradas de Fernandópolis – FIFE-FEF, Fernandópolis-SP.

1. Introdução

Com o constante crescimento da tecnologia da informação, consequentemente, tem com ele um grande obstáculo, o aumento exponencial na quantidade de ataques e vazamentos de monopólios de dados, ocasionando altos prejuízos para as organizações; assim como desvantagens em relação aos concorrentes

Armazenar informações em épocas passadas era mais simples do que nos dias atuais, tais eram guardadas em caixas e/ou gavetas, nas quais se localizavam em locais físicos de acesso restrito. Com o avanço tecnológico, os computadores pessoais e redes que conectam o mundo todo, tornaram a tarefa de administrar essas mais difícil (BRASIL, 2012).

Sabe-se que a informação é essencial no mundo atual, principalmente, nas empresas, pois essas utilizam da mesma para tomadas de decisões. À vista disso, torna-se essencial que cada organização possua uma política de segurança da informação, com regras, métodos e procedimentos bem definidos, com objetivo de proteger dados da empresa e *stakeholders*[3] a ela inerente. Para obter uma boa segurança de informação, não basta apenas buscar soluções para reduzir ou conter possíveis ameaças físicas, mas também as virtuais (BRASIL, 2012).

Segundo Pinheiro e Silva (2019), o motivo dos crescentes ataques cibernéticos é explícito, as organizações querem acompanhar o avanço tecnológico, contudo deixam de lado ou então dão pouca importância as boas práticas de assegurarem as informações. Pode-se citar com destaque as técnicas de *phishing*[4] que roubam dados de usuários, ataques em massas a bancos, órgãos governamentais e empresas grandes de tecnologia, esses são os casos mais comuns que acontecem frequentemente.

Segurança da Informação é definida de diversas formas por variados autores. Para Ferreira (2003, p.162), a Segurança da Informação, “Protege a informação de diversos tipos de ataques que surgem no ambiente organizacional, garante a continuidade dos negócios, reduz as perdas e maximiza o retorno dos investimentos e das oportunidades”.

Aos aspectos atinentes à Segurança da Informação, de fato as informações são os pilares de todo conhecimento de uma organização. Essas informações, por sua relevância passaram a

[3] *Stackholders*: Expressão inglesa que significa, indivíduos e organizações impactados pelas ações da sua empresa.
[4] *Phishing*: Expressão inglesa que significa "pescando". Ataque que “pesca”, rouba dinheiro ou identidade revelando informações pessoais, em forma de um email falso, que contém um link para um site de phishing.

serem muito almejadas, resultando em ataques constantes. Diante desse fato, pode-se citar, que está em vigor a Lei 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI), visando regular o acesso a informações públicas presentes nas três esferas de poder, federal, estadual e municipal (LIMA, 2018).

Assim como é direito do cidadão ter acesso a informações públicas referentes ao governo, o mesmo também tem o direito de ter seus dados mantidos em segurança, quando fornecidos para uma empresa. A Lei que visa essa proteção é a Lei Geral de Proteção de Dados.

Baseada no Regulamento Geral de Proteção de Dados (RGPG), a Lei Geral de Proteção de Dados Brasileira (LGPD), Lei nº13.709, foi aprovada no Brasil em 14 de agosto de 2018, que dispõe:

> Sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018 Lei n°13.709, Art. 1º)

De acordo com Barbosa *et al*. (2021), devido a quarentena exigida pela COVID-19, as organizações necessitaram adaptar-se rapidamente a proteção de dados e segurança da informação. Sucedeu que adaptações fossem realizadas para que os trabalhos acontecessem remotamente, o que causou um arranjo pessoal nas empresas, além de dispositivos e equipamentos, causando aumento de ataques constantes.

Ante o exposto e, de acordo com dados da pesquisa realizada por Bohler *et al* (2020), o trabalho *home-office*[5] já era tendência, após o início da pandemia do COVID-19, a modalidade ganhou ainda mais destaque no mundo todo. Contudo, aumenta se a preocupação com os dados e informações que trafegam entre redes e *hardware*[6] dos colaboradores, uma vez que com o trabalho remoto, muitos ainda não possuem equipamentos com a proteção necessária, o que resulta em utilização de *softwares*[7] piratas, uns dos maiores vilões de roubo de dados.

Toda empresa que procura manter seus dados seguros, deve seguir normas que são conhecidas como *International Organization for Standardization*[8] (ISO), essas foram criadas

[5] Home-office: Expressão inglesa que significa “escritório em casa”.
[6] *Hardware*: Expressão inglesa que significa “equipamentos” ou as partes físicas de uma máquina são chamadas de hardware.
[7] *Softwares*: Expressão inglesa que significa “programa” e executa uma sequência de instruções para realizar tarefas.
[8] *International Organization for Standardization*: Organização Internacional para Padronização.

pela Organização Internacional de Padronização para que as regras sejam seguidas com padrão internacional em divergentes áreas de gestão. As normas que serão abordadas nessa pesquisa, são da família 27000, as quais estabelecem regras de políticas, planejamentos, responsabilidades, processos e práticas de como proteger os dados da organização, certificando e provando aos clientes e fornecedores que se preocupam com a segurança da informação (PEDRA, 2022).

Visando as informações supracitadas, o objetivo dessa pesquisa é apresentar a importância da política de segurança das informações nas empresas, por meio de boas práticas de segurança. Essas práticas envolvem não somente profissionais de Tecnologia da Informação (TI) especializados em segurança da informação, mas também dirigentes, colaboradores e usuários que se preocupam em proteger o patrimônio da organização.

2. Objetivos

O objetivo apresenta a ideia central do artigo: segurança da informação, descrevendo a sua finalidade, conceitos e passos para atingir uma boa segurança dos dados nas empresas.

2.1. Objetivo Geral

De acordo com informações já citadas, apresenta-se a importância da política de segurança das informações nas empresas, por meio de boas práticas de segurança. Envolve não somente profissionais de Tecnologia da Informação (TI) especializados em segurança da informação, mas também dirigentes, colaboradores e usuários que se preocupam em proteger o patrimônio da organização.

Apresentar a importância da política de segurança das informações nas empresas, por meio de boas práticas de segurança. Essas práticas envolvem não somente profissionais de Tecnologia da Informação (TI) especializados em segurança da informação, mas também dirigentes, colaboradores e usuários que se preocupam em proteger o patrimônio da organização.

2.2. Objetivos Específicos

Realizar pesquisas e coletar informações em fonte bibliográficas, artigos acadêmicos e normas, leis e fatos abordados.

Analisar e explicar o conteúdo referente a Segurança da Informação nas organizações.

Apresentar variados tipos de ataques e suas consequências, interpretando o funcionamento das falhas, em virtude de abordar a necessidade de boas técnicas de segurança e seu uso no ambiente individual.

3. Justificativa

Em função da grande importância da segurança da informação na sociedade atual, a presente pesquisa realizada proporcionará informações pertinentes para uma melhor compreensão da necessidade e vantagens da adoção de práticas de políticas de segurança e, também, informar os riscos que a falta dessas práticas pode provocar as organizações e aos usuários.

Portanto, conscientizará e conduzirá entidades a buscar proteção de seus dados e informações armazenadas de pessoas mal intencionadas, realçando as possíveis consequências que existem sem a adoção dessas medidas protetivas.

4. Desenvolvimento Teórico

O desenvolvimento explicará de forma abrangente e objetiva sobre os fundamentos teóricos da segurança da informação, leis, normas e sua importância nas organizações. Também abordará sobre o processo detalhado da análise de riscos das vulnerabilidades definidas e ameaças, com o intuito de instruir em como adquirir mecanismos para evitar ataques e, consequentemente, impactos.

4.1. Classificação da Informação

Para Fontes (2017), "a informação, independentemente de seu formato, é um ativo importante da organização".

> (...) por isso, os ambientes e os equipamentos utilizados para o processamento, seu armazenamento e sua transmissão devem ser protegidos. A informação tem valor para a organização (FONTES, 2017).

Reis, Mota, Oliveira (2022, p. 01), destacam que "a classificação da informação é fundamental para que as organizações possam direcionar os seus recursos para sistemas de segurança".

Assim, os diversos procedimentos são adotados com o intuito de que, seja garantido a segurança da informação, desempenhando os processos adequados próximo de cada tipo de necessidade, direcionando os critérios e práticas relevantes. O fato é que para implementar isso é imprescindível conhecer a importância das informações recebidas, utilizadas e armazenadas

pela organização. Dessa forma, se faz necessário a classificação das informações, visando facilitar o trabalho de segurança, definindo o nível que deve ser utilizado no armazenamento.

Com o propósito de uniformizar a discussão no âmbito deste trabalho, exerce realizar a classificação da informação, sendo que, essa deve-se muito mais a uma necessidade de diferenciação para termos práticos das regras voltadas à segurança. Portanto, é importante ressaltar que é descrita em um documento próprio.

De acordo com Lima (2018), um documento trará as classificações das seguintes formas:

> Informação secreta, não são todos que têm autoridade para julgar uma informação secreta. Essa prerrogativa só cabe ao Conselho Diretor, ao Conselho Fiscal, ao diretor-presidente, ao diretor-superintendente e aos demais diretores; informação reserva, para classificar uma informação como reservada, além das autoridades que podem julgá-las secretas, são acrescidos os ocupantes de cargos gerenciais; informação corporativa, essa classificação pode ser feita por qualquer empregado do Serpro lotado na empresa; informação corporativa-legal, qualquer empregado do Serpro lotado em unidade que manipule dados de cliente da empresa tem competência para utilizar esta classificação (LIMA, 2018).

Em conformidade com Reis, Mota, Oliveira (2022, p. 09), com uma boa classificação das informações, a organização:

> (...) poderá conhecer melhor os seus processos, pois se verá forçada a fazer um inventário das informações, poderá também conhecer as informações que precisa disponibilizar para seus clientes e que ainda não têm um canal apropriado para isso (REIS; MOTA; OLIVEIRA, 2022, p.09).

Conclui-se que, para que a segurança da informação e sua classificação seja possível, é necessária a elaboração de políticas específicas das quais é imprescindível entender a importância da informação, a seguir é apresentada uma definição da mesma.

4.2. A importância da Informação

A evolução da tecnologia está cada vez maior, consequentemente, a informação se torna um dos maiores e mais importantes bens da empresa. Segundo Ramos (2008, p. 287), a informação deve ser entendida como:

> (...) todo patrimônio que se refere à cultura da empresa ou ao seu negócio, podendo tais informações ser de caráter comercial, técnico, financeiro, legal, de recursos humanos, ou de qualquer natureza, que tenha valor para organização e que se encontrem armazenadas em recursos computacionais da empresa, com tráfego dentro da sua infraestrutura tecnológica (RAMOS, 2008, p. 287).

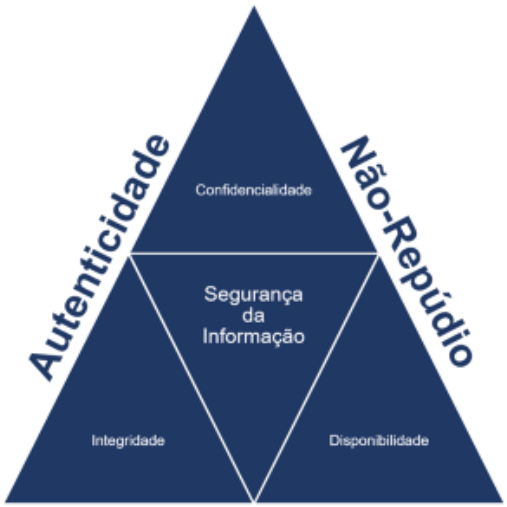
Nos últimos anos, a forma como uma empresa organiza e controla suas informações atualiza-se a cada dia. Em tempos passados, ficavam mantidas em papéis e guardadas em caixas ou pastas. Com o crescimento empresarial e as atividades se tornando mais complexas, surge a necessidade de automatizar e facilitar o processo de gestão de armazenamento das informações.

Com o intuito de melhorar ainda mais a organização, o controle e o planejamento, surgiu-se a área da Segurança de Informação. Essa abrange desde a entrada, processamento e armazenamento da informação e, se necessário, recuperação de dados.

4.3. Conceitos e Objetivos da Segurança da Informação

Segurança da Informação conforme definido pela ISO/IEC 17799 (2001, p. 2) "é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades". É caracterizada pela preservação dos seguintes três princípios básicos (ISO/IEC 17799, 2001, p. 4).

Figura 1 – Os princípios básicos da segurança da informação.



Fonte: PISA, Adriana, (2020)

A Figura 1 representa a tríade CID em que define: confidencialidade: garantia do acesso à informação somente por pessoas autorizadas; integridade: garantia de que a informação acessada é confiável, completa e permanente; disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes quando necessário.

É importante destacar que a ISO/IEC 17799 (2001, p. 2) informa que a "Segurança da Informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software*". Tais controles citados na norma, devem ser estabelecidos de forma clara e organizada para assegurar que os objetivos da segurança da informação sejam alcançados.

Sabe-se que a expectativa das organizações é de que as informações armazenadas em seu sistema computacional permaneçam lá, sem invasões de pessoas não autorizadas. Essas expectativas citadas são referentes aos objetivos gerais da segurança da informação.

Além dos princípios já citados anteriormente, de acordo com Figueirêdo (2002, p. 4), destacam-se: legalidade - estado legal da informação, conforme os preceitos da legislação em vigor; consistência – garantia de que o sistema atua de acordo com a expectativa dos usuários; auditoria – garantia da proteção contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, é usado trilhas de auditorias e *logs*[9], que registram o que foi executado no sistema, quem executou e quando.

Existem muitas pessoas que são focadas em buscar meios de invasão as barreiras de segurança de sistemas. Um exemplo que se pode citar, é a invasão que houve no sistema de informática do Ministério da Saúde em 2022, chamada de *ransomware*[10], em que um grupo de *crackers*[11] roubou os dados do aplicativo ConecteSus (SOUZA, 2022).

Diante disso, tem como principal objetivo conter as vulnerabilidades em três aspectos: falta de preparo pessoal, falhas na rede e falhas nos programas. É de extrema importância que a organização contrate um profissional de segurança, ele deverá saber identificar e informar as falhas independente de seu aspecto para evitar ataques e impactos. Com essa identificação, torna-se mais fácil corrigi-las e trabalhar a fonte para não repetir os mesmos problemas.

4.4. Vulnerabilidades, Ameaças, Ataques, Análise de Riscos e Impactos

Para garantir os objetivos citados anteriormente, é necessário entender o conceito dos principais problemas, suas causas e consequências, pois permanecendo dispersos nos ambientes organizacionais, os ativos da informação estão sujeitos a diversos eventos e potencialidades nocivos à sua segurança, divididos em quatro categorias: vulnerabilidades, ameaças, ataques e impactos, os quais compõem e caracterizam os riscos.

---

[9] *Logs* - Em computação, *log* de dados é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional.
[10] *Ransomware* - Tipo de *malware* de sequestro de dados, feito por meio de criptografia.
[11] *Cracker* - indivíduo que pratica a quebra de um sistema de segurança de forma ilegal ou sem ética.

4.4.1. Vulnerabilidade

Tendo em vista que, a segurança da informação tem como princípio a manutenção da confidencialidade, da integridade e da disponibilidade das informações, qualquer uma destas três propriedades não deve ser violada de maneira alguma. Desta forma, cada vulnerabilidade existente pode permitir a ocorrência de determinados incidentes de segurança.

> "(…) fraqueza de um sistema informático, revelada por um exame à sua segurança (por exemplo, devido a falhas na análise, conceção, implementação ou operação), que se traduz por uma incapacidade de fazer frente às ameaças informáticas que pesam sobre ele" (COIMBRA, 2018, p. 5 *apud* CNCS, 2017).

Do mesmo modo, Marciano (2006, p. 51) afirma que:

> (...) representa um ponto potencial de falha, ou seja, um elemento relacionado à informação que é passível de ser explorado por alguma ameaça - pode ser um servidor ou sistema computacional, uma instalação física ou, ainda, um usuário ou um gestor de informações consideradas sensíveis (...)

Nesse sentido, dada a incerteza associada aos ativos e às vulnerabilidades Silva, Carvalho, Torres (2003) afirma que, "a identificação das vulnerabilidades permite calcular a probabilidade da realização das ameaças à empresa". Segundo Laureano (2005, p. 07) "todos os ambientes são vulneráveis, partindo do princípio de que não existem ambientes totalmente seguros. Muitas vezes, encontramos vulnerabilidades nas medidas implementadas pela empresa". Laureano (2005, p. 07) ainda diz que, a identificação das vulnerabilidades, ajuda na identificação de medidas de segurança adequadas.

Nas palavras de Ferreira (2017, p. 05) a exploração de vulnerabilidade é:

> (...) uma técnica muito difundida e bastante explorada por indivíduos maliciosos. Existem ainda inúmeros portais, sites e sistemas especializados em procurar e divulgar estas vulnerabilidades. Sendo assim, a gestão de vulnerabilidade tornou-se uma necessidade no processo de gestão de segurança da informação.

A vulnerabilidade, exclusivamente, não pode ser considerada um incidente, pois trata-se de um elemento passivo, necessitando para tanto de um agente causador ou de condição favorável, para tornar-se uma ameaça.

Sendo assim, em concordância anteriormente, quando uma vulnerabilidade é explorada de forma intencional ou mesmo acidental por um elemento interno ou estranho. Sendo assim, há uma ameaça.

4.4.2. Ameaças

Segundo Galvão (2015, p. 19), entende-se por ameaça, todo e qualquer aspecto capaz de causar problemas, de forma que prejudique a empresa, sejam elas naturais (causadas por fenômenos da natureza, como tempestades, incêndios, entre outros), ou não. Com outras palavras, se a informação armazenada sofre qualquer tipo de risco e, consequentemente os negócios deterioram-se, há uma plausível ameaça.

As ameaças são divididas em categorias, baseadas na tríade da segurança da informação, confidencialidade, disponibilidade e integridade. De acordo com Galvão (2015, p. 19), as categorias são: perda de confidencialidade – quando a ameaça causa a exposição de informações confidenciais a pessoas não autorizadas; perda de disponibilidade – quando a ameaça impede o acesso das informações para pessoas autorizadas; perda de integridade - quando a ameaça permite a manipulação da informação por pessoas não autorizadas.

De forma básica e complementar, as ameaças ainda possuem mais duas categorias referentes a integridade. Ameaças passivas ocorrem, normalmente por *hackers*[12], os quais desejam apenas acessar as informações e não as alterar, somente observar. Em contraposição, as ameaças ativas ocorrem quando as informações sofrem modificações, geralmente realizadas por *crackers* (GALVÃO, 2015, p. 19). Contudo, após ameaças não resolvidas, as informações ficam sujeitas a ataques, causando prejuízos para a empresa.

4.4.3. Ataques

No contexto atual, conforme afirma Domingos (2018, p. 51) "(...) um ataque corresponde à concretização de uma ameaça, não necessariamente bem-sucedida (do ponto de vista do atacante), mediante uma ação deliberada e por vezes meticulosamente planejada".

Nesse sentido, Laureano (2005, p. 16) afirma que "o ataque é o ato de tentar desviar dos controles de segurança de um sistema de forma a quebrar os princípios". De maneira geral, passa por quatro processos, reconhecimento – o invasor reconhece um potencial entrada no sistema; análise - avalia a possibilidade de ataque e quais ferramentas para tal; adaptação - a segurança está em risco e os dados no mesmo podem ser acessados remotamente; execução - o invasor tem acesso a todas as informações que deseja, bem como alterar e deletar dados e informações.

[12] *Hacker* - Indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores.

Ainda assim, a segurança é um conjunto de procedimentos que ajudam a proteger os dados armazenados e que são transmitidos por meio das redes de comunicação, como a internet.

Conforme afirma Laureano (2005, p. 16), para a implementação de medidas de segurança, torna-se necessário classificar as possíveis formas de ataques em sistemas:

> interseção – baseia-se no acesso a informações por pessoas não autorizadas; interrupção – consiste na interrupção do fluxo normal das mensagens da origem até ao destino; modificação – procede na modificação ou transformação por pessoas não autorizadas, violando, deste modo, a integridade da mensagem; personificação – resulta no acesso não autorizado de pessoas que enviam mensagens fazendo-se passar por uma pessoa autorizada (LAUREANO, 2005, P. 16).

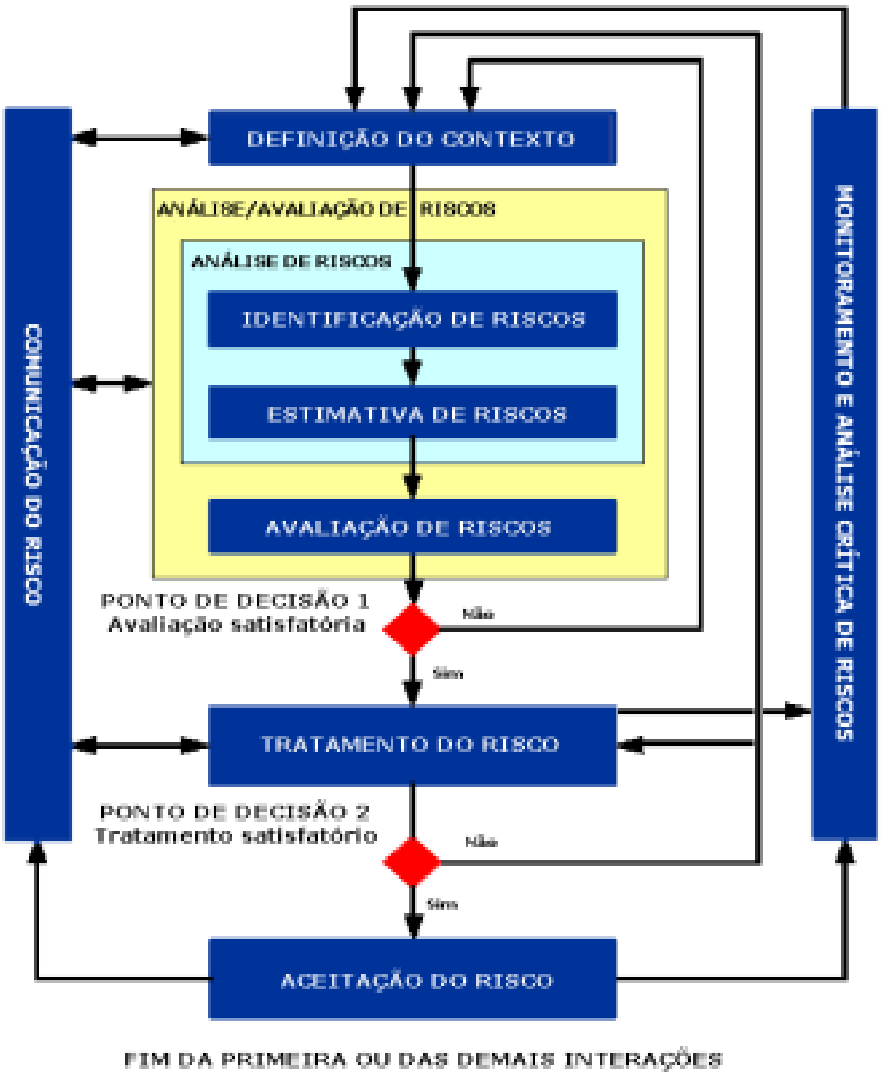
Diante disso, entende-se que a ameaça é um potencial comprometimento da Segurança da Informação, seja ele acidental ou deliberado, e por vulnerabilidade a existência de uma fraqueza ou a falta de controle do sistema, que poderá permitir ou facilitar a atuação de ameaça (COIMBRA, 2018 *apud* CEMFA, 2008). Do mesmo modo, Coimbra (2018, p. 6) ressalta que "uma ameaça pode explorar acidentalmente ou propositadamente uma determinada vulnerabilidade e pode ter origem interna ou externa, estando diretamente relacionada com a perda de um dos seus princípios".

4.4.4. Análise de Riscos

A análise de riscos procura identificar e avaliar as falhas e vulnerabilidades que podem expor informações da organização a ameaças e aos impactos negativos causados aos negócios. Dias (2000, p. 54) afirma que o "risco é uma combinação de componentes, tais como ameaças, vulnerabilidades e impactos". Os riscos não podem ser totalmente eliminados, mas podem ser reduzidos a partir de medidas de segurança bem estabelecidas.

A norma NBR ISO/IEC 27005:2011 define um processo de gestão de riscos composto de seis fases: estabelecimento do contexto, processo de avaliação de riscos, tratamento do risco, aceitação do risco, comunicação e consulta do risco e monitoramento e análise crítica de riscos que são representadas na figura 2.

Figura 2: Processo de gestão de riscos da ISO/IEC 27005:2011



Fonte: Araújo; Neto Mascarenas, (2019, p. 47)

O processo começa com a definição do contexto, no qual são definidos os critérios e o escopo. Após essa etapa, os riscos são identificados, estimados e avaliados. No final dessa etapa, surge o primeiro ponto de decisão, se a avaliação do retorno for não, o processo deverá ser repetido até que os resultados sejam satisfatórios (ARAÚJO; NETO MASCARENAS, 2019, p. 48).

Próxima etapa é a realização do tratamento dos riscos, em que podem ser reduzidos, evitados, transferidos, mas também, reavaliados pela empresa. A fase de aceitação do risco é onde a organização deverá realizar o aceite dos riscos, e deverão ser avaliados e documentados. A etapa de comunicação é um conjunto de atividades que devem ser executadas continuamente entre os *stakeholders* da organização. Na fase de monitoramento e de revisão do risco, será

identificado mudanças no contexto da organização, a fim de atualizar e melhorar o processo da gestão (ARAÚJO; NETO MASCARENAS, 2019, p. 48)

A fase da análise dos riscos é realizada de forma quantitativa - definem o impacto, a probabilidade e o nível de risco por qualificadores como “alto”, “médio” e “baixo”; ou qualitativa - proporciona estimativas numéricas (RUPPENTHAL, 2013, p. 37).

Dantas (2011, p. 55) afirma que:

> A análise qualitativa é geralmente utilizada quando não existe a disponibilidade de dados, ou quando eles são precários, e a sua análise é realizada com base em valores referenciais. A análise quantitativa é utilizada quando os dados são confiáveis e estão disponíveis, e a sua análise é realizada com base em valores absolutos.

É imprescindível que os riscos estejam bem definidos e documentados. Desta forma, poderão ser reduzidos e, consequentemente, a chance de ocorrer impactos na organização também.

4.4.5. Impactos

Para Dias (2000, p. 57) “a análise de impactos identifica os recursos críticos do sistema, isto é, recursos que mais sofrerão impactos na ocorrência de uma quebra de segurança”. Em vista disso, é necessário fazer a análise dos impactos para poder identificar e classificá-los conforme sua importância na organização, com objetivo de evitá-los e também, se necessário, recuperar informações de forma ágil.

Existem dois aspectos em que os impactos são enquadrados para ser analisados que são: a curto prazo e a longo prazo, ambos são determinados a partir do tempo que se mantém afetando a organização. Dentro dessa ótica, os impactos podem ser classificados em uma escala de 0 a 5 conforme apresentado na tabela 1 elaborada pelos autores.

Tabela 1 – Classificação dos Impactos

ESCALA DO IMPACTO	IMPACTO
0	Impacto irrelevante.
1	Efeito pouco significativo, sem afetar a maioria dos processos de negócios da instituição.
2	Sistemas não disponíveis por um determinado período de tempo, podendo causar perda de credibilidade junto aos clientes e perdas financeiras.
3	Perdas financeiras de maior vulto e perda de cliente para a concorrência.
4	Efeitos desastrosos, porém, sem comprometer a sobrevivência da instituição.
5	Efeitos desastrosos, comprometendo a sobrevivência da instituição.

Fonte: Elaborado pelos autores, 2022.

Além do nível de impacto, podem ser definidos vários tipos de impactos intrinsecamente relacionados aos negócios da instituição que devem ser definidos pelas pessoas que mais os conhecem. Na tabela 2, elaborada pelos autores, está descrito a classificação dos tipos de impactos e suas descrições.

Tabela 2 – Tipos de Impactos

TIPO	DESCRIÇÃO
01	Modificação de dados
02	Sistemas vitais não disponíveis
03	Divulgação de informações confidenciais
04	Fraude
05	Perda de credibilidade
06	Possibilidade de processo legal contra a constituição
07	Perda de clientes para concorrência

Fonte: Elaborado pelos autores, 2022.

As probabilidades de risco também podem ser distribuídas em uma escala de 0 a 5 conforme tabela 3 elaborada pelos autores.

Tabela 3 – Probabilidade de Risco

TIPO	PROBABILIDADE
0	Ameaça completamente improvável de ocorrer.
1	Probabilidade de a ameaça ocorrer menos de uma vez por ano.
2	Probabilidade de a ameaça ocorrer pelo menos uma vez por ano.
3	Probabilidade de a ameaça ocorrer pelo menos uma vez por mês.
4	Probabilidade de a ameaça ocorrer pelo menos uma vez por semana.
5	Probabilidade de a ameaça ocorrer diariamente.

Fonte: Elaborado pelos autores, 2022.

Dias (2000, p.114) classifica os impactos, em termos administrativos como: diretos - são aqueles que envolvem perdas financeiras (reposição ou reparação de equipamentos, por exemplo), diminuição da receita, aumento de custos ou penalidades financeiras pelo descumprimento de contratos; indiretos - são aqueles que não envolvem diretamente perdas financeiras, mas podem originá-las. Nessa categoria, encontra-se a perda da reputação e credibilidade no mercado, os conflitos com acionistas, políticos, sindicatos etc.

A verificação das vulnerabilidades, ameaças, ataques e impactos, é necessária para determinar quais medidas deverão ser implementadas pela organização por meio de políticas de segurança da informação.

4.4.5.1. Estudo de Caso

A partir da classificação dos impactos, tipos de impactos e suas probabilidades é feito a matriz de relacionamento. Essa é uma ferramenta de gerenciamento, que serve para identificar e determinar o tamanho de um risco e possibilitar as ações de impedimento ou controle (LEC, 2020).

O estudo de caso referente as possibilidades de riscos, foi realizado na Fundação Educacional de Fernandópolis (FEF), um dos maiores polos universitários da região noroeste do estado de São Paulo, localizada em Fernandópolis, Avenida Theotonio Vilela, Nº 1685, Campus Universitário, 15.608-380.

A faculdade possui um grande volume de dados gerados diariamente e protegê-los é dever da instituição. Para isso, riscos devem ser calculados, considerando a probabilidade de ocorrer, assim como os tipos e graus de impactos, conforme apresenta a tabela 4, elaborada pelos autores.

Tabela 4 – Matriz de Relacionamento Fundação Educacional de Fernandópolis

AMEAÇAS GENÉRICAS	TIPOS IMPACTO	IMPACTO 0-5	PROBABILIDADE 0-5
INSTALAÇÃO DE HARDWARE E SOFTWARE NÃO AUTORIZADO	6	2	1
AMEAÇA PROGRAMADA (VÍRUS, BOMBAS LÓGICAS)	3	4	3
BUGS DO SISTEMA OPERACIONAL.	2	2	5
QUEDA DE ENERGIA	2	1	5
AMEAÇAS NÃO PROGRAMADAS (CRACKERS)	1	5	3
FALTA DE INTERNET	2	2	4
MAL FUNCIONAMENTO DO PORTAL EDUCACIONAL	7	3	1
DESASTRES NATURAIS	5 - 6	5	1
FALHA NO SERVIDOR	2	5	1
FALHAS RELACIONADAS À CONFIDENCIALIDADE	3 - 6	5	0

Fonte: Elaborado pelos autores, 2022.

4.5. Política da Segurança da Informação

As políticas de segurança da informação são apresentadas como códigos de conduta, aos quais os usuários dos sistemas devem-se adequar integralmente, além de expressar a

verdade, sendo viável para implementação. Logo, é imprescindível que em nível estratégico e entre outras políticas agregadas a mesma, bem como documentos e normas, estejam ligadas ao objetivo principal da organização. Sendo assim, a possibilidade de uma implementação real e de execução é necessária. Os regulamentos têm como objetivo fazer com que o uso da informação na organização realiza-se de uma forma estruturada, possibilitando que não seja prejudicada por mau uso.

A formulação e aplicação de Políticas de Segurança da Informação tem atingido um amplo escopo de organizações. Marciano (2006, p.6) afirma que:

> As políticas de segurança da informação devem contemplar o adequado equilíbrio dos aspectos humanos e técnicos da segurança da informação, em contraposição aos modelos de políticas atuais, extremamente voltados às questões tecnológicas.

Pragmaticamente, cada vez mais empresas buscam a aderência a padrões internacionais ou nacionais de segurança, mesmo que advindos de fóruns externos. Porém, deve-se salientar, ainda, que a adequação aos padrões, principalmente os internacionais, é necessária, mas é essencial o alinhamento aos processos e ao contexto da organização bem como a preocupação com a clareza dos termos empregados e a proximidade com as situações vivenciadas no ambiente organizacional (HÖNE; ELOFF, 2002).

Evidenciando a todos que acessam a informação, toda empresa tem como obrigação assegurar a proteção contra perdas, danos, destruição/mau uso. Segundo Fontes (2017), proteger a informação é responsabilidade de cada pessoa na organização, independentemente de seu nível hierárquico.

Convém lembrar os princípios que a, Organização para a Cooperação e Desenvolvimento Econômico (OCDE), apresenta para o desenvolvimento de uma cultura de segurança da informação (OCDE, 2002): vigilância; responsabilidade; participação; ética; democracia; avaliação de risco; delineamento e implementação da segurança; gestão da segurança; reavaliação.

Assim, de acordo com Lima (2018 *apud* Baloni, 2007) "após a implementação da política, devem ser implementadas algumas ações que levam ao conhecimento dos usuários", sendo necessário, a existência de divulgação ampla, geral e irrestrita; acesso coerente a essa política; processo que, garanta que a política e os demais regulamentos estejam sempre atualizados. Deste modo, ao levar conhecimento ao usuário, o mesmo tem papéis e responsabilidades a serem desempenhados.

4.6. Papéis e Responsabilidades

Todo e qualquer ativo e/ou processo devem ser atribuídos a pessoas (HINTZBERGEN *et al*, 2018, p. 70). Assim, mapeando os papeis e responsabilidades colabora para a segurança da informação. Conforme afirma Jhonnye (2022, p. 6) "Organizações precisam estabelecer uma estrutura de gerenciamento de risco da segurança da informação para definir, explicitamente, o que se espera de cada indivíduo". Desta forma, a mesma tem o compromisso de nomear encarregado para cada ativo, tornando-se responsável por uma operação diária, evitando assim a chance de alteração não autorizadas, não intencionais, ou uso indevido dos ativos da organização.

Nas palavras de Jhonnye (2022, p. 5):

> A norma ABNT NBR ISO/ IEC 27005 (2008) estabelece que dentre os principais papéis e responsabilidades da organização para gestão de riscos de segurança da informação está a identificação e análise das partes interessadas e o estabelecimento das relações necessárias entre a organização e as partes interessadas, das interfaces com as funções de alto nível de gestão de riscos da organização (por exemplo: a gestão de riscos operacionais), assim como as interfaces com outros projetos ou atividades relevantes.

Portanto, para que seja atingida é compromisso de todos os usuários quanto à aplicação das normas e procedimentos estabelecidos.

4.7. Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) é baseada no Regulamento Geral de Proteção de Dados da União Europeia (RGPD). De acordo com Piurcosky *et al* (2019, p. 90), a RGPD dá aos proprietários dos dados acesso direto total aos seus dados, além de maior responsabilidade as empresas com objetivo de proteger direitos como liberdade e privacidade.

Fundamentada em alguns princípios RGPD, a Lei Geral de Proteção de Dados, é aplicada à operações realizadas por pessoas naturais ou jurídica, seja de direito público ou privado, de qualquer meio, país, sede ou localização de dados desde que:

> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
> III - os dados pessoais objeto do tratamento tenha sido coletados no território nacional (BRASIL, 2018).

De acordo com a Lei nº13.709 (BRASIL, 2018), os titulares devem confirmar o consentimento de seus dados para uma determinada finalidade, sendo que possam acessar,

alterar ou cancelar quando necessário. Dessa forma, as empresas devem ter pessoas ou equipes responsáveis para responder as requisições segundo ordem pessoal ou governamental.

Segundo Piurcosky (*apud* BRASIL, 2018), para garantir a segurança no tratamento dos dados, os dirigentes devem adotar e se enquadrar em normas, boas práticas, políticas de segurança, ações educativas, seguranças lógicas e físicas entre outros. Contudo, ressalta que todas as empresas carecem de aderir a lei, assim como receber punições caso não a aderem.

4.8. Segurança Lógica

Segundo Leite (2018, p.15), a Segurança Lógica é focada em proteger o sistema de ataques, vulnerabilidades, erros não intencionais e remoção acidental de dados, por meio de softwares de controle de acesso ou regras. Para o sucesso dessa segurança, é necessária a implementação de *firewalls*[13], antivírus e políticas de segurança. Assim, como o uso de dispositivos que permite monitorar, registrar e filtrar acessos, identificação e tratamento de ataques tentados.

O processo lógico do controle de acesso engloba identificação, autenticação e registro em *logs*, para que evite o ataque da integridade das informações e, pessoas não autorizadas a acessar as informações. Identificar o usuário é extremamente importante para saber quais as permissões que o mesmo terá dentro do sistema. Normalmente, o usuário possui um número de identificação que deve ser único. Logo após, inicia se a autenticação desse usuário, ou seja, a comprovação da identidade feita através de uma senha, ou alguma outra identificação, por exemplo, biométrica. Todos os acessos, alterações e outras atividades precisam ser registradas, no que se conhece por registro de *logs* (CAETANO, 2020, p. 9-11).

De acordo com Caetano (2020, p. 10), o registro de *logs* é instrumento de auditoria que permite saber qual usuário acessou determinada função no sistema e quais foram as alterações realizadas por ele. Esses devem ser gerenciados iniciando pela sincronia de relógios das diversas máquinas que atuarão, o armazenamento em uma parte especial e, por fim, a rotação desse que caracterizada pelo transporte dos *logs* antigos para um local de armazenamento, liberando espaço para novos *logs.*

Ressalta-se que para a segurança ser completa, bem planejada e alcançar o objetivo comum, as camadas de Segurança Lógica e Segurança Física não podem funcionar separadamente, pois ataques podem acontecer na segurança lógica e afetar a segurança física. De nada vale, quando tem uma perfeita segurança lógica, mas não tem uma boa segurança

[13] *Firewall* - dispositivo de uma rede de computadores, na forma de um programa ou de equipamento físico, que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

física, em outras palavras, o controle de acessos de usuários no sistema com um número único de identificação funciona corretamente, porém qualquer pessoa pode entrar a hora que quiser na sala onde localiza-se todos os servidores de uma empresa com informações valiosas (CAETANO, 2020, p. 9-11).

4.9. Segurança Física

Conforme Caetano (2020, p. 12), são originados por funcionários da devida empresa 72% de ataques como, fraudes, sabotagens, roubos, entre outros. O segundo lugar dos causadores desses ataques, ou seja, 20% são causados por terceirizados da empresa ao manipular informações e, somente 8% são provocados por redes ou pessoas externas.

Deste modo, fortalece que além do uso de segurança lógica é imprescindível a segurança física. Caetano (2020, p. 12), entende que a segurança física consiste em limitar o acesso físico, por meio de controles de segurança como: crachás: identificam funcionários e visitantes, permitindo acesso a locais para cada um de acordo com sua identificação; portas, grades, muros: monitoram entrada e saída de pessoas limitando áreas; portas duplas: exige a identificação para que intrusos não entrem junto com pessoas autorizadas;

Acrescenta-se à segurança física a localização dos servidores ou equipamentos que armazenam informações valiosas. Devem estar protegidos de agentes naturais e criminosos como inundações, fogo, falta de energia, entre outros.

5. Material e Método

Utilizou-se alguns recursos físicos e materiais como computadores e celulares com acesso à internet para a realização das pesquisas citadas a seguir. As fontes utilizadas para coletar informações foram bibliográficas, artigos acadêmicos, normas, leis e fatos de acontecimentos que englobam o assunto proposto.

A pesquisa científica realizada também possui caráter descritivo, pois será analisado e explicado o assunto de Segurança da Informação em Corporações, apresentando como ocorre o processo desde a prevenção de ataques que infringem a integridade dos dados até a recuperação desses. Dados serão interpretados e explorados, o que também torna a pesquisa qualitativa e explicativa. Segundo Andrade (2010, p. 126), "pesquisa é o conjunto de procedimentos sistemáticos, baseado no raciocínio lógico, que tem por objetivo encontrar soluções para problemas propostos, mediante a utilização de métodos científicos".

Complementa-se a pesquisa com a realização de um estudo de caso, o qual apresenta dados analisados sobre a Segurança da Informação na Fundação Educacional de Fernandópolis, mostrando possíveis riscos, tipos e graus de impactos e, a probabilidade do risco acontecer.

6. Conclusão

A pesquisa aborda o tema da segurança da informação empresarial, apresentando leis e fatos e sua importância. Além disso, demonstra os mais variados tipos de ataques e suas consequências e, a necessidade do uso de técnicas de segurança da informação.

As informações tornaram-se valiosas em qualquer âmbito, devido o avanço da tecnologia, principalmente em organizações, pois as usam para tomadas de decisões. Por esse motivo, os ataques estão cada vez mais frequentes em busca de roubá-las ou alterá-las, causando prejuízos grandiosos a empresas.

Para evitar os danos que podem ou são causados à essas informações, deve-se aplicar a Segurança da Informação. Essa, é responsável por garantir a proteção de ameaças, continuidade do negócio e maximização de oportunidades no mercado, baseada na tríade composta por integridade, confiabilidade e disponibilidade.

As informações podem estar vulneráveis a possíveis ameaças, as quais resultam em ataques e permitem riscos a organização. Dessa forma, a empresa sofre impactos de variados tipos, resultando a prejuízos desde irrelevantes até desastrosos que comprometem a sobrevivência da empresa.

Para comprovação da importância da segurança da informação, um estudo de caso foi realizado na Faculdades Integradas de Fernandópolis (FEF), o qual aponta possíveis impactos e, qual a probabilidade do risco ocorrer. Assim, como a instituição está vulnerável á ataques, maiormente estão empresas que trabalham com maior número de dados.

Conclui-se que a segurança da informação deve funcionar corretamente em qualquer tipo e tamanho de empresa, pois independente desses aspectos, os clientes confiam dados a essas. Por meio de políticas de segurança, controles físicos e lógicos, ferramentas e técnicas de prevenção de riscos, as informações estarão protegidas de acessos indevidos. Portanto, garantir a tríade da segurança da informação – confidencialidade, integridade e disponibilidade - é o objetivo.

7. Referências

1. ANDRADE, M. M. Pesquisa científica: noções introdutórias. Introdução à metodologia do trabalho científico: elaboração de trabalhos na graduação. 10. ed. São Paulo: Atlas, 2010. Cap. 10, p. 126.

2. ARAÚJO, W.J; NETO MASCARENAS, P.T. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: Editora UFPB, 2019. 160 p. Disponível em: <http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/download/209/75/905-1?inline=1>. Acesso em: 10 nov. 2022.

3. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005: Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio e janeiro, 2011.

4. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799: tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001. p. 2-51.

5. BARBOSA, Juliana Souza *et al*. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. [S. l.]: Research, Society and Development, 2021. v. 10, n.2, 11p. Disponível em: <https://rsdjournal.org/index.php/rsd/article/view/12557/11384>. Acesso em 27 abr. 2022.

6. BOHLER, Fernanda Ribas *et al*. Relatório Técnico Da Pesquisa: O Trabalho Remoto/Home-Office No Contexto Da Pandemia Covid-19 Parte I. Curitiba: Universidade Federal do Paraná, Grupo de Estudos Trabalho e Sociedade, 2020. 79 p. Disponível em: <https://www.eco.unicamp.br/remir/images/Artigos_2020/RELATRIO_DE_DIVULGAO_DA_PESQUISA_SOBRE_O_TRABALHO_REMOTO.pdf>. Acesso em 27 abr. 2022.

7. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: nov. 2022.

8. BRASIL. Tribunal de Contas da União. Boas Práticas em Segurança da Informação. 4. ed. Brasília, 2012. Disponível em: <http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24D6E86A4014D72AC823F5491>. Acesso em 17 abr. 2022.

9. CAETANO, Daniel. Aula 02: Princípios da Segurança da Informação. [S. l.]: Aula 02: Princípios da Segurança da Informação, 2020. 13p. Disponível em: <https://www.caetano.eng.br/aulas/2020a/getfile.php?fn=CCT0894_ap02.pdf>. Acesso em: 28 out. 2022.

10. COIMBRA, Sara Alexandra M. P. Ameaças e Vulnerabilidades à Segurança Da Informação dos Sistemas de Informação da Força Aérea. Política de Segurança e Prevenção. Pedrouços: Instituto Universitário Militar Departamento De Estudos Pós-Graduados, 2018. 60 p. Disponível em: <https://comum.rcaap.pt/bitstream/10400.26/24931/1/10_CapSaraCoimbra_TII_VF.pdf>. Acesso em: out. 2022.

11. DANTAS, L. M. Segurança da informação: uma abordagem focada em gestão de riscos. Olinda, 2011. p. 55.

12. DIAS, C. Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro: Axcel Books do Brasil, 2000. p. 54, 57, 114.

13. DOMINGOS, dos Santos Filipe. Segurança da informação: vírus ataques e contramedidas. Niterói: Trabalho de Conclusão de Curso (Graduação em Tecnologia de Sistemas de Computação) - Universidade Federal Fluminense, Escola de Engenharia, 2018. 51 p. Disponível em: <https://app.uff.br/riuff/bitstream/handle/1/8793/TCC_FILIPE_DOS_SANTOS_DOMINGOS.pdf?sequence=1&isAllowed=y>. Acesso em: 8 de nov. 2022.

14. FERREIRA, Fernando N. F. Segurança da Informação. Rio de Janeiro: Ciência Moderna. 2003.

15. FERREIRA, Lucas Vinicius A. Uma solução para gestão de vulnerabilidades de segurança da informação. Faculdade de Tecnologia Universidade de Brasília: Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica, 2017. 54 p. Disponível em: <https://bdm.unb.br/bitstream/10483/30315/1/2017_LucasViniciusAndradeFerreira_tcc.pdf>. Acesso em: out. 2022.

16. FIGUEIRÊDO, L.S. Segurança da Tecnologia da Informação. 2002. Disponível em: <http://www.modulo.com.br/> Acesso em: 03 nov. 2022.

17. FONTES, Edison Luiz G. Segurança da Informação. São Paulo: Saraiva Uni, 2017. 223 p. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=FyprDwAAQBAJ&oi=fnd&pg=PT7&dq=classifica%C3%A7%C3%A3o+da+seguran%C3%A7a+da+informa%C3%A7%C3%A3o++artigos+cientificos&ots=2ZnnaZvOZE&sig=30ONqUirZhypepYTACF-5Oh41ug#v=onepage&q&f=false>. Acesso em: 2 nov. 2022.

18. GALVÃO, Michele da Costa. Fundamentos em Segurança da Informação, I Série. São Paulo: Pearson Education do Brasil, 2015.

19. HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. 1. ed. BRASPORT, 2018. 256 p.

20. HÖNE, K.; ELOFF, J. Information security policy: what do international information security standards say Computers & Security. Atenas. v. 21, n. 5, p. 402–409, Oct. 2002.

21. JHONNYE, Rayan. Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança. Ceará: Mestrado Profissional em Computação UECE/IFCE (MPCOMP), s.d. 2022, 7 p. Disponível em: <https://www.academia.edu/7520311/Seguran%C3%A7a_em_Cloud_Computing_Governan%C3%A7a_e_Gerenciamento_de_Riscos_de_Seguran%C3%A7a>. Acesso em: 11 nov. 2022.

22. LAUREANO, M. A. P. Gestão de Segurança da Informação. [s. l.]: 2005. 130 p. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 2 nov. 2022.

23. LEC, Redação. Matriz de Risco: Como funciona e como implementá-la na empresa. 2020. Disponível em:< https://lec.com.br/matriz-de-risco/>. Acesso em: 22 nov. 2022.

24. LEITE, Luciano. Políticas de segurança física e lógica de tecnologia da informação em redes de computadores e seus ativos. Curitiba: Monografia de Especialização, apresentada ao Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, 2018. 34 p. Disponível em: <https://repositorio.utfpr.edu.br/jspui/bitstream/1/17306/1/CT_GESER_X_2018_04.pdf>. Acesso em: 2 nov. 2022.

25. LIMA, Adriano. Gestão da segurança e infraestrutura de tecnologia da informação. São Paulo: Editora Senac São Paulo, 2018. 158p. Disponível em: <https://books.google.com.br/books?hl=ptBR&lr=&id=pBlfDwAAQBAJ&oi=fnd&pg=PT6&dq=classifica%C3%A7%C3%A3o+da+informa%C3%A7%C3%A3o+seguran%C3%A7a&ots=Ddiz07iJcw&sig=YajDE_FyfActjlD0ZpU9Unyk7pk&redir_esc=y#v=onepage&q&f=false>. Acesso em: 8 nov. 2022.

26. MARCIANO, Pereira L.J. Segurança da Informação -uma abordagem social. Brasília: Pós- Graduação em Ciência da Informação do Departamento de Ciência da Informação e Documentação da Universidade de Brasília, 2006. 212 p. Disponível em: <https://repositorio.unb.br/bitstream/10482/1943/1/Jo%c3%a3o%20Luiz%20Pereira%20Marciano.pdf>. Acesso em: 2 nov. 2022.

27. OCDE, Organisation For Economic Co-Operation And Development. OECD Official Site. Paris, 2002. Disponível em: < https://www.oecd.org/>. Acesso em: 2 nov. 2022.

28. PEDRA, David. Segurança da informação: o que é e como criar uma política para proteção de dados. [S. l.]: 2022. Disponível em: <https://www.siteware.com.br/processos/seguranca-da-informacao/>. Acesso em 30 abr. 2022.

29. PINHEIRO, Nickollas Barros; SILVA, Rogério Oliveira da. Uso Da Tecnologia Na Solução De Crimes Virtuais e Boa Práticas De Segurança Da Informação. Revista Tecnologias em Projeção, v10, n°1, ano 2019. Disponível em: <http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/download/1358/1063>. Acesso em 27 abr. 2022.

30. PISA, Adriana. A tríade do Sistema de Gestão da Segurança da Informação. 2020. Diponível em: < https://www.adrianapisaadvocacia.com.br/2020/11/17/a-triade-do-sistema-de-gestao-da-seguranca-da-informacao/>. Acesso em: 06 dez. 2022.

31. PIURCOSKY, Fabrício Pelloso *et al*. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. Minas Gerais: Suma de Negócios, 2019. 11 p. Disponível em: <http://www.scielo.org.co/pdf/sdn/v10n23/2215-910X-sdn-10-23-89.pdf>. Acesso em: nov. 2022.

32. RAMOS, A. Security Officer 1: guia oficial para a formação de gestores em Segurança da Informação. 2. ed. Porto Alegre: Zouk, 2008.

33. REIS, Bruno; MOTA, Jimmy; OLIVEIRA, Patryck. Classificação da Informação. Universidade Católica de Brasília (UCB), Campos Universitário II, SGAN 916 – Módulo B– Brasília – DF – Brasil, s.d, 2022, 10 p. Disponível em: <http://www.lyfreitas.com.br/ant/artigos_mba/artclassinfo.pdf>. Acesso em: 08 nov. 2022.

34. RUPPENTHAL, J.E. Gerenciamento de Riscos. Santa Maria: Universidade Federal de Santa Maria, Colégio Técnico Industrial de Santa Maria ; Rede e-Tec Brasil, 2013. 120 p. Disponível em: <https://site.educacao.go.gov.br/files/SESMT/GerenciamentodeRiscosOcupacionais.pdf>. Acesso em: 10 nov. 2022.

35. SILVA, P. T; CARVALHO, H; TORRES, C. B. Segurança dos Sistemas de Informação. Lisboa: Centro Atlântico, 2003. 255 p. Disponível em: <http://www.centroatl.pt/titulos/si/imagens/excerto-ca-seguranca-si.pdf>. Acesso em: 2 nov. 2022.

36. SOUZA, Renata. Crackers que invadiram sistemas do Ministério da Saúde sofrem contra-ataque. Brasília: Brasília, 2022. Disponível em: <https://noticias.r7.com/brasilia/crackers-que-invadiram-sistemas-do-ministerio-da-saude-sofrem-contra-ataque-01032022>. Acesso em: 08 nov. 2022