CERTIFICAÇÃO ISO 27001: A IMPORTÂNCIA EM SUA UTILIZAÇÃO

ISO 27001 CERTIFICATION: THE IMPORTANCE OF USING IT

Andréia A. Sartore[1], Ronaldo L. Oliveira[2], Rogério L. S. Oliveira[3]

[1]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales,andreia.oliveira11@fatec.sp.gov.br
[2]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales, ronaldo.oliveira23@fatec.sp.gov.br
[3]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales, rogerio.leao@fatec.sp.gov.br

Informação e Comunicação
Subárea: Arquitetura de Computadores, Redes e Segurança.

RESUMO

O presente trabalho aborda a importância e as vantagens de uma empresa com norma ISO 27001 implementada, descobrindo quais os tipos de empresa precisam ter a certificação para proteção das informações, tanto da empresa, quanto dos funcionários, clientes e parceiros. Descreve, também, o processo para obter a certificação, o tempo para adequação e implementação das regulamentações exigidas pela ISO 27001, a fim de evitar o vazamento das informações. Trata, inclusive, da importância do treinamento dos colaboradores para que não haja problemas durante a regulamentação, bem como o acompanhamento de um consultor experiente na área para evitar processos e documentos desnecessários para a implementação.
Palavras-chave: ISO 27001; proteção das informações; regulamentação.

ABSTRACT

The present work aims to address the importance and advantages of a company implementing the ISO 27001 standard, in addition to discovering which areas actually need to be certified to protect the company's information, as well as employees, customers and partners. Describes the process to obtain certification, time for adaptation and implementation of the regulations required by ISO 27001 to avoid information leakage, the importance of employee training so that there are no problems during the regulation, as well as the monitoring of an experienced consultant in the area, thus prevents processes and documents unnecessary for implementation.
Keywords: ISO 27001; safety; regulation.

1 INTRODUÇÃO

Sabe-se que a informação é o bem mais importante de uma organização, o que antes podia ser guardado e trancado dentro de uma gaveta, nos dias atuais, podem ser acessados por dispositivos que cabem na palma da mão.

Para que haja a proteção de tais dados, foram desenvolvidas normas que descrevem como deve ser gerenciada a segurança da informação dentro de uma organização. A ISO 27001 é uma norma internacional, que pode ser implementada em qualquer tipo de organização, e conta com uma metodologia para que haja a implementação da gestão da segurança da informação em uma empresa.

Uma empresa com a ISO 27001 implementada passa maior confiabilidade e credibilidade para seus clientes e parceiros, pois as informações serão tratadas de acordo com elevados padrões de gestão e proteção da Segurança da Informação, garantindo confidencialidade e integridade da informação armazenada.

Os sites consultados, compostos em sua maioria de empresas que realizam a implementação da norma, explicam a importância do acompanhamento de um profissional

treinado e habilitado na área de implementação da norma, a fim de otimizar o tempo para elaboração dos documentos realmente necessários e treinar toda a equipe durante o processo de regulamentação da norma.

2 REFERENCIAL TEÓRICO

2.1 O QUE É A ISO 27001

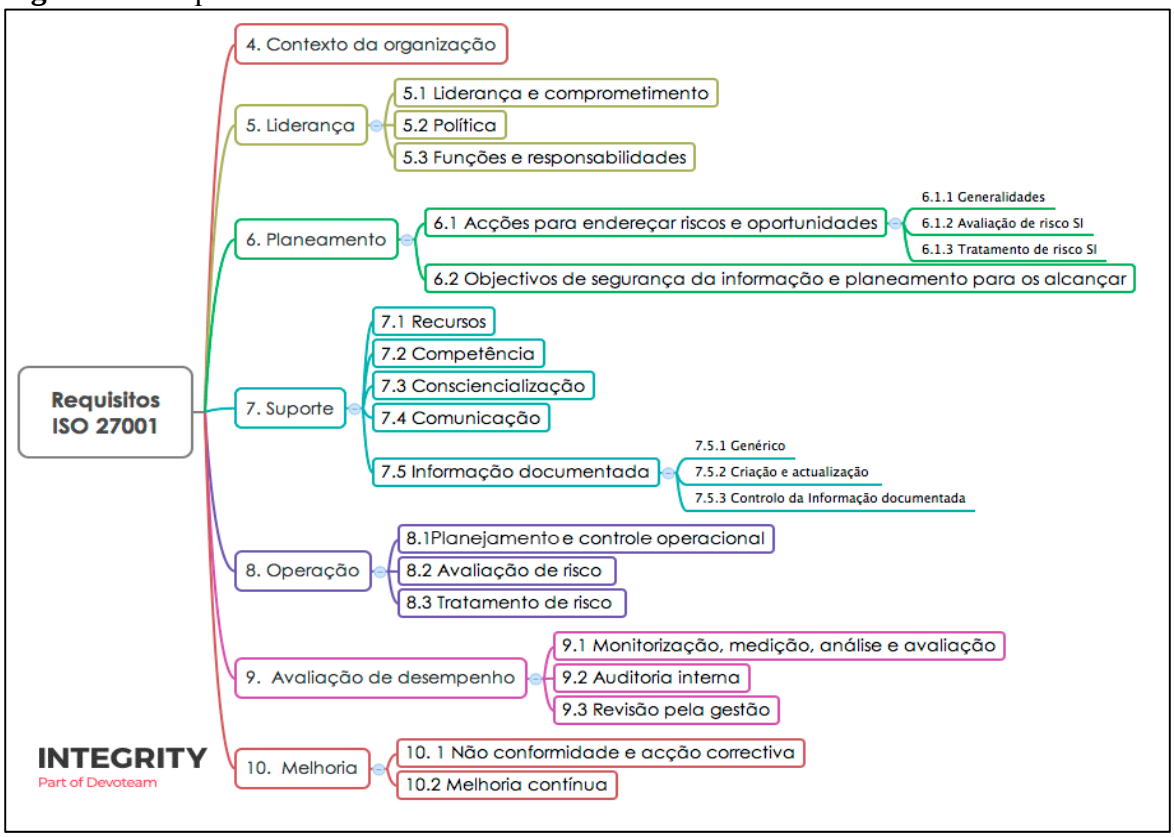
A ISO (*International Organization for Standardization*) é uma entidade responsável por promover normas internacionais para padronizar produtos, serviços e processos. Para a regulamentação da segurança da informação é utilizada a Norma ISO 27001.

Para Hintzbergen et al. (2018), "a ISO/IEC 27001:2013 trata-se de uma norma para estabelecer a segurança da informação na organização", o autor também fala que uma organização pode ser certificada com a ISO 27001 e mostrar, aos seus clientes e fornecedores que atende, os requisitos de qualidade de segurança da informação.

A implementação da norma ISO 27001 tem por objetivo garantir um alto compromisso com a proteção da informação, oferecendo às empresas referências e quais as melhores práticas para identificar, analisar e implementar controles que farão a gestão dos riscos de segurança, mantendo a confidencialidade e integridade de dados essenciais aos negócios.

É composta por dois componentes distintos, na qual, a primeira parte contém as definições das regras e dos requisitos de cumprimento da norma. Na Figura 1 são ilustrados os aspectos explícitos da norma.

Figura 1 – Requisitos ISO 27001

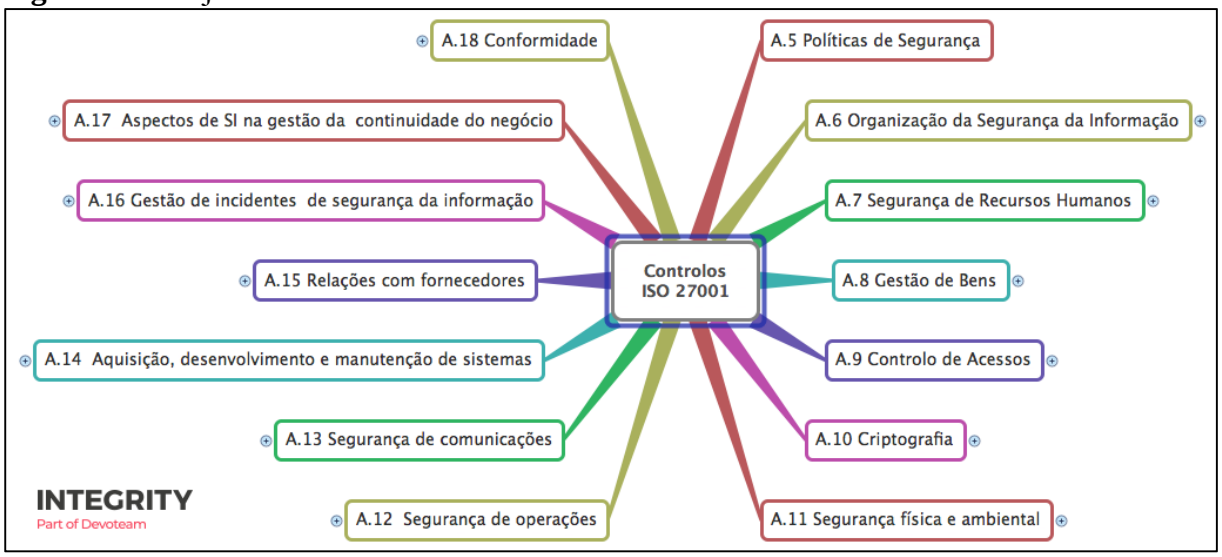


Fonte: INTEGRITY, 2023.

A imagem acima demonstra quais os requisitos que devem ser cumpridos na implementação da norma ISO 27001 em qualquer empresa.

O segundo componente da norma é composto por um conjunto de normas que as organizações devem adotar, conforme ilustra a Figura 2.

Figura 2 – Conjunto de normas a serem adotadas



Fonte: INTEGRITY, 2023.

A figura acima aborda os conjuntos de normas a serem adotadas pela empresa, para que haja melhor segurança dos dados ali armazenados, além da elaboração de documentos para facilitar a implementação da norma.

2.2 BENEFÍCIOS

De acordo com a empresa Integrity (2023), qualquer empresa que lida com dados pode solicitar a implementação da ISO 27001, trazendo benefícios únicos para quem a implementa, como: demonstração de compromisso dos executivos da organização com a segurança da informação; aumento da confiabilidade e segurança em termos de confidencialidade, disponibilidade e integridade; garantia de investimentos mais eficientes, com orientações de risco, ao invés de baseados em tendências; aumento da confiança e satisfação dos clientes e parceiros, dando maior potencial na realização de negócios futuros; e melhoria no desempenho operacional da organização, dotando a empresa de um sistema de controle de gestão, demonstrando a eficácia da organização.

Para clientes e parceiros, a implementação da norma demonstra um elevado compromisso com a proteção de suas informações.

2.3 COMO OBTER A CERTIFICAÇÃO ISO 27001

Santos (2022) do site Automação Industrial, explica que antes de obter a certificação, é preciso entender que há duas versões da ISO 27001, uma para organizações e uma para indivíduos.

Para uma organização obter a certificação é preciso seguir à risca as etapas e os conselhos para a norma ser implementada dentro da empresa. Após se certificar que está tudo conforme deveria, é realizada uma auditoria com um dos órgãos de certificação oficial.

Tal auditoria é dividida em três estágios: 1) análise completa da documentação; 2) auditoria para verificação das atividades exercidas pela empresa, se estão de acordo com a

proposta de ISO 27001; e 3) visitas de supervisão que serão realizadas durante os três anos de validade da certificação.

Já para indivíduos que querem receber a certificação da ISO 27001, é necessário realizar alguns exames e cursos, como: Curso de Implementador Líder da ISO 27001, Curso de Auditor Interno ISO 27001, e Curso de Auditor Líder ISO 27001.

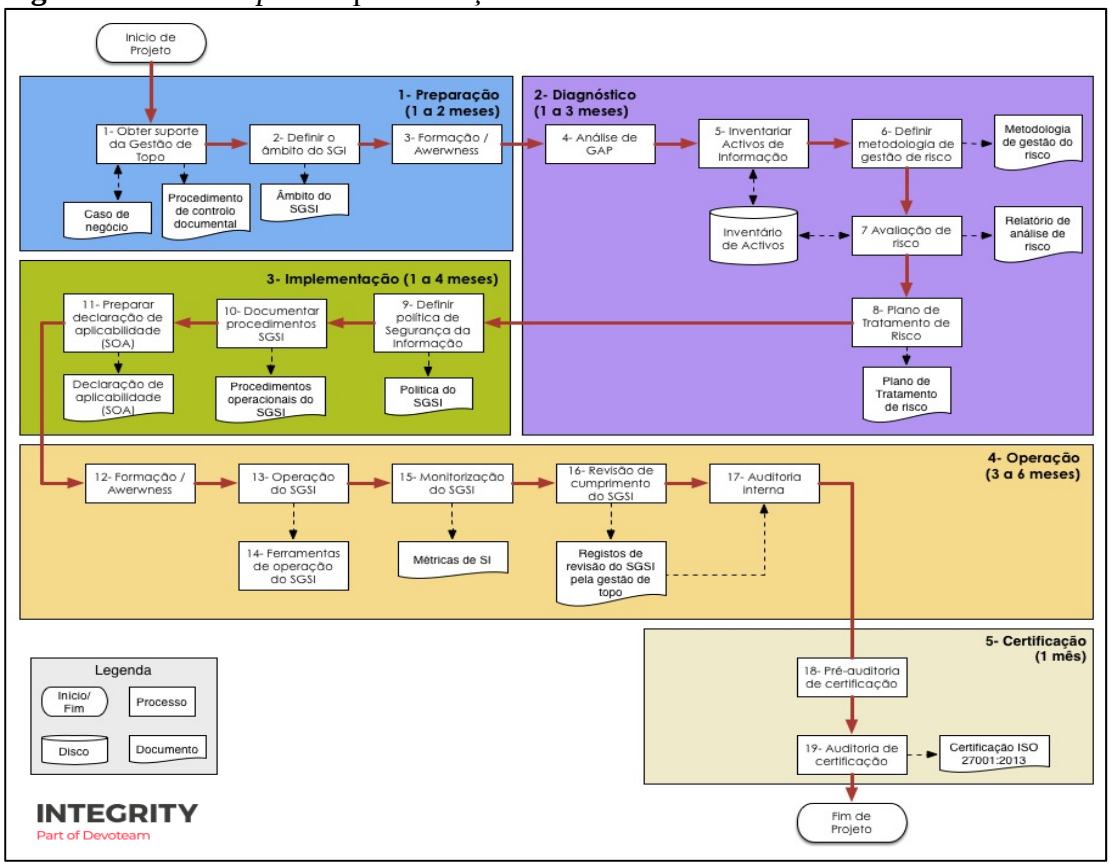
2.4 QUANTO TEMPO DEMORA A PREPARAÇÃO DA CERTIFICAÇÃO

O site Integrity (2023) fala que para implementar a certificação é necessária a implementação e adoção de uma série de requisitos, políticas, procedimentos, controles e práticas requeridas pela norma ISO 27001, sempre ajustados à realidade tecnológica de cada organização que deseja se certificar.

O tempo de implementação varia de acordo com a realidade, tamanho e maturidade de cada organização.

A Figura 3 ilustra o processo de implementação.

Figura 3 – *Roadmap* de implementação de um SGSI



Fonte: INTEGRITY, 2023.

A Figura 3 acima aborda todos os processos e tempo estimado para a implementação de cada etapa, porém, deve-se lembrar que esse tempo muda dependendo do tamanho da empresa, nível de organização e digitalização desses dados, sempre com a ajuda de um especialista na implementação da norma.

2.5 CUSTOS PARA ADQUIRIR A ISO 27001

De acordo com o site Advisera (2023), o custo para implantar depende do tamanho da organização e/ou unidades de negócios a serem incluídas no escopo da ISO 27001, além da tecnologia utilizada, exigências da legislação (setor financeiro e governamental são fortemente regulamentados no que diz respeito a segurança da informação).

Deve-se levar em consideração o nível de proteção que a empresa precisa, executar a avaliação de riscos e tal análise indica as medidas de segurança necessárias.

Além disso, deve-se levar em consideração os seguintes custos: livros especializados e treinamentos: os funcionários devem ser preparados com livros e cursos sobre o assunto, além de comprarem a própria norma ISO 27001; e custo da ajuda externa: não basta apenas treinar os funcionários, o gerente de projetos precisa ter profunda experiência na implementação da norma, caso não possua ninguém qualificado na empresa, precisará contratar um consultor.

É vantajoso ter alguém experiente ajudando com a implementação, pois não corre o risco de realizar etapas que não são necessárias ou elaborar documentos que não são, de fato, exigidos. É importante lembrar que a implementação não é feita pelo consultor, e sim pelos funcionários.

Outros custos que podem ser elencados são: o custo da tecnologia: muitas vezes, será necessário investir em hardware e ferramentas mais atuais para melhor implementação; o custo do tempo dos funcionários: como os funcionários vão passar um tempo descobrindo onde estão os riscos, para melhorar os procedimentos e políticas, também precisam reservar parte do seu tempo para o treinamento e adaptar as novas regras; e o custo da certificação: para obter a prova pública de que está cumprindo com as especificações da norma, será necessário realizar uma auditoria de certificação, o custo da auditoria depende de quantos dias e quantas pessoas serão necessárias para a conclusão do trabalho.

2.6 POR QUE A ISO 27001 É BOA PARA SUA EMPRESA

De acordo com a empresa Templum (FABIANA, 2021), obtendo a certificação, a empresa atinge quatro benefícios implementando a norma, sendo eles: 1) conformidade com requisitos legais – como sempre aparecem novas leis, regulamentações e requisitos contratuais, muitos desses “problemas” podem ser resolvidos com a implementação da norma; 2) vantagem de marketing – ao obter a certificação, tem-se a vantagem sobre os concorrentes que não são certificados, garantindo maior confiança dos clientes em relação aos serviços da empresa; 3) redução de custos – por prevenir incidentes de segurança, a empresa economizará uma certa quantia em dinheiro, caso tivesse que reparar danos causados por falha de segurança; e 4) melhor organização – para as organizações que crescem rápido e acabam não definindo processos e procedimentos, deixando os funcionários perdidos, com a norma implementada, muitos processos serão escritos, reduzindo a perda de tempo dos funcionários.

2.7 TIPOS DE EMPRESAS QUE PRECISAM DA ISO 27001

Segundo o site da empresa Templum (CONRADO, 2023), a empresa de qualquer área pode solicitar a implementação da ISO 27001, mas têm algumas áreas que realmente precisam da certificação, por lidarem com informações muito importantes de seus clientes.

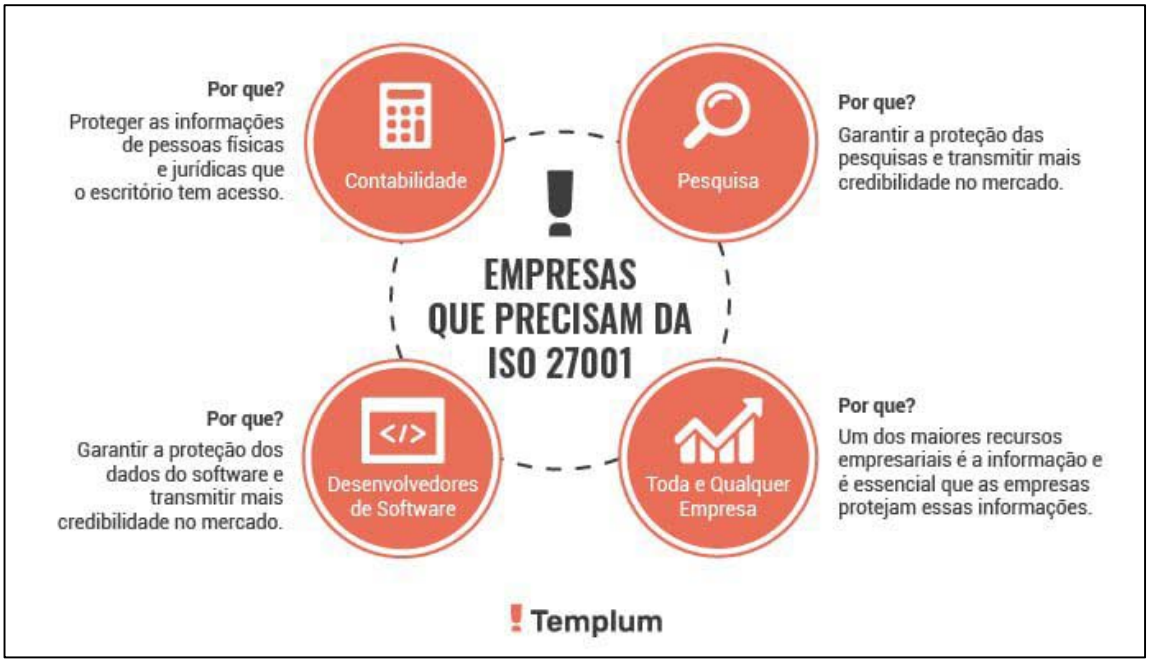
As empresas que precisam da ISO 27001 são: as de contabilidade: por trabalhar com informações de pessoas físicas e jurídicas, a implementação da ISO 27001 ajuda a garantir a segurança das informações, além de propor cuidados específicos para o gerenciamento de riscos; as de desenvolvedores de softwares: ter a certificação passa maior credibilidade no mercado, pois não adianta ter a preocupação com a segurança da informação, se os softwares

de armazenamento de dados não possuírem esse cuidado; e as de pesquisa: a ISO 27001 abrange até mesmo as agências governamentais.

É importante lembrar que empresas que trabalham com pesquisa ou pesquisa científica precisam tem a certificação, pois é extremamente importante para o mercado que as informações sejam idôneas e confiáveis, uma vez que essas empresas lidam com informações que precisam de segurança e um Sistema de Gerenciamento para eliminar ou reduzir o risco dessas informações.

A Figura 4 ilustra um gráfico sobre quais empresas precisam da ISO 27001.

Figura 4 – Empresas que precisam da ISO 27001



Fonte: CONRADO, 2023.

De acordo com a Figura 4 acima, as empresas da área de contabilidade, pesquisa e de desenvolvimento software são as que mais possuem a necessidade de implementar a Norma ISO 27001, garantindo uma melhor proteção dos dados que são armazenados por elas.

3 METODOLOGIA

Para o presente trabalho, foi utilizado o método monográfico, sendo realizada uma pesquisa bibliográfica em livros, artigos e pesquisas para discussão do assunto proposto.

Quanto a pesquisa bibliográfica, usou-se o máximo de bibliografia já tornada pública pertinente ao assunto, sendo vídeos, jornais, boletins, livros, revistas, teses etc. O artigo tem por finalidade colocar o pesquisador em contato direto com tudo relacionado ao assunto pesquisado.

Para Manzo (1971, p. 32 apud LAKATOS; MARCONI, 2023), a bibliografia pertinente "oferece meios para definir, resolver, não somente problemas já conhecidos, como também explorar novas áreas onde os problemas não se cristalizaram suficientemente" e tem por objetivo permitir ao cientista "o reforço paralelo na análise de suas pesquisas ou manipulação de suas informações". Portanto, a pesquisa bibliográfica não é uma repetição de tudo que já foi dito/escrito sobre determinado assunto, mas proporciona um novo ponto de vista, uma análise, chegando a novas conclusões.

O material utilizado para a realização do presente artigo pautou-se em livros e sites especializados no assunto abordado.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Com base nas informações encontradas durante a pesquisa bibliográfica, observou-se que as empresas que tiveram problemas com violação de dados resultaram em prejuízo financeiros e também perderam a credibilidade diante dos clientes, além de precisarem pagar multas devido à legislação da Lei Geral de Proteção de Dados (LGPD).

Tal vulnerabilidade pode atingir empresas pequenas e grandes, até mesmo as instituições governamentais não saem ilesas de ataques cibernéticos de roubo de informações. A adoção de medidas é essencial para proteger os dados confidenciais da empresa, dos funcionários e dos clientes.

Além de ajudar as empresas a cuidarem de dados essenciais, demonstra o grau de seriedade e segurança em relação aos seus clientes, pois incentiva uma atitude proativa em relação aos riscos de segurança da informação.

Estando implementado corretamente, é possível antecipar e prevenir possíveis ameaças de ataques, assegurando aos clientes atuais e potenciais a segurança de que seus dados estão seguros de qualquer tipo de vazamento de dados. Também insere a empresa à frente de seus concorrentes, por demonstrar que a organização adota uma atitude séria e sensata em relação à segurança da informação.

Apurou-se também que a ISO 27001 visa proteger três aspectos da informação: confidencialidade, integridade, disponibilidade, no qual:

- Confidencialidade: somente pessoas autorizadas possuem acesso à informação;
- Integridade: somente pessoas autorizadas podem alterar as informações;
- Disponibilidade: informação precisa estar acessível sempre que necessário para as pessoas autorizadas.

Na implementação da ISO 27001, são identificados os potenciais problemas que podem ocorrer com a informação, para então definir as principais necessidades que serão atendidas, para a evitar que tais problemas aconteçam, a fim de descobrir onde os riscos estão para, enfim, tratá-los.

Os controles são implementados na forma de políticas, procedimentos e implementações técnicas. Em muitos casos, certas organizações já possuem toda a estrutura de hardware e software instalados, porém são utilizados de forma insegura, e fazem com que a maioria das implementações sejam sobre definir regras organizacionais para prevenirem brechas de segurança.

Gerir a segurança da informação da empresa não se trata apenas da parte de tecnologia da informação, mas abrange o gerenciamento de processos, proteção legal, recursos humanos, dentre outros.

5 CONSIDERAÇÕES FINAIS

Com o presente trabalho, foi possível observar a importância que a certificação tem para uma empresa, pois além de proporcionar maior segurança das informações, traz mais confiabilidade para os clientes e parceiros ao saberem que suas informações estarão totalmente íntegras e protegidas, sem riscos de vazamento de tais dados.

Apesar de inicialmente parecer um processo demorado, oneroso e até mesmo repetitivo, é importante para se estabelecer por escrito normas e procedimentos a serem adotados pelos funcionários, deixando os processos e tomadas de decisões mais rápidos e padronizados, evitando que haja a invasão e vazamento das informações.

Observou-se também que a implantação da norma ISO 27001 evita passar por adequações de novas leis e regulamentações que vão surgindo, pois com a padronização e adequação da norma, facilita os processos, até mesmo sobre as novas regulamentações, além de prevenir brechas de segurança.

REFERÊNCIAS

ADVISERA. **O que é a ISO 27001?** Disponível em: https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/. Acesso em: 9 maio 2023.

CONRADO. **Empresas que precisam da ISO 27001**. Disponível em: https://certificacaoiso.com.br/empresas-que-precisam-da-iso-27001/. Acesso em: 9 de maio. 2023.

FABIANA. **10 Benefícios ISO 27001 para a sua organização**. 2021. Disponível em: https://templum.pt/10-beneficios-iso-27001-para-a-sua-organizacao. Acesso em: 7 de maio. 2023.

HINTZBERGEN, J. *et al*. **Fundamentos de segurança da informação com base na ISO 27001 e na ISO 27002**. 3. ed. Rio de Janeiro: Brasport, 2018.

INTEGRITY. **O que é a norma ISO 27001?** Disponível em: https://www.27001.pt/index.html. Acesso em: 8 maio 2023.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

SANTOS, G. **ISO 27001**: o que é, como funciona e para que serve. 2022. Disponível em: https://www.automacaoindustrial.info/iso-27001/. Acesso em: 8 maio 2023.