A ABNT NBR ISO/IEC 27701:2019 E A SEGURANÇA DA INFORMAÇÃO

Ana Laura Borsari Diniz
Graduanda em Engenharia de Software – Uni-FACEF
analauradiniz16@gmail.com

Débora Pelicano Diniz
Mestre em Computação – Uni-FACEF
deboradiniz@facef.br

Resumo
O presente artigo visa apresentar e elucidar de que maneira a ABNT NBR ISO/IEC 27701:2019 relaciona-se com a Segurança da Informação. Para o desenvolvimento do artigo, cujo caráter foi de uma pesquisa exploratória, utilizou-se de materiais e artigos da área da Segurança da Informação, Lei Geral de Proteção de Dados e da série de normas ISO 27000. Compreende-se, após o estudo, que a ABNT NBR ISO/IEC 27701:2019 proporciona um novo enfoque para a família de normas ISO 27000, ao abranger a Segurança da Informação para a área de proteção de dados pessoais. Baseado no estudo das temáticas abordadas no artigo, uma Política de Segurança da Informação foi desenvolvida para uma empresa do ramo de eventos e lazer.

Palavras-chave: ABNT NBR ISO/IEC 27701:2019. LGPD. Segurança da Informação.

Abstract
This article aims to present and elucidate how ABNT NBR ISO/IEC 27701:2019 is related to Information Security. For the development of the article, whose character was an exploratory research, it used materials and articles from the General Data Protection Law and the series of ISO 27000 standards. It is understood, after the study, that ABNT NBR ISO/IEC 27701:2019 offers a new approach to a family of ISO 27000 standards, covering Information Security for personal data. Discussed in the article, an Information Security Policy was developed for a company in the events and leisure sector.

Keywords: ABNT NBR ISO/IEC 27701:2019. LGPD. Information Security.

1 Introdução

O artigo em questão visa abordar a Lei Geral de Proteção de Dados (LGPD) e a sua correlação com a família da norma ISO 27000. O foco central do artigo visa responder a seguinte pergunta: qual a associação entre a série ISO 27000, mais especificamente a ABNT NBR ISO/IEC 27701:2019, e a LGPD, e qual sua correlação com a Segurança da Informação?

O objetivo geral do artigo foi analisar a LGPD, a série ISO 27000 e a Segurança da Informação de forma a elucidar a relação entre os temas. Para isso é

necessário atingir os seguintes objetivos específicos: conhecer os critérios da lei; verificar a série da ISO 27000; estabelecer a correlação entre a LGPD e ABNT NBR ISO/IEC 27701:2019 com a Segurança da Informação.

A justificativa do artigo é devido a LGPD ser um tema emergente e crítico quando se refere à Segurança da Informação. É imprescindível compreender alguns conceitos da área de Segurança da Informação, bem como entender ao que se refere a série de normas da ISO 27000.

A motivação para o desenvolvimento do artigo é devido a necessidade de assimilar em quais pontos a LGPD e a ABNT NBR ISO/IEC 27701:2019 se relacionam e quais são as particularidades de cada uma. Foi utilizado o método Kanban para gerenciar o projeto e o andamento da execução das atividades, com o auxílio do *software Trello*. Desta forma, buscou-se garantir uma *deadline* dentro do prazo e com entregas com a qualidade esperada.

Em relação a metodologia de pesquisa, o presente artigo possui caráter exploratório, no qual visa abranger o estudo de bibliografias da área que abordam a LGPD, série ISO 27000 e Segurança da Informação.

Como conclusão do estudo teórico realizado ao longo do artigo, aplicou-se os conhecimentos adquiridos no desenvolvimento de uma Política de Segurança da Informação para uma empresa específica do setor de eventos e lazer.

2 Referencial teórico

Nesta seção são apresentados os embasamentos teóricos que sustentam a discussão sobre a importância dos dados nos dias atuais.

2.1 Os dados no século XXI

No mundo contemporâneo a disponibilização de dados pessoais em troca de algum benefício ou para utilizar algum serviço/produto se tornou tão comum, que chega a ser algo corriqueiro. A forma como esta troca ocorre é espontânea, e muitas vezes não se reflete sobre o porquê ou quais dados são coletados. Raramente são questionados os motivos que a pessoa física e/ou jurídica tem para pedir o CPF, data de nascimento e nome completo em troca de um cupom de 15% de desconto na compra dos produtos que são oferecidos em um *e-commerce*, por exemplo.

Antes de prosseguir, é importante ressaltar a diferença de significados entre o que se entende por dado e informação. Conforme definido por Hintzberguer *et al* (2018, p. 556), “o dado pode ser processado pela tecnologia da informação, mas ele se torna informação após adquirir certo significado. Na nossa vida diária, deparamos com informações em incontáveis diferentes formas”. Desta maneira, pode-se dizer que a informação é o dado antes de ser processado e inserido dentro de um contexto.

É imprescindível entender o porquê dos dados serem tão importantes e o motivo das empresas terem passado a olhar para eles com uma visão estratégica e como diferencial competitivo. Para Taurion (2013, p. 36), os “dados são os recursos naturais da sociedade da informação, como o petróleo para a sociedade industrial. Tem valor apenas se tratados, analisados e usados para tomada de decisões”. Ou seja, as empresas, nos dias atuais, utilizam as informações provenientes do tratamento de dados para a visão estratégica e como diferencial competitivo, desenvolvendo a inteligência de mercado, que é definida como

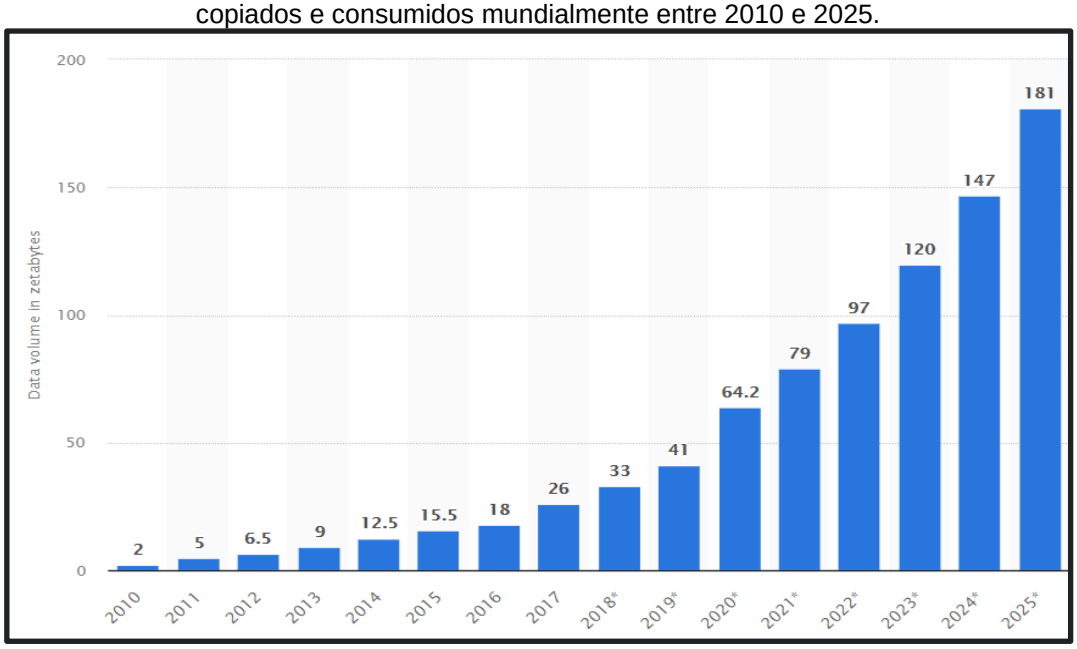
> uma ferramenta de captura e análise de dados, transformados em informações inteligentes, que apoiarão a tomada de decisão na área mercadológica. Tem como objetivo contextualizar a presença de incertezas geradas pelo mercado, exigindo dos executivos medidas concretas para neutralizar as ações dos concorrentes (MARÓSTICA; MARÓSTICA; CASTELO BRANCO, 2020, p. 113).

Para Pereira e Silva (2021), “dados talvez sejam, hoje, o *commodity* mais desejado na era digital; o efeito prático decorrente deste fato é que, quanto maior o volume de dados ‘controlados’ por determinada pessoa ou empresa, maior o poder que ela exercerá em uma economia movida a dado”. Ou seja, os dados são parte central para as empresas em seus mercados de atuação, e trazem com eles, informações que são essenciais para os negócios.

Os dados, de acordo com Taurion (2013, p. 37), são “gerados por *e-mails*, mídias sociais (*Facebook, Twitter, YouTube* e outros), documentos eletrônicos, apresentações estilo *PowerPoint*, mensagens instantâneas, sensores, etiquetas *RFID* [*Radio Frequency Identification*, ou identificação por radiofrequência], câmeras de vídeo etc”. Deste modo, entende-se que os dados são criados pelas mais diferentes fontes.

O volume de dados digitais gerados é colossal. De acordo com *Statista* (2020), em uma pesquisa de âmbito global e divulgada em 2021, é estimado que em 2024 exista 149 *zettabytes* de dados (1 *zettabyte* (ZB) equivale a 10^{21}).

Figura 1: Estimativa do volume de dados/informações criados, capturados, copiados e consumidos mundialmente entre 2010 e 2025.



Fonte: *Statista, 2021*

Como apresentado na Figura 1, pode-se perceber que a quantidade de dados gerados apresenta um crescimento com tendência exponencial desde meados de 2018.

No relatório anual divulgado pelo *Facebook* em janeiro de 2021, sobre o ano de 2020, informa que há em média 1.84 bilhões de usuários ativos diariamente (*daily active users* (DAUs)), e 2.80 bilhões de usuários ativos mensalmente (*monthly active users* (MAUs)). Em uma pesquisa realizada pela *Domo* em 2020, *Data Never*

Sleeps 8.0, sugere que a população presente na *Internet* seja de 4.5 bilhões, e que a cada minuto do dia em 2020,

- O *Twitter* ganha 319 novos usuários
- Consumidores gastam 1 milhão de dólares online
- Usuários do *Facebook* compartilham 150 mil mensagens
- Mais de 41 milhões de mensagens são enviados no *WhatsApp* pelos usuários
- São postados mais de 347 mil *stories* no *Instagram*
- *Netflix* exibe mais de 404 mil horas de vídeo

(Tradução das autoras. *Domo*, *Data Never Sleeps 8.0*, 2020)

Fica claro, com o que já foi exposto e o que outras pesquisas demonstram (*We Are Social/Hootsuit*, 2020*)*, que há um volume gigantesco de dados gerados a todo momento na *Internet*, das mais diversas fontes. Além disso, a tendência, como apresentado pelo estudo da *Statista* (2020), é que esse volume cresça ainda mais ao longo dos anos.

2.2 O fator humano na segurança dos dados

Devido a quantidade imensa de dados que são produzidos, como exposto na seção anterior, a preocupação com a segurança destes dados passa a ser cada vez mais presente para as empresas, e também, para os próprios usuários. De acordo com Pereira e Silva (2021), uma pesquisa do *Massachusetts Institute of Technology* (MIT) “aponta que vazamentos de dados aumentaram 493% no Brasil, sendo que mais de 205 milhões de dados de brasileiros vazaram de forma criminosa em 2019”.

Em janeiro de 2021, um dos mais graves vazamentos de dados do Brasil foi a público. Conforme diz Gustavo Rodrigues (2021), coordenador de políticas e pesquisador no Instituto de Referência em Internet e Sociedade (IRIS), a PSafe divulgou que “mais de 220 milhões de pessoas tiveram informações relacionadas aos mais diversos aspectos de suas vidas publicizadas para *download* na *internet*”. Entre os dados vazados estão nome completo, data de nascimento, CPF, gênero, RG, situação na Receita Federal e outros dados pessoais.

O vazamento de dados impacta não somente as instituições que foram alvo dos vazamentos, mas também a cada indivíduo que teve dados pessoais expostos sem seu consentimento, e muitas vezes, sem sequer ter o conhecimento de que seus dados foram vazados.

Cada vez mais, torna-se imprescindível os usuários de *Internet* preocuparem-se com a sua segurança no meio digital. Ter um olhar atento para quais dados são fornecidos, e para quem, pode ser o diferencial para prevenir que dados pessoais sejam expostos.

Uma pesquisa, intitulada de Segurança de Dados no Brasil: a visão da sociedade (recorte regional), divulgada pelo Observatório FEBRABRAN (Federação Brasileira de Bancos), “evidencia que o medo de ser vítima de crimes a partir da violação de dados pessoais está presente entre os entrevistados das cinco regiões do país” (FEBRABRAN, 2021, p. 6).

A pesquisa indica que devido ao aumento no número de ocorrências de fraudes no meio eletrônico, medidas de segurança passaram a ser tomadas pelas pessoas como forma de prevenção, e a principal delas refere-se a escolher senhas fortes (FEBRABAN, 2021, p. 7). O conhecimento referente à legislação brasileira que

envolve a proteção e privacidade de dados pessoais ainda não abrange a totalidade da população. A pesquisa demonstra que

> o entendimento declarado em relação à legislação que rege a proteção e a privacidade dos dados pessoais é maior no Sul do Brasil (62%) e menor no Nordeste (53%). Em relação à principal Lei que assegura o direito à privacidade e à proteção de dados pessoais, a LGPD, o conhecimento é inferior a 40% no Norte (35%), Nordeste (32%) e Centro Oeste (35%), e maior no Sudeste (41%) e Sul (40%) (FEBRABAN, 2021, p. 41).

Devido a pesquisa realizada pela FEBRABAN, pode-se concluir que a população brasileira, no cenário apresentado no ano de 2021, preocupa-se com a segurança de seus dados, e passa a tomar medidas para prevenir vazamentos e exposição dos dados pessoais. Além disso, apesar da legislação que rege a proteção e privacidade de dados pessoais não ser amplamente difundida e conhecida pelos brasileiros, há a expectativa que estas leis assegurem que os dados estarão seguros e protegidos.

Para Mitnick e Simon (2003, p. 3), o fator humano é considerado o “elo mais fraco da segurança”; e ainda que “a segurança não é um problema para a tecnologia — ela é um problema para as pessoas e a direção”. Conforme exposto pelas ideias de Mitnick e Simon, pode-se considerar que o ativo mais imprescindível na gestão de segurança da informação é o fator humano, Bruce Schneier, consultor de segurança, afirma que “a segurança não é um produto, ela é um processo" (MITNICK, SIMON, 2003, p. 3). Dizer isso significa que a segurança não é algo a ser vendido e utilizado apenas, mas sim algo a ser estruturado e conquistado, por meio de ações e metodologias.

3 A Lei Geral de Proteção de Dados

A Lei Nº 13.709, conhecida como a Lei Geral de Proteção de Dados, ou apenas LGPD, foi sancionada em 14 de agosto de 2018, e passou a vigorar desde agosto de 2020, de acordo com o site oficial do Planalto (2018). Esta lei tem por objetivo “visar a proteção de dados sensíveis e a criação de regras para coleta e compartilhamento das informações, e dessa forma proteger a privacidade do indivíduo”, conforme afirma Gabriella F. Garcia (2021), analista comercial no Consignet.

A *General Data Protection Regulation* (*GDPR*) é a lei que regula a proteção de dados na Europa, e que serviu de inspiração para o desenvolvimento da lei brasileira. De acordo com Lara Rocha Garcia *et al* (2020, p.16), “a LGPD não tem como escopo os dados das empresas (pessoas jurídicas), mas sim os dados que as empresas têm das pessoas físicas, sejam elas funcionárias, terceiras, clientes, acionistas etc. - ou seja, todo mundo”, dessa maneira, o enfoque da LGPD está na proteção de dados das pessoas físicas, não das jurídicas.

Para compreender a LGPD é importante entender o que ela protege e o que ela regulamenta. O artigo 1º da Lei Nº 13.709 diz que a Lei Geral de Proteção de Dados se “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”. Esta definição trazida pelo

artigo 1º abre espaço para a discussão sobre o que seria tratamento de dados e quais dados poderiam ser classificados como dados pessoais, de acordo com a lei.

No artigo 3º a lei diz em quais cenários de tratamento de dados a LGPD pode ser aplicada, e há três casos em que isso ocorre: quando o tratamento dos dados é realizado no Brasil; quando há viés econômico no tratamento; e quando os dados que são tratados foram coletados no território brasileiro. Ou seja, é uma lei que possui interesse nacional, e toda atividade referente ao tratamento de dados que ocorra no Brasil é abrangida pela LGPD.

Para a LGPD, como disposto na lei no inciso I do artigo 5º, dado pessoal é entendido como a "informação relacionada a pessoa natural identificada ou identificável". Ou seja, o dado pessoal é qualquer tipo de dado que identifica ou pode identificar uma pessoa natural, que é a detentora dos dados. Ao se falar de dados pessoais, é importante entender que há uma definição específica para os dados pessoais sensíveis.

O dado pessoal sensível é o que trata "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural", conforme o inciso II do artigo 5º. A lei entende que este tipo de dado demanda uma atenção especial, por serem dados que trazem risco de discriminação para o titular (pessoa natural) do dado, e no momento do tratamento de dados deste tipo, é necessário um cuidado a mais.

O tratamento de dados, de acordo com o inciso X do artigo 5º, refere a

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2018)

A LGPD conta com três atores no cenário de tratamento de dados: operador, controlador e encarregado de dados. Os agentes de tratamento são os responsáveis pelo tratamento de dados pessoais. Sendo assim, de acordo com o artigo 5º da Lei Nº 13.709

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador. (BRASIL, 2018)

Há dez princípios que devem ser seguidos para que o tratamento de dados pessoais possa ser feito e o artigo 6º da lei expõe cada um desses princípios. Em conjunto com os princípios, há a premissa da boa-fé no tratamento de dados. A boa-fé na LGPD "é fundamental no equilíbrio dos interesses envolvidos, porque há o temor produzido por não se conhecer quem os solicita, tampouco se tem como avaliar os riscos advindos do que se fará com os dados coletados, uma vez que podem ser usados de forma lícita, mas também de forma ilícita", conforme expõe Eduardo Tomasevicius Filho, professor associado do Departamento de Direito Civil da Faculdade de Direito da USP. Para tanto, o Artigo 6º da Lei Nº 13.709 afirma que os

princípios da LGPD são os seguintes: I - finalidade, II - adequação, III - necessidade, IV - livre acesso, V - qualidade dos dados, VI - transparência, VII - segurança, VIII - prevenção, IX - não discriminação e X - responsabilização e prestação de contas.

A LGPD dispõe de situações específicas nas quais o tratamento de dados é permitido para ser realizado pela pessoa física ou jurídica, que é exposto no artigo 7º da lei. É indispensável que o tratamento de dados se enquadre em uma das alternativas que são definidas pela lei.

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão da administração pública federal criado para garantir a fiscalização e aplicação da LGPD, bem como lidar com as sanções previstas em lei para os responsáveis que não se adequarem à mesma. A ANPD também conta com um viés de conscientização, de buscar ensinar aos titulares e pessoas físicas e jurídicas a importância da proteção de dados.

É importante ressaltar que a LGPD não se aplica a alguns casos específicos de tratamento de dados pessoais previstos em lei. Por exemplo, a Lei Geral de Proteção de Dados não abrange o tratamento de dados feito por pessoa natural, cujo objetivo é exclusivamente particular e sem caráter econômico. Ademais, a LGPD estabelece sanções para o caso da lei ser descumprida. As punições podem ser mais brandas, como uma advertência, até mais severas, como multas, e estas podem chegar a até 2% do faturamento da empresa (valor que é limitado pela lei de até R$ 50 milhões). As penalidades passaram a ser aplicadas a partir de 1º de agosto de 2021 (PEREIRA, SILVA, 2021).

Uma pesquisa, desenvolvida por Barcellos Tucanduva Advogados e *E-Commerce* Brasil, teve por objetivo avaliar o quanto os profissionais do setor de *e-commerce* estão preparados para a adoção e adequação a LGPD. A pesquisa revelou que apenas 30% das empresas entrevistadas estão totalmente alinhadas aos requisitos necessários de governança determinados pela lei, e contam com uma

> estrutura de time interno de privacidade, mapeamento de dados, criação de políticas, revisão de questões de segurança da informação, nomeando encarregados de proteção de dados e treinamento da equipe. Além disso, essas empresas dispõem de um processo estruturado de resposta a incidentes e a direitos titulares (E-commerce Brasil, 2021)

A maior parte das empresas entrevistadas, 56%, contam com apenas a criação de políticas de privacidade. Desta forma, os resultados da pesquisa, que abrangeu apenas um setor específico (*e-commerce*), demonstra que a adequação à LGPD ocorreu em partes, portanto muitas empresas ainda não estão totalmente alinhadas com as questões de tratamento de dados conforme a lei exige.

4 Segurança da Informação

Para Hintzberguer *et al* (2018, p. 24), a Segurança da Informação “é a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Ainda de acordo com os autores (2018, p. 26), é essencial que “antes de começarmos a definir uma estratégia de segurança, precisamos saber o que estamos protegendo e do que estamos protegendo”. Ou seja, é importante compreender o que deve ser protegido, antes de simplesmente o proteger.

Conforme diz Hintzberguer *et al* (2018, p. 26), a segurança da informação pode ser

> alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, onde necessário, para assegurar que os objetivos específicos de segurança e do negócio da organização sejam atendidos. Isso deve ser feito em conjunto com outros processos de gerenciamento de negócio. (HINTZBERGUER *et al*, 2018, p. 26)

Ainda conforme os autores,

> A gestão da informação descreve o meio pelo qual uma organização planeja, coleta, organiza, utiliza, controla, dissemina e descarta suas informações de forma eficiente, e através da qual garante que o valor dessa informação seja identificado e explorado em toda a sua extensão
> Quando você traduz essa definição para o português, pode dizer que este campo interdisciplinar se baseia em e combina habilidades e recursos de:
> - Biblioteconomia e ciência da informação.
> - Tecnologia da informação.
> - Gerenciamento de registros.
> - Arquivamento e administração geral.
>
> Seu foco é a informação como um recurso, independentemente da forma física em que ela ocorre. (HINTZBERGUER *et al*, 2018, p. 58)

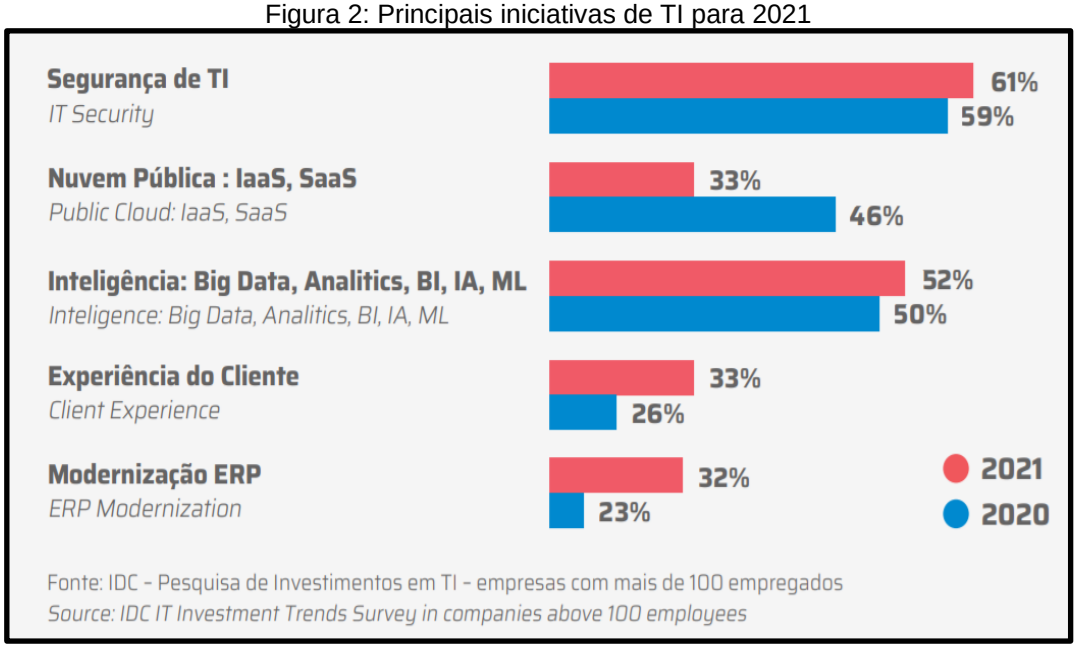
Portanto, pode-se dizer que a Segurança da Informação é a área da computação que visa proteger a informação por meio de uma série de ações, práticas e metodologias, que precisam estar sempre em consonância com os parâmetros estabelecidos pela entidade responsável.

Os resultados divulgados pela *Fortinet* (2021), empresa especializada em segurança cibernética, indicam que o Brasil foi alvo de uma série de ataques cibernéticos, totalizando mais de 8,4 bilhões de tentativas, isso, somente no ano de 2020. Na América Latina e Caribe, houveram 41 bilhões de iniciativas, ou seja, apenas o Brasil foi o foco de 20,4% das tentativas de ataques identificadas pela Fortinet (2021).

O estudo “Mercado Brasileiro de *Software* – Panorama e Tendências 2021”, realizado e publicado em 2021 pela Associação Brasileiras das Empresas de *Software* (ABES), e que fez uso de dados do *IDC* (*International Data Corporation*), diz que em 2020 “os investimentos em TI apresentaram crescimento, atingindo cerca de 2,8% do PIB, fazendo com que o Brasil recuperasse a 9ª posição no *ranking* mundial de TI” (ABES, 2021, p. 4). De acordo com o estudo, “para poder continuar a conduzir seus negócios, as empresas apostaram na introdução de novos produtos, no aumento da segurança em TI, no aumento da produtividade e na redução de custos” (ABES, 2021, p. 4).

O estudo (ABES, 2021, p. 24), com os dados do *IDC*, mostra que uma das tendências para 2021 será o investimento em segurança de tecnologia da informação (TI). Como demonstrado na Figura 2, ao responder a seguinte pergunta “em termos de importância estratégica, quais das seguintes opções estão incluídas nas principais iniciativas de TI em sua organização?”, a segurança de TI aparece em primeiro lugar para as ações de TI das empresas dos participantes da pesquisa.

Figura 2: Principais iniciativas de TI para 2021



Fonte: Pesquisa Mercado Brasileiro de *Software* – Panorama e Tendências 2021, ABES, p. 24

O Relatório Sobre o Prejuízo de um Vazamento de Dados 2020, realizado pela *IBM* (2020, p. 30)*, International Business Machines Corporation,* afirma que ataques mal-intencionados (52%), falhas no sistema (25%) e erro humano (23%) são as causas mais comuns de vazamento de dados. Em valores monetários, "os vazamentos causados por ataques mal-intencionados custaram, em média, US$ 4,27 milhões" (*IBM*, 2020, p. 31). Diante deste fato, a preocupação das organizações com a segurança da informação torna-se uma imprescindível, uma vez que o prejuízo de vazamentos de dados é real e no cenário atual, prováveis de acontecer caso não haja uma estrutura de segurança voltada para isso.

Ainda conforme o relatório da *IBM*, a

> complexidade do sistema de segurança e o teste do plano de resposta a incidentes tiveram o maior impacto no prejuízo total de um vazamento de dados. A complexidade do sistema de segurança, criada pelo número de tecnologias facilitadoras e pela falta de conhecimento interno, aumentou o prejuízo total médio de um vazamento de dados, em média, em US$ 291.870. Entre os fatores que reduziram o prejuízo total médio de um vazamento de dados estavam testes extensivos do plano de resposta a incidentes e o gerenciamento da continuidade de negócios, reduzindo o prejuízo médio, em média, em US$ 295.267 e US$ 278.697, respectivamente. (IBM, 2020, p. 42)

Diante do que é afirmado pelo relatório, os danos e custos com a ocorrência de um vazamento de dados é minimizado caso haja políticas e práticas voltadas para a segurança da informação presentes na organização.

Uma pesquisa desenvolvida pela PwC, a *Global Digital Trust Insights Survey 2021*, divulgada em outubro de 2020, diz que "novas tecnologias e modelos de negócios – e o ritmo acelerado de adoção – trazem novos riscos. Mas, como os freios de alta potência de um carro de corrida, a segurança cibernética torna a mudança digital em alta velocidade muito mais segura". A pesquisa da PwC (2020)

> revela que 57% dos executivos de TI e segurança brasileiros e 55% dos globais planejam aumentar seus orçamentos de segurança cibernética,

> sendo que 60% (51% no mundo) pretendem adicionar equipe cibernética em tempo integral em 2021 – mesmo com a maioria dos executivos afirmando esperar que as receitas de negócios diminuam (62% no Brasil e 64% no mundo). Claramente, a segurança cibernética é mais crítica para os negócios do que nunca. (PWC, 2020)

Para a *Global Digital Trust Insights Survey 2021*, “extrair o máximo valor de cada centavo gasto em segurança cibernética torna-se mais essencial à medida que as entidades se digitalizam: cada novo processo e ativo digital é uma nova vulnerabilidade para ataques cibernéticos”. Diante deste cenário, as empresas se mostram mais dispostas “a considerar a segurança cibernética em todas as decisões de negócios”, ou seja, a segurança passa a ser fator decisivo para a continuidade das organizações.

A fim de esclarecimento, como ressaltado em um artigo no blog da STW Brasil (2020), empresa voltada para soluções em segurança da informação, a

> Segurança cibernética não é apenas outro termo para segurança da informação. Estes são conceitos diferentes. A confusão nesse caso é comum e ocorre por diversos motivos, como pela associação com a tecnologia da informação ou mesmo por que o ambiente digital é a grande ferramenta de informação do nosso tempo.
> Mas então, qual a diferença entre a segurança cibernética e segurança da informação?
> A cibersegurança se aplica a uma parte da segurança da informação com foco na proteção digital, cuidando das ameaças as informações transportadas por meios cibernéticos. Já a segurança da informação tem um foco mais amplo, cuidando da redução de riscos no transporte de dados por qualquer meio, seja digital ou não. (STW, 2020).

Após apresentar e contextualizar sobre a Segurança da Informação e sobre a LGPD, no próximo tópico é abordado a série ISO 27000.

5 A série ISO 27000

A série ISO 27000 contempla as normas que se referem ao Sistema de Gestão de Segurança da Informação (SGSI). Nesta família de normas, a ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013 são as mais conhecidas. De acordo com o site Normas Técnicas (2021), “o SGSI é uma forma de segurança para todos os tipos de dados e informações, e possui quatro atributos básicos: confidencialidade, integridade, disponibilidade e autenticidade”. Portanto, compreende-se que a família ISO 27000 é a responsável por padronizar e garantir a segurança de dados.

De acordo com Hintzberguer *et al* (2018, p. 25), Sistema de Gerenciamento da Segurança da Informação, do inglês *Information Security Management System* (ISMS), é considerado como “parte do sistema total de gerenciamento, baseado em uma abordagem de riscos de negócio, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação”. Ainda de acordo com Hintzberguer *et al* (2018, p. 25), o SGSI possui “estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos”. Ou seja, o SGSI oferece uma visão sistemática para a gestão e proteção de dados (KOSUTIC, 2016).

De acordo com o *ebook* “Panorama Geral ISO 27001:2013/ISO 27701:2020: Sistema de Gestão da Segurança e Informação/Sistema de Gestão de Informação Privada”, escrito por Silvana Ponce e divulgado pela QMS Brasil, empresa voltada para certificações internacionais, diz que (2021, p. 6)

> a norma ISO 27001 – Sistema de Gestão de Segurança da Informação é uma norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão em segurança da informação, enquanto a norma ISO 27701 – Sistema de Gestão da Privacidade da Informação é uma extensão da norma ISO 27001 e ISO 27002 - Código de prática para controles de segurança da informação, tem como objetivo adicionar novos controles ao sistema de gestão da informação para auxiliar as empresas na gestão de riscos de privacidade relacionados com dado pessoal.
> Vale ressaltar que é necessário implementar a ISO 27001 para que possa atender também a ISO 27701, porém não é possível implementar somente a ISO 27701 sem a ISO 27001, pois os controles relacionados a um sistema de gestão de segurança da informação estão na ISO 27001. As duas normas podem ser implementadas simultaneamente como um único sistema de gestão. (PONCE, 2021, p. 6).

A família de normas ISO 27000 contempla uma série de ISOs, cada uma responsável por um segmento específico no que se refere a Segurança da Informação. Devido o enfoque do presente trabalho na ABNT NBR ISO/IEC 27001:2013, é apresentado brevemente, a título de curiosidade, algumas outras normas da ISO 27000.

A seguir, de acordo com Fernando Palma (2013), fundador do site Portal GSTI, expõe e descreve algumas ISOs da série 27000, da seguinte forma

> ISO 27003: contém um conjunto de diretrizes para a implementação do SGSI. Enquanto a 27001 disponibiliza apenas requisitos, aqui obtemos uma orientação detalhada.
> ISO 27004: define métricas de medição para a gestão da segurança da informação. Pode ser uma importante aliada no momento de definir-se metas de níveis de serviço para a segurança da informação, ou mesmo executar o check e act do SGSI.
> ISO 27005: cobre a Gestão de Riscos de segurança da informação. ISO/IEC 27009: norma apoia a indústrias específicas que pretendem trabalhar orientadas às normas ISO 27000.
> ISO 27011: guia de gestão da segurança da informação para empresas de telecomunicações.
> ISO 27031: propõe um guia de princípios/conceitos por trás do papel da segurança da informação para TIC no sentido de garantir a continuidade dos negócios. Inclui diretrizes de mensuração do nível de proteção da organização para a gestão da continuidade na ótica da tecnologia e comunicação.
> ISO 27799: gerenciamento de segurança da informação para a área de saúde. (PALMA, 2013).

Os exemplos apresentados anteriormente mostram como a série ISO 27000 aborda várias áreas e temáticas dentro da Segurança da Informação.

6 A relação entre a família ISO 27000, LGPD e Segurança da Informação

Após apresentar e contextualizar sobre a LGPD, Segurança da Informação e a série ISO 27000, nesta seção é abordada a correlação entre estes temas.

A partir do momento que a LGPD entrou em vigor, a Segurança da Informação foi impactada. Como bem exposto e elucidado por Silvana Ponce (2021, p. 4) na introdução do *ebook* Panorama Geral ISO 27001:2013/ISO 27701:2020: Sistema de Gestão da Segurança e Informação/Sistema de Gestão de Informação Privada,

> vivemos em uma era tecnológica, em que a maior parte das informações está armazenada em dispositivos eletrônicos e o risco de acesso indevido ou vazamento de informações aumenta significativamente.
> O crescente número de vazamentos de informações de usuários nos diversos sites e serviços de armazenamento deixa claro a importância da implementação de controles de segurança da informação. A segurança da informação é entendida como um conjunto de ações para a proteção de dados de pessoas físicas e jurídicas.
> Outro fator que também impulsionou a procura por controles de segurança da informação, foi o surgimento e necessidade de adequação à nova Lei Geral de Proteção de Dados (LGPD). (PONCE, 2021, p. 4).

De acordo com a autora, “a importância da segurança da informação é extrema, independentemente do tamanho da organização ou ramo de atuação, é fundamental tratar as informações como os maiores bens da organização e nunca foi tão importante protegê-los, como no cenário atual” (PONCE, 2021, p. 6). No século XXI, no qual a Segurança da Informação é cada vez mais necessária, a família de normas ISO 27000 desempenha um papel essencial neste caso.

> a norma ISO 27701 especifica requisitos relacionados ao SGPI (Sistema de Gestão da Privacidade da Informação) e diretrizes para os controladores e operadores de dados pessoais, atores com grandes responsabilidades no tratamento de dados. A ISO 27701 é uma extensão dos requisitos da ISO 27001 e de diretrizes da 27002, todos focados em privacidade da informação e complementando as demais normas de segurança da informação com seus requisitos específicos. Para compreensão da ISO 27701 é preciso ter em mente que ela se relaciona a todo instante com as normas de segurança da informação (PONCE, 2021, p. 21).

De outra forma, a ABNT NBR ISO/IEC 27701:2019 possui foco na segurança da informação e proteção de dados pessoais, ao complementar as normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, ao proporcionar como enfoque o Sistema de Gestão da Privacidade da Informação.

A Segurança da Informação baseia-se em três pilares que a ABNT NBR ISO/IEC 27001:2013 segue, e que, conforme o *ebook* Panorama Geral ISO 27001:2013/ISO 27701:2020: Sistema de Gestão da Segurança e Informação/Sistema de Gestão de Informação Privada (2021, p. 19), são os seguintes: princípio da disponibilidade, princípio da integridade e princípio da confidencialidade.

Com o mesmo objetivo da ABNT NBR ISO/IEC 27001:2013, “a ISO 27701 visa proteger as informações e o conjunto de valores compartilhados, governando a proteção de privacidade de dados pessoais (DP), quando tratados em sistemas de tecnologia da informação e comunicação” (PONCE , 2021, p. 22). Assim como a ABNT NBR ISO/IEC 27001:2013, a ABNT NBR ISO/IEC 27701:2019 segue os princípios da disponibilidade, integridade, confidencialidade e outros dois que são

exclusivos da ABNT NBR ISO/IEC 27701:2019. Os princípios específicos desta norma são os princípios do tratamento de dados pessoais e da proteção da privacidade.

De acordo com Rafael Rodrigues (2020), mestre em Sistemas de Informação pela Universidade Federal do Rio de Janeiro, a ABNT NBR ISO/IEC 27701:2019 possui uma correlação de termos com a LGPD, “o que mostra a íntima relação entre a lei e a norma de extensão”. Os termos são os seguintes

> PII – *Personally Identifiable Information* – (LGPD: Dado Pessoal): Dados que possam permitir a identificação do Titular dos Dados.
> PII *Controller* (LGPD: Controlador de Dados): é a parte interessada que determina os objetivos e meios pelos quais os dados pessoais serão tratados;
> PII *Processor* (LGPD: Processador de Dados): é a parte interessada que trata/processa os dados pessoais para o Controlador de Dados, seguindo suas instruções;
> PII *Principal* (LGPD: Titular dos Dados): pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. (RODRIGUES, 2020).

A ABNT NBR ISO/IEC 27701:2019, de acordo com o Rodrigues (2020), traz como foco o

> “*Privacy Information Management System*” (PIMS), que é um sistema de gestão preocupado também com a gestão da privacidade dos dados pessoais. Esse sistema de gestão busca ajudar as empresas a gerenciar os riscos de privacidade relacionados aos dados pessoais, seja ela na relação com o controlador ou com o processador dos dados (RODRIGUES, 2020).

A proteção de dados tornou-se parte essencial quando se refere a Segurança da Informação e, como exposto ao longo do artigo, a preocupação com a privacidade dos dados pessoais é cada vez mais crescente, tanto por parte da legislação (*GDPR* e LGPD) e organizações (certificação ISOs 27000), quanto por parte dos próprios indivíduos. Devido a isto, a *GDPR* entrou em vigor em 2018 na Europa, e em 2020, a LGPD passou a vigorar em território nacional, após dois anos de sua sanção. Em 2019, ABNT NBR ISO/IEC 27701:2019 (enfoque na privacidade de dados) foi publicada, para completar a ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013.

De acordo com Cinara Silva (2021)

> a ISO 27701, assim como a ISO 27001, é uma norma certificável, ou seja, após a implementação a empresa estará apta a receber a auditoria de um organismo acreditado e independente que atestará a conformidade da empresa em relação a estas normas implementadas. A Certificação ISO 27001 traz uma confiança para a empresa em relação a forma como está protegendo suas informações e garantindo a privacidade de dados, mas também, uma confiança para os stakeholders de que as diretrizes utilizadas para esse fim são de uma norma reconhecida e com credibilidade internacional. Além do próprio certificado ser uma evidência prática e muito mais consistente que poderá ser utilizado como evidência a clientes e parceiros de negócios para atestar a segurança da informação e privacidade dos dados pessoais.(SILVA, 2021).

Como discorrido por Silva (2021), a ABNT NBR ISO/IEC 27701:2019, assim como a ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, atestam que a empresa está em conformidade com padrões, protocolos, diretrizes e ações que garantem que a Segurança da Informação é parte da organização.

Um dos princípios da LGPD, como mencionado na Seção 3, é o princípio da segurança, que diz que se faz necessário a “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão”, conforme determinado pelo Artigo 6º da Lei. É exatamente neste ponto que as certificações ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019 enquadram-se, como forma de estabelecer que haja uma maneira de auditar e verificar o que está previsto em Lei, no que tange a Segurança da Informação.

7 Política de Segurança da Informação

Ao considerar os aprendizados adquiridos ao longo do desenvolvimento do artigo sobre a área de Segurança da Informação, conclui-se que uma das medidas que uma organização pode tomar para buscar estar adequada a LGPD e a série de normas ISO 27000 é a criação de uma Política de Segurança da Informação.

De acordo com a *High Security Center* (HSC) Brasil, empresa voltada para a segurança da informação,

> a Política de Segurança da Informação (PSI) pode ser definida como um documento que reúne um conjunto de ações, técnicas e boas práticas para o uso seguro de dados empresariais. Em outras palavras, é um manual que determina as medidas mais importantes para certificar a segurança de dados da organização.
> Para facilitar o entendimento, pode-se dizer que o PSI funciona como o código de conduta interno de um negócio, no qual é estabelecido como os profissionais devem agir, o que é permitido e o que é proibido fazer e quais atitudes devem ser tomadas no caso de uma emergência (HSC Brasil, 2018)

Como resultado do estudo teórico para o desenvolvimento do artigo, uma PSI foi desenvolvida de acordo com a realidade organizacional de uma empresa ainda em estruturação do segmento de eventos e lazer. A empresa, nomeada como X, é situada em Cristais Paulista - São Paulo, planeja ter em média 20 funcionários, com a oferta de diversos serviços (restaurante, pesca esportiva, pesque-pague e eventos em geral). Para gerenciar a infraestrutura, a empresa contará com um *software* terceirizado que será responsável por controlar as operações do setor financeiro e operacional da organização.

Diante da necessidade de desenvolver uma PSI para a empresa, algumas Políticas de Segurança da Informação já estabelecidas por outras organizações foram estudadas. Para efeito de estudo e referência, considerou-se as seguintes PSI:

- Política de Segurança da Informação e Comunicação do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE);
- PSI do Laboratório Nacional de Computação Científica (LNCC) - Santos Dumont;
- PSI *Level 4 Consulting;*
- PSI do Serviço Nacional de Aprendizagem Comercial (SENAC); e
- PSI da FIDD

Para a primeira versão da Política de Segurança da Informação para a empresa X, estimou-se qual seria a realidade organizacional da mesma, baseado nas informações que foram repassadas pelo setor de recursos humanos da organização.

Junto a isto, e por se tratar de uma empresa ainda em fase de estruturação e não estar em plena atividade e funcionamento, a PSI foi definida com base em outras PSI.

Desta forma, a Política de Segurança da Informação abrange os princípios da Segurança da Informação que são baseados na ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019, respeita a LGPD ao informar quem é o operador, controlador e encarregado.

A PSI apresenta quais são os deveres e responsabilidades de cada setor da empresa (diretoria, recursos humanos, administrativo, operacional e colaboradores externos). O foco da Política de Segurança está nas diretrizes e respostas a acidentes de segurança da informação, nos quais o documento detalha o que deve ser seguido pelos colaboradores para manter a Segurança da Informação na empresa X, e o que deve ser feito caso ocorra uma quebra na Segurança da Informação.

O documento com a primeira versão da PSI para a empresa está disponível para consulta, de forma *online,* no *link* <https://drive.google.com/file/d/1x_QclMoopIcge_jwwSMiKxSCTajxv-1l/view?usp=sharing> ou através do *QR Code* abaixo:

Figura 3: *QR Code* para acesso à Política de Segurança da Informação

Fonte: as autoras

8 Conclusão

Como exposto ao longo do artigo, pode-se dizer com clareza que os dados atualmente são ativos essenciais para a sobrevivência de uma organização. Juntamente com esta importância, a preocupação com a segurança da informação entra em foco como um diferencial competitivo para os negócios.

Na busca de compreender a relação entre a Lei Geral de Proteção de Dados, Segurança da Informação e a série ISO 27000, pesquisou-se individualmente cada item para que, posteriormente, fosse possível a análise da correlação entre as temáticas.

Ao final do estudo teórico, pode-se concluir que a LGPD, ao regulamentar a proteção de dados sensíveis em território brasileiro, relaciona-se intimamente com a ABNT NBR ISO/IEC 27701:2019, que visa proporcionar um olhar

atento para a segurança dos dados pessoais, e com a ABNT NBR ISO/IEC 27001:2013 que tem como foco estabelecer diretrizes para lidar com a Segurança da Informação nas organizações.

Como desfecho do presente artigo, apresenta-se uma Política de Segurança para a empresa X. Por decorrência disto, para trabalhos futuros, pode vir a ser desenvolvido um mapeamento do fluxo de dados da empresa X, para que a empresa compreenda os processos que possui e que envolvem dados. Recomenda-se a revisão periódica da PSI já definida, de forma a mantê-la atualizada e alinhada aos objetivos e realidade organizacional.

Referências

A América Latina sofreu mais de 41 bilhões de tentativas de ataques cibernéticos em 2020. Fortinet. Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020> Acesso em: 06 ago. 2021

ABNT NBR ISO/IEC 27001:2013. ABNT Catálogo. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=306580>. Acesso em: 01 nov. 2021.

ABNT NBR ISO/IEC 27002:2013. ABNT Catálogo. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 01 nov. 2021.

ABNT NBR ISO/IEC 27701:2019 Versão Corrigida:2020. . ABNT Catálogo. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=437612>. Acesso em: 01 nov. 2021.

Apenas 30% das empresas estão completamente adequadas à LGPD. *E-commerce* Brasil. Disponível em: <https://www.ecommercebrasil.com.br/noticias/adequacao-empresas-a-lgpd/>. Acesso em: 03 ago. 2021.

Cyber Security: Descubra as principais diferenças entre segurança cibernética e segurança da informação. STW Brasil. Disponível em: <https://www.stwbrasil.com/blog/cyber-security-diferencas-seguranca-cibernetica-e-seguranca-informacao/>. Acesso em: 08 ago. 2021.

Data Never Sleeps 8.0. Domo. Disponível em: <https://www.domo.com/learn/data-never-sleeps-8>. Acesso em: 27 maio 2021.

Digital 2020 October Global Statshot Report (October 2020) v01. Slide Share. Disponível em: <https://www.slideshare.net/DataReportal/digital-2020-october-global-statshot-report-october-2020-v01?ref=https://s3-ap-southeast-1.amazonaws.com/>. Acesso em: 27 maio 2021.

Facebook Reports Fourth Quarter and Full Year 2020 Results. Investor Relations. Facebook. 2021. Disponível em: <https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx>. Acesso em: 27 maio 2021.

FILHO, Eduardo Tomasevicius. **O princípio da boa-fé na Lei Geral de Proteção de Dados**. Conjur. 2020. Disponível em: <https://www.conjur.com.br/2020-mar-09/direito-civil-atual-principio-boa-fe-lgpd/>. Acesso em: 19 maio 2021.

GARCIA, Gabrielle Franciane. **Lei Geral de Proteção de Dados e a ISO 27001**: foco na segurança da informação. Consignet. Disponível em: <https://www.consignet.com.br/blog/lei-geral-protecao-iso-27001/>. Acesso em: 12 abr. 2021.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados (LGPD)**: guia de implementação. 1. ed. Edgar Blüncher, 2020. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/183221/pdf/>. Acesso em: 12 abr. 2021.

HINTZBERGER, Jules et al. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. 3. ed. Rio de Janeiro, Brasport, 2018. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/160044/epub/>. Acesso em: 11 mar. 2021.

KOSUTIC, Dejan. **O que é um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ISO 27001?** Advisera. 2016. Disponível em: <https://advisera.com/27001academy/pt-br/blog/2016/05/30/o-que-e-um-sistema-de-gestao-de-seguranca-da-informacao-sgsi-de-acordo-com-a-iso-27001//>. Acesso em: 19 maio 2021.

Lei Nº 13.709 de 14 de agosto de 2018. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 abr. 2021.

MARÓSTICA, Eduardo; MARÓSTICA, Neiva Alessandra Coelho; BRANCO, Valdec Romero Castelo. **Inteligência de Mercado**. 2. ed. São Paulo, Cengage Learning, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788522129546/>. Acesso em: 27 maio 2021.

Mercado Brasileiro de *Software* – Panorama e Tendências 2021. ABES. Disponível em: <https://abessoftware.com.br/wp-content/uploads/2021/08/ABES-EstudoMercadoBrasileirodeSoftware2021v02.pdf> Acesso em: 06 ago. 2021

MITNICK, Kevin D.; SIMON, William L. **Mitnick A arte de enganar**: ataques de hackers: controlando o fator humano na segurança da informação. 1. ed. São Paulo, Pearson Makron Books. 2003. Disponível em: <https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzdGFmZnR1dG9zfGd4OjQ0Njg2ZTgyYWJjODg1MWQ >. Acesso em: 03 ago. 2021.

PALMA, Gustavo. **As normas da família ISO 27000**. Portal GSTI. Disponível em: <https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html>. Acesso em: 03 ago. 2021.

PEREIRA, Fabio Luiz Barboza; SILVA, Cecília Alverton Coutinho. **Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT**. VC S/A. Disponível em: <https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit/>. Acesso em: 27 maio 2021.

Política de Segurança da Informação e Comunicação. SEBRAE. Disponível em: <https://www.sebraepr.com.br/wp-content/uploads/Politica_de_Seguranca_da_Informacao_e_Comunicacao.pdf>. Acesso em: 02 set. 2021.

Política de Segurança da Informação. HSC Brasil. Disponível em: <https://www.hscbrasil.com.br/politica-de-seguranca-da-informacao/>. Acesso em: 02 set. 2021.

Política de Segurança da Informação. FIDD Group. Disponível em: <https://www.fiddgroup.com/wp-content/uploads/2020/10/Poli%CC%81tica-de-Seguranc%CC%A7a-da-Informac%CC%A7a%CC%83o-e-Seguranc%CC%A7a-Ciberne%CC%81tica-v2.pdf>. Acesso em: 02 set. 2021.

Política de Segurança da Informação. Laboratório Nacional de Computação Científica (LNCC) - Santos Dumont. Disponível em: <https://sdumont.lncc.br/archives/Politica%20de%20Seguranca%20da%20Informacao%20LNCC%20Santos%20Dumont-.pdf>. Acesso em: 02 set. 2021.

Política de Segurança da Informação. *Level 4 Consulting*. Disponível em: <http://www.level4.com.br/upload/psi_level4_revisado_v2.pdf>. Acesso em: 02 set. 2021.

Política de Segurança da Informação. SENAC. Disponível em: <https://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf>. Acesso em: 02 set. 2021.

PONCE, Silvana. **Panorama Geral ISO 27001:2013/ISO 27701:2020**: Sistema de Gestão da Segurança e Informação/Sistema de Gestão de Informação Privada. QMS Brasil. Acesso em: <https://qmsbrasil.com.br/wp-content/uploads/2021/06/iso-27001-iso-27701-compactado.pdf>. Acesso em: 12 ago. 2021.

QR Code Generator. Disponível em: <https://br.qr-code-generator.com/>. Acesso em: 01 nov. 2021.

Redefina sua estratégia cibernética, desenvolva a liderança para os novos tempos. *Global Digital Trust Insights Survey* 2021. PwC. Disponível em: <https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2020/global-digital-trust-insights/estrategia-cibernetica.html>. Acesso em: 07 ago. 2021.

Relatório sobre o prejuízo de um vazamento de dados 2020. IBM. Disponível em: <https://www.ibm.com/downloads/cas/OW6BN657>. Acesso em: 06 ago. 2021.

Repense seu orçamento cibernético para tirar mais proveito dele. *Global Digital Trust Insights Survey* 2021. PwC. Disponível em: <https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2020/global-digital-trust-insights/orcamento-cibernetico.html>. Acesso em: 07 ago. 2021.

RODRIGUES, Gustavo. **O Brasil teve o maior vazamento de dados de sua história. E agora?** Instituto de Referência em Internet e Sociedade. Disponível em: <https://irisbh.com.br/o-brasil-teve-o-maior-vazamento-de-dados-de-sua-historia-e-agora/>. Acesso em: 27 maio 2021.

RODRIGUES, Rafael. **O que é ISO 27701?** Promove Soluções. Disponível em: <https://promovesolucoes.com/o-que-e-iso-27701/>. Acesso em: 12 ago. 2021.

Segurança de Dados no Brasil: a visão da sociedade (recorte regional). FEBRABRAN. Disponível em: <https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/RELAT%C3%93RIO%20OBSERVAT%C3%93RIO%20FEBRABAN%20-%20RECORTE%20REGIONAL%20-%20JUN%2021%20-%20SEGURAN%C3%87A%20DE%20DADOS%20NO%20BRASIL_VF.pdf>. Acesso em: 02 ago. 2021.

Série ISO 27000. Normas Técnicas. Disponível em: <https://www.normastecnicas.com/iso/serie-iso-27000/>. Acesso em: 11 mar. 2021.

SILVA, Cinara. ***Qual a relação da ISO 27001 com a ISO 27701?*** Certificação ISO. Disponível em: <https://certificacaoiso.com.br/qual-a-relacao-da-iso-27001-com-a-iso-27701/>. Acesso em: 13 ago. 2021.

TAURION, Cezar. ***Big Data***. 1. ed. Rio de Janeiro, Brasport, 2013. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/160676/>. Acesso em: 27 maio 2021.

Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025. Statista. Disponível em: <https://www.statista.com/statistics/871513/worldwide-data-created/>. Acesso em: 27 maio 2021.