

CONGRESSO NACIONAL DE DIREITO EMPRESARIAL

GOVERNANÇA CORPORATIVA E COMPLIANCE

Organizadores:
Mariana Ferreira de Souza
Patricia Fernanda Macedo Possamai
Júlia Helena Ribeiro Duque Estrada Lopes

**Novas tecnologias
aplicadas às falências e
recuperações e
governança corporativa
e compliance: congresso
nacional
de direito empresarial**

1ª edição

Santa Catarina

2024



CONGRESSO NACIONAL DE DIREITO EMPRESARIAL

GOVERNANÇA CORPORATIVA E COMPLIANCE

Apresentação

Entre os dias 3 e 5 de junho de 2024, a Faculdade Milton Campos, em parceria com o Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI, realizou o Congresso Nacional de Direito Empresarial: Perspectivas e Desafios da Falência e da Recuperação de Empresas. O evento, em formato híbrido, contou com a presença de renomados especialistas e promoveu discussões profundas sobre temas relevantes para o Direito Empresarial contemporâneo.

Trata-se de um evento científico vinculado ao Programa de Mestrado em Direito nas Relações Econômicas e Sociais da Faculdade Milton Campos, com conexão temática às suas duas linhas de pesquisa, “O Direito Empresarial na Ordem Econômica Brasileira e Internacional” e “Relações Econômicas, políticas públicas e tensões entre autonomia privada e interferência estatal”, e que almejou expandir o importante debate sobre as repercussões jurídicas que as falências e a recuperação de empresas acarretam para o Direito Empresarial pátrio, com o convite ao público interno e externo para a submissão de trabalhos relacionados aos seguintes eixos temáticos: contextos e premissas das falências e da recuperação judicial e extrajudicial, novas tecnologias aplicadas às falências e recuperações, governança corporativa e compliance, Environmental, Social and Governance (ESG), startups e empreendedorismo, crimes falimentares, arbitragem e solução de conflitos societários e ética empresarial.

A abertura do congresso, no dia 3 de junho, foi marcada pelo lançamento do livro "Direito Governança Corporativa e Startups", coordenado por Fabrício de Souza Oliveira (UFJF) e José Luiz de Moura Faleiros Júnior (Milton Campos). O evento, que ocorreu às 18h, foi amplamente prestigiado pela comunidade jurídica!

Após o credenciamento, teve início o primeiro painel do evento. O Prof. Dr. Vinicius Jose Marques Gontijo (Milton Campos) apresentou importante palestra sobre o "Plano de Recuperação Judicial Alternativo: Apresentação Impactos e Responsabilidade Civil", seguido pelo Prof. Dr. Tiago Gomes de Carvalho Pinto (Milton Campos), que discutiu "Novas perspectivas jurisprudenciais em matéria de falência e recuperação de empresas". As apresentações encerraram o primeiro dia de atividades com debates enriquecedores sobre os impactos e desafios das novas jurisprudências no campo da recuperação judicial.

O segundo dia iniciou-se com o credenciamento, seguido do segundo painel. O Prof. Dr. Moacyr Lobato de Campos Filho (PUC Minas) abordou "Conciliações e Mediações na Recuperação Judicial: Eficácia Prática", destacando a importância e os benefícios dessas práticas. Em seguida, o Prof. Dr. Luciano Santos Lopes (Milton Campos) falou sobre "Crime Falencial: Bem Jurídico Tutelado", e o Prof. Dr. Eronides Aparecido Rodrigues Santos (MPSP) trouxe reflexões sobre o "Direito Recuperacional Falimentar e Empresarial Moderno". A mesa foi mediada pela mestrandia Júlia Ribeiro Duque Estrada.

O terceiro painel contou com a participação da Prof^a. Ms. Taciani Acerbi Campagnaro Colnago Cabral (MG), que discutiu a "Administração Judicial: Responsabilidade Civil". O Prof. Dr. Victor Barbosa Dutra (BA) apresentou os "principais entendimentos" do Fórum Nacional de Recuperação Empresarial e Falências do CNJ, seguido pelo Prof. Dr. Cássio Cavalli (SP) que abordou "Aspectos Tributários na Reforma da Lei de Falências e Recuperação de Empresas". O Prof. Dr. Hugo Leonardo Teixeira (Milton Campos) finalizou com uma discussão sobre "Administração judicial e reformas à Lei de Falências e Recuperações", sob a mediação da Mestra Ana Flávia Valladão Ferreira.

No período da tarde, iniciou-se o quarto painel com a presença do Prof. Dr. Gladston Mamede (MG), que discutiu "Holding Familiar Recuperação e Falência", seguido pelo Prof. Dr. Fabrício de Souza Oliveira (UFJF) com "Reflexões metodológicas em governança corporativa". O Prof. Dr. Gustavo Ribeiro Rocha (Milton Campos) finalizou com "Preservação da empresa na falência", com mediação do mestrando Marcelo Cezar Teixeira.

O quinto painel, às 15:00h, trouxe a Prof^a. Dr^a. Viviane Coelho de Séllos-Knoerr (UniCuritiba) abordando a "Resiliência e recuperação extrajudicial de empresas afetadas pela catástrofe climática de 2024 no RS/Brasil". Em seguida, o Prof. Dr. Pedro Freitas Teixeira (OAB/RJ) discutiu "Recuperação Judicial e Sociedade Anônima do Futebol", seguido pelo Prof. Ms. José Luiz de Moura Faleiros (TJMG) que falou sobre "Compliance criminal e Sociedade Anônima do Futebol". A mesa foi mediada pelo mestrando Amadeu Pedersoli.

A conferência de encerramento foi realizada pelo Prof. Dr. Jason Soares de Albergaria Neto (Milton Campos), que apresentou o tema "O compliance como instrumento da recuperação judicial de empresas", finalizando o segundo dia com reflexões importantes sobre a aplicação do compliance na recuperação judicial.

O último dia do congresso foi dedicado aos grupos de trabalho, realizados de forma on-line a partir das 08:00h. O evento contou com a participação de oradores de diversos estados da federação, demonstrando a abrangência e a relevância do evento. Os estados representados

pelos oradores dos Grupos de Trabalho foram: Santa Catarina (SC), Minas Gerais (MG), São Paulo (SP), Rio de Janeiro (RJ), Espírito Santo (ES), Rio Grande do Norte (RN), Bahia (BA), Rio Grande do Sul (RS), Goiás (GO), Pernambuco (PE), Ceará (CE), Pará (PA), Mato Grosso do Sul (MS) e Paraná (PR). Os temas discutidos foram variados e de grande relevância:

- GT 1 – Falências e Recuperação Judicial e Extrajudicial: Contextos e Premissas

o Coordenadores: Luiz Felipe de Freitas Cordeiro, Marcelo Cezar Teixeira e Victor Hugo Kohnert

- GT – Novas Tecnologias Aplicadas às Falências e Recuperações, Governança Corporativa e Compliance

o Coordenadores: Mariana Ferreira de Souza, Patricia Fernanda Macedo Possamai e Júlia Helena Ribeiro Duque Estrada Lopes

- GT – ESG e Função Social da Empresa

o Coordenadores: José Luiz de Moura Faleiros Júnior, Iani Fávaro Casagrande e Nicácio Carvalho

- GT – Startups e Empreendedorismo

o Coordenadores: Matheus Antes Schwede, Luiz Felipe de Freitas Cordeiro e Juan Lemos Alcasar

- GT – Crimes Falenciais e Empresariais, Empresa e Sustentabilidade

o Coordenadores: André Vecchi, Pedro Felipe Naves Marques Calixto e Julia Garcia Resende Costa

- GT – Arbitragem e Solução de Conflitos Societários

o Coordenadores: Arthur Magno e Silva Guerra, Júlia Helena Ribeiro Duque Estrada Lopes e Marcelo Cezar Teixeira

Em sua primeira edição, o Congresso Nacional de Direito Empresarial proporcionou uma rica troca de conhecimentos e experiências, contribuindo significativamente para o debate sobre as falências e recuperações judiciais e extrajudiciais no Brasil. As discussões realizadas e os trabalhos apresentados reforçam a importância da contínua atualização e reflexão sobre esses temas no cenário jurídico e empresarial.

O evento, com estreita conexão com o Programa de Mestrado em Direito nas Relações Econômicas e Sociais da Faculdade Milton Campos, evidenciou o compromisso da instituição com o aprofundamento e a disseminação de conhecimentos no campo do Direito. Além disso, a presença de renomados palestrantes e a ativa participação dos mestrandos e professores reforçaram a importância acadêmica e prática dos temas debatidos.

Acreditamos que, ao proporcionar um espaço para o debate e a troca de conhecimentos, estamos contribuindo significativamente para o avanço do Direito no Brasil. Esperamos, assim, continuar fomentando essas valiosas interações acadêmicas e profissionais em muitas futuras oportunidades, consolidando este congresso como um evento de referência no calendário jurídico nacional.

Agradecemos profundamente a todos os participantes, cujas contribuições enriqueceram sobremaneira o evento, e ao CONPEDI pelo imprescindível apoio na realização do congresso. Proporcionar debates sobre falências e recuperações judiciais e extrajudiciais é fundamental para a evolução do Direito Empresarial, e esse encontro destacou-se como um espaço privilegiado para tais discussões, promovendo avanços significativos na área.

Nova Lima-MG, 10 de julho de 2024.

Prof^a. Dr^a. Tereza Cristina Monteiro Mafra

Diretora Geral do Programa de Pós-Graduação em Direito

Faculdade Milton Campos

Prof. Dr. André Rubião Resende

Coordenador do Mestrado em Direito nas Relações Econômicas e Sociais

Faculdade Milton Campos

Profª. Ms. Ana Luísa Coelho Perim

Coordenadora Geral do Curso de Direito

Faculdade Milton Campos

Prof. Dr. José Luiz de Moura Faleiros Júnior

Coordenador dos cursos de pós-graduação lato sensu

Faculdade Milton Campos

Prof. Dr. Jason Soares de Albergaria Neto

Professor do Mestrado em Direito nas Relações Econômicas e Sociais

Faculdade Milton Campos

Prof. Dr. Vinícius José Marques Gontijo

Professor do Mestrado em Direito nas Relações Econômicas e Sociais

Faculdade Milton Campos

**A ADOÇÃO DA ISO/IEC 27001 E DA ISO/IEC 27018 NO CONTEXTO DA
SEGURANÇA DA INFORMAÇÃO INTRODUZIDA PELA LEI GERAL DE
PROTEÇÃO DE DADOS (LGPD)**

**THE ADOPTION OF ISO/IEC 27001 AND ISO/IEC 27018 IN THE CONTEXT OF
INFORMATION SECURITY INTRODUCED BY THE GENERAL DATA
PROTECTION LAW (LGPD)**

Giulia Name Vieira ¹
Diego Ramos Pinzolas ²
José Luiz de Moura Faleiros Júnior ³

Resumo

A partir da criação de novas tecnologias, vulnerabilidades surgem. Sob esse viés, urge a necessidade de proteger de maneira eficaz o compartilhamento de dados pessoais, evitando o uso indevido por terceiros, sendo imprescindível que haja regulamentação. No texto, há a abordagem das normatizações ISO/IEC 27001 e ISO/IEC 27018 em um contexto de inovações tecnológicas e regulamentação do ambiente virtual, em que, atrelados à Lei Geral de Proteção de Dados, auxiliam na segurança informacional de cada usuário. Com isso, dificulta a ocorrência da difusão, divulgação e do uso de dados pessoais, sensíveis ou não, por terceiros mal-intencionados.

Palavras-chave: Lei geral de proteção de dados (lgpd), Segurança da informação, Iso/iec 27001, Iso/iec 27018, Segurança virtual

Abstract/Resumen/Résumé

This article addresses the adoption of ISO/IEC 27001 and ISO/IEC 27018 standards in the context of technological innovations and regulation of the virtual environment. The information security parameter requirements of the General Data Protection Law can be met by adopting internationally certified standards. Both data clouds and information storage are assets of economic value that will have greater protection when adopting vulnerability protection procedures and breach response techniques.

Keywords/Palabras-claves/Mots-clés: General data protection law (lgpd), Information security, Iso/iec 27001, Iso/iec 27018, Virtual security

¹ Graduanda em Direito pela SKEMA Business School. E-mail: giulianamevieira@gmail.com

² Graduando em Direito pela Universidade Federal de Minas Gerais. E-mail: diego.pinzolas@gmail.com

³ Orientador. Doutor em Direito pela USP. Mestre e Bacharel em Direito pela UFU. E-mail: josefaleirosjr@outlook.com

1. Introdução

O avanço das tecnologias é acompanhado por mudanças em todas as esferas da vida, com a atenção à segurança da informação e aos dados pessoais alcançando patamares internacionais. Ao tratar da segurança, logo associa-se a uma ideia físico-material de tutela de certo bem que é mandamental sua proteção. A perspectiva de segurança da informação, após a primeira década do século XXI, sofreu modificações, uma vez que usuários e empresas de grande porte perceberam que seus dados e os de outros agentes em sua posse eram bens de alto valor e visados por pessoas mal-intencionadas (Fontes, 2017). Com isso, surge a demanda por métodos eficazes de proteção nas redes de sistemas interligadas mundialmente, em que lacunas de proteção podem surgir e ser exploradas por criminosos.

A padronização, a adoção de parâmetros comuns e a governança dos sistemas tornam mais eficiente e rápida as abordagens quanto a um tema específico, quando é objeto comum de conhecimento diversos operadores (Barbieri, 2019). Essas técnicas, além de proporcionarem certeza quanto ao objeto trabalhado, possibilitam o estudo e o aprofundamento das matérias de tecnologia e segurança, com a certeza de que os parâmetros mínimos serão entendidos por qualquer habitado com as normas. Disso, extrai-se vantagens das iniciativas de padronização, uma vez que internacionalizadas, difundidas e adotadas, essas serão um mecanismo para balizar as medidas de segurança para a proteção dos dados sensíveis.

A análise, no presente texto, das medidas de padronização seguirá os padrões internacionalmente adotados da Organização Internacional de Normalização (ISO), em especificidade dos padrões ISO27001 e ISO27018 e a legislação brasileira de proteção de dados, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.853 de 2019).

A pesquisa será conduzida utilizando o método dedutivo, iniciando com uma explicação contextual para compreender as circunstâncias e os termos envolvidos. A abordagem incluirá uma análise jurídica exploratória que objetiva delinear as nuances e implicações do tema em estudo. Esse processo metódico permitirá uma progressão lógica dos argumentos, cujo método sistemático busca fornecer uma fundamentação sólida para as conclusões tiradas, garantindo assim uma análise profunda e bem fundamentada do tema-problema, pautando-se pela pós-normalização da proteção de dados e informações pelas empresas que lidam com informações fornecidas por seus clientes.

2. Organização Internacional de Normatização (ISO)

Criada no ano de 1946, a *International Organization for Standardization* (Organização Internacional de Normalização, ISO) é um órgão independente que emana normas e padronizações para diversas áreas (Inmetro, 2024). A adoção é global das mais variadas medidas e procedimentos, como a ISO 9000, que trata da gestão da qualidade, a ISO 14000, da gestão do meio ambiente e a ISO 45001, com enfoque na gestão de riscos em ambientes de trabalho. No que tange ao objeto do trabalho, as normas pertinentes de segurança tecnológica são adotadas por pequenas empresas – com pouca quantidade de informações sensíveis –, instituições de médio porte, pelas maiores companhias de tecnologia do mercado, as denominadas *Big-Techs*, e por órgãos governamentais.

Os órgãos de normatização de cada país recebem as propostas da ISO e as traduzem e interpretam para a aplicação como padrão de normatização nacional. Ademais, como medida para a democratização e a adoção ampla dessas normas, é fundamento das ISOs o uso de linguagem técnica, simples e acessível, com orientações claras e eficientes, que passam pelo crivo de órgãos especializados na área, além da colaboração de especialistas para a elaboração normativa (Microsoft, 2023).

2.1. ISO/IEC 27001

A ISO/IEC 27001 é uma norma criada no ano de 2005, com atualização última no ano de 2022, resultante da parceria da Organização Internacional de Normalização (ISO) com a *International Electrotechnical Commission* (Comissão Eletrotécnica Internacional, IEC), visando criar uma padronização, políticas e procedimentos de segurança quanto às informações digitais em posse de órgãos públicos ou privados de variadas proporções.

Há a criação de um procedimento *Information Security Management System* (Sistema de Gestão de Segurança da Informação, ISMS) relacionado a um sistema de proteção de dados genérico que estabelece medidas próprias a serem seguidas para garantir a segurança da informação manipulada pelas empresas. A consecução do sistema de segurança da informação é feita pela adoção de requisitos listados nas cláusulas da norma, abordando pontos como a segurança física da organização, segurança de dados, análise de aspectos vulneráveis, organização interna, gestão de incidentes, práticas de controle de acesso (em sistemas e no ambiente físico) e tecnologia de informação (Hintzbergen; Hintzbergen; Baars; Smulders,

2018). A análise crítica e o monitoramento periódico do desempenho e da eficácia do ISMS contribui para a revalidação da certificação, visto que os riscos e as brechas estão em constante mudança, consequência da ascensão tecnológica.

A integridade dos métodos de processamento e informações, assim como a proteção contra fraudes informáticas, são pontos triunfantes, fruto da adoção da norma. O processo de implementação oscila em tempo de duração, uma vez que é variável o tamanho da empresa e a necessidade de implementação de novas práticas. A mudança para a conformidade dos sistemas com a ISO 27001 exige da organização planejamento, aplicação, averiguações prévias, ajustes sugeridos por especialistas e, por fim, uma análise de auditoria para a certificação de acordo com os *standards* da ISO 27001. Com isso, a norma é uma possibilidade para a adaptação das entidades que buscam proteção das informações no meio digital e conformidade com exigências normativas.

2.2 ISO/IEC 27018

A normatização da ISO 27018 é derivada da ISO 27000, que também abrange a segurança de dados no meio eletrônico. A especificidade desta norma reside no fato de ser voltada para sistemas que lidam com materiais privados nos serviços de “nuvem”. Tal termo se refere a um conjunto interligado de redes de servidores que armazenam e interpretam as informações inseridas (Microsoft, 2024) sendo que um único ecossistema lida com centenas de dados.

Nesse diapasão, a segurança dos dados armazenados nessas redes em nuvem são objeto de preocupação, visto que há valor financeiro e pessoal envolvido na manipulação desses dados sensíveis. O objeto da normatização em questão é a codificação e padronização de procedimentos e práticas para a proteção das informações que identificam pessoalmente os indivíduos (*personally identifiable information*, PII) nos processos internos das nuvens de armazenamento.

Na ISO 27018 há 13 tópicos específicos sobre os métodos a serem aplicados na política de proteção de dados, incluindo organização da política de segurança, controle dos recursos humanos envolvidos, criptografia, segurança das operações e técnicas de gerenciamento de incidentes. Essa normatização objetiva empresas que lidam ou fornecem produtos de armazenamento de dados pessoais em redes especializadas, sendo acessível a todos os

envolvidos nessa cadeia. Na eventualidade de uma empresa não ser a responsável direta pela gestão de conteúdos em nuvem, surge o dever de exigência por esse tipo de certificação, uma vez que, é de sua responsabilidade legal garantir a segurança de suas informações sensíveis e das armazenadas de seus clientes (Gonçalves, 2024). Em suma, as nuvens de dados são bens de alto valor para qualquer usuário e empresa, portanto a segurança no meio digital deve ser uma das prioridades em todos os cenários.

3. A Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei nº 13.709, de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados e conhecida por “LGPD”, para Eugênio Facchini Neto e Fabiana Rampazzo Soares (2021), consubstancia-se em um microssistema que trata de dados pessoais, acoplando-se ao sistema jurídico vigente e tendo como uma das consequências frente às questões centrais da lei o vazamento de dados, sobretudo sob a ótica do direito dos danos. Tal lei possui como abrangência toda a Federação, diferenciando das normatizações das ISOS, tendo em vista que essas são voluntárias quanto à aceitação.

Nesse sentido, a necessidade de proteção crescente dos dados pessoais e das informações sensíveis no ambiente digital cria uma demanda de padronização nos sistemas de segurança, sendo conjuntamente exigidas por normas do direito internacional e doméstico. O direito estatal também se modifica face às novas tecnologias exigindo, por meio da criação de leis de proteção de dados, que os padrões de segurança sejam obrigatórios para uma empresa manipular materiais de clientes, por exemplo. A adaptação é constante e segue a cadência do surgimento de inovações tecnológicas e complexificação dos sistemas digitais, exigindo um esforço incessante para a garantia da segurança no espaço digital.

Ante o exposto, o vazamento de dados no mundo atual tornou-se um fenômeno cada vez mais comum. Sobre tal fato, tem-se:

O vazamento de dados em uma sociedade de informação ocorre, muitas vezes, por meio de sucessivas transferências ou apropriações de dados que, mesmo em casos de investigação policial, se tem dificuldade em reconstituir. A fonte originária de dados pessoais expostos indevidamente nem sempre é passível de identificação (*trackable*) e caminho percorrido pelos dados pessoais frequentemente restará demonstrado mais a título de efetiva probabilidade que de certeza matemática. (Schreiber, 2021)

Dessa forma, a LGPD se relaciona com as ISOS expostas por também visar à proteção e garantia da privacidade dos dados pessoais, sejam eles sensíveis ou não, dos usuários, fornecendo um maior controle e, conseqüentemente, uma maior segurança aos que utilizam.

Portanto, é possível inferir que ambos reforçam o direito pleno dos titulares de dados. Com isso, será viável que se tenha uma maior transparência e ampla condição de acesso aos dados próprios, propiciando um maior conhecimento por parte dos cidadãos frente à importância da proteção das informações pessoais, bem como os danos de uma divulgação indiscriminada.

4. Considerações finais

Nesta brevíssima exposição, procurou-se destacar a relevância das ISOS, bem como a sua relação com a LGPD, a fim de, eventualmente conter situações hodiernas, deixando os dados pessoais e os dados pessoais sensíveis dos indivíduos em situações de risco.

Isso posto, é importante ressaltar que a combinação entre a LGPD e as ISOS provoca uma maior força e eficácia quanto ao controle dos dados pessoais, sobretudo em ambientes virtuais, auxiliando, portanto, na criação e manutenção de ambientes mais seguros, atrelados às boas práticas dos indivíduos.

Dessa forma, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme abordado pelo Art. 1º da LGPD, urge que as ISOS sejam implementadas e seguidas por todos, permitindo um ambiente de segurança a eles. Através desse âmbito, torna-se possível uma construção de confiança generalizada, aliada a práticas transparentes. A partir de tal fato, as informações serão armazenadas com mais robustez, evitando que terceiros de má-fé obtenham acesso a dados alheios protegidos.

Portanto, com uma ação conjunta entre entes públicos e privados, almeja-se que o Brasil prossiga na evolução da proteção de dados pessoais, implementando cada vez mais medidas de segurança que ajudem na mitigação de danos frente a dados de terceiros divulgados sem prévia autorização. Através dessas medidas, será possível evitar abusos de publicidade das informações e de exposição dos indivíduos de maneira indevida.

Referências

ABNT; ISO; IEC. *Norma brasileira ABNT NBR ISO/IEC 27001*. 2006. Disponível em: <https://jkolb.com.br/wp-content/uploads/2016/09/ABNT-NBRISOIEC27001-20060331Ed1.pdf>. Acesso em 11 maio 2024.

BARBIERI, Carlos. *Governança de dados: práticas, conceitos e novos caminhos*. Rio de Janeiro: Alta Books, 2019.

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 4 maio 2024.

FACCHINI NETO, Eugênio; SOARES, Fabiana Rampazzo. Responsabilidade civil pela violação ao dever de proteção de dados na LGPD. In: PINHO, Anna Carolina (Org.). *Discussões sobre Direito na Era Digital*. Rio de Janeiro: GZ Editora, 2021.

FONTES, Edison Luiz Gonçalves. *Segurança Da Informação*. São Paulo: Saraiva Uni, 2017.

GONÇALVES, Mariana Sbaite. A importância da integração entre a LGPD e a ISO 27018: proteção de dados pessoais em nuvem pública. *Migalhas*, 28 fev. 2024. Disponível em: <https://www.migalhas.com.br/depeso/402514/a-importancia-da-integracao-entre-a-lgpd-e-a-iso-27018>. Acesso em 11 maio 2024.

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

INMETRO. Instituto Nacional de Metrologia, Normalização e Qualidade Industrial. *O que é ISO*. 2024. Disponível em: http://www.inmetro.gov.br/qualidade/responsabilidade_social/o-que-iso.asp. Acesso em 11 maio 2024.

ISO; IEC. *International Standard ISO/IEC 27018*. 2019. Disponível em: <https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027018-2019.pdf>. Acesso em 11 maio 2024.

MICROSOFT. *O que é nuvem*. 2024. Disponível em: <https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-the-cloud/>. Acesso em 11 maio 2024.

MICROSOFT. *Padrões de gerenciamento de segurança de informações ISO/IEC 27001:2013*. 2023. Disponível em: <https://learn.microsoft.com/pt-br/compliance/regulatory/offering-iso-27001>. Acesso em 11 maio 2024.

SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (Coord.); BIONI, Bruno Ricardo (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Editora Forense, 2021.